



Town of Raymond Select Board ePacket January 10, 2023 Table of Contents

(Click on item to go to that page)

Agenda	2
Previous Meeting Minutes	4
East Shore Tavern - Liquor License Application	10
East Shore Tavern - CUM County Calls 2022	21
East Shore Tavern - CUM County Calls 2023	22
East Shore Tavern - Dept of Health Report	23
East Shore Tavern - Fire Marshall's Report.....	27
East Shore Tavern - Dept of Liquor and Labor	37
East Shore Tavern - Special Amusement Application.....	38
Post Issuance Compliance Policy - Red-Lined.....	41
Post Issuance Compliance Policy - Clean.....	46
Liquor License Renewal - The Beacon.....	50
Email to Beacon from Fire Inspector	58
Business License Application - Moon Enterprises DBA Eclipse	59
New Street Name - Sheila's Way	65
MOU Correction - Raymond PFFA IAFF Local 5278.....	66
Cyber Security Policy	67
Quit Claim Deeds	196
RSU #14 Referendum Question Warrant.....	201

Agenda



SELECT BOARD Agenda

October 10, 2023

5:30pm – Regular Meeting

At Broadcast Studio &
Via Zoom & on YouTube

Resolution: We, the Raymond Select Board, recognize our individual and collective responsibilities as leaders and representatives of our community. To this end, we pledge to conduct ourselves in a manner befitting these roles and duties. We pledge and encourage others to "Be the Influence" and to recognize that decisions matter.

- 1) **Call regular meeting to order**
- 2) **Presentation of Plans for New Middle School** – Chris Howell, RSU #14 Superintendent
- 3) **Minutes of previous meetings**
 - a) September 12, 2023
- 4) **Old Business**
 - a) Consideration of Liquor License Application – East Shore Tavern – Kyle Bancroft, owner
 - b) Consideration of Special Amusement License Application – East Shore Tavern – Kyle Bancroft, owner
 - c) Consideration of Update of the Post Issuance Compliance Policy – Charisse Keach, Finance Director
- 5) **New Business**
 - a) Consideration of Liquor License Renewal – The Beacon – Pam & Robert Wing, owners
 - b) Consideration of Business License Application – Moon Enterprises LLC DBA Eclipse – Tyler Monahan, owner
 - c) Introduction of New Librarian – Richard Dowe – Sue Look, Interim Town Manager
 - d) Consideration of New Street Name – Sheila's Way – Bruce Tupper, E911 Addressing Officer
 - e) Consideration of MOU with the New Raymond Professional Fire Fighters Association IAFF Local 5278 – Bruce Tupper, Fire Chief and Michael J Crouse, President
 - f) Consideration of Cyber-Security Policy – Sue Look, Interim Town Manager
 - g) Consideration of Quit Claim Deeds – Sue Carr, Tax Collector

- h) Consideration of the Warrant for the RSU #14 Referendum Vote – Sue Look, Interim Town Manager

6) Public Comment

7) Selectman Comment

8) Town Manager's Report and Communications

a) Confirm Dates for Upcoming Regular Meetings

- November 14, 2023
- December 12, 2023

b) Reminder of Upcoming Events/Holidays

- **October 31, 2023 – Tuesday – 4pm to 9pm – Halloween on Main Street**
 - Running shuttle from Sheri Gagnon Park to Main Street
 - Main Street closed from Southern end at Route 302 to the intersection of Route 121
 - RVL and Town Office will collect candy and monetary donations to help home owners along Main Street
- **November 7, 2023 – Tuesday – 7am-8pm – Referendum Election – JSMS Gym**
 - November 2, 2023 – Thursday – 4pm – Deadline to request an absentee ballot

9) Adjournment

Previous Meeting Minutes



SELECT BOARD Minutes

September 12, 2023

5:30pm – Regular Meeting

At Broadcast Studio &
Via Zoom & on YouTube

Resolution: We, the Raymond Select Board, recognize our individual and collective responsibilities as leaders and representatives of our community. To this end, we pledge to conduct ourselves in a manner befitting these roles and duties. We pledge and encourage others to "Be the Influence" and to recognize that decisions matter.

Select Board members in attendance: Joe Bruno, Rolf Olsen, Teresa Sadak, Samuel Gifford, Derek Ray

Select Board members absent: none

Town Staff in attendance:

Wayne Jones – Fire Inspector
Alex Sirois – CEO
Charisse Keach – Finance Director
Sue Look – Town Clerk

1) **Called to order** at 5:30pm by Chair Bruno

2) **COLAB Broadband High Speed Access Presentation** – Andrew Davis, Sebago Fiber & Wifi LLC owner, and Clara McCool, Regional Broadband Coordinator for GPCOG

Mr Davis and Ms McCool showed a PowerPoint presentation overviewing high speed internet (broadband), the history of the project, and the proposal to roll out for Raymond. Began at the request of several Town Managers who were hearing a need from their citizens. It now encompasses Raymond, Naples, Sebago, Casco and Standish. Goal to recommend a broadband solution. Mission Broadband has been our consultant. Awarded \$50,000 grant from the State of Maine for community outreach and free legal services. Issued RFP to Internet Service Providers for universal coverage of the communities. The Steering Committee consisted of Town Managers, Select Board members, and citizens from each town. 5 ISPs responded and Sebago Fiber with a private ISP with Municipal partner model was awarded the bid. There will be a town financial contribution to connect all of the town buildings on a "dark fiber ring". A ring has redundancy, scalability, equal access, simpler cabling which reduces cost, higher bandwidth, and easier troubleshooting. Spokes will build out from the ring. Initial implementation cost is higher, but ongoing maintenance is much lower for a ring. Sebago Fiber is a Maine based company. They have connected all of Frye Island from 2020-2023. They will do a demand survey to find community support and plan their implementation based on the results. The survey will go out digitally mid-Sept-Oct, with flyers and signage, and with in-person events. There is a "Affordable Connectivity Program" available for citizens who may need a bit of help. Asked for a letter of support for the project in Sebago.

Motion to approve the recommendation letter for the Town of Sebago by Select Olsen.

Seconded by Select Gifford.

Unanimously approved

Motion to continue to the survey phase of the project by Select Olsen. Seconded by Select Gifford.

Unanimously approved

3) Minutes of previous meetings

a) August 15, 2023

Motion to approve as presented by Select Olsen. Seconded by Select Sadak.

Unanimously approved

b) September 5, 2023

Motion to approve as presented by Select Olsen. Seconded by Select Sadak.

Unanimously approved

4) Old Business

a) Consideration of Liquor License Application – East Shore Tavern – Kyle Bancroft, owner

Mr Bancroft hired a different company for the grease hood cleaning and he is missing some filters in the grease hood. Recommend approval contingent upon doing the 6 month cleaning of the grease hood and reinspection at that point. The parking space issue still needs to be corrected. Mr Bancroft has abandoned the expansion of his business to this space and is not using this space for business. CEO Sirois stated that the area must be loamed and seeded to be out of violation or possible signage to stop parking there. Mr Bancroft feels that the violation should not exist as he is not using the parcel for his business. There have been dumpsters parked back there.

The leased parcel behind the building is what is under violation and can not be used for any business purpose. Mr Bancroft said he would add no parking signs around that area. The area around the old tie-dye place is for extra parking if needed. Mr Bancroft said the signs would be added within 7 days, actually by tomorrow.

Motion to approve the liquor license with contingencies of 6 month follow up cleaning and inspection and installation of no parking signs in 7 days for the leased parcel behind the building by Select Olsen. Seconded by Select Sadak.

Unanimously approved

b) Consideration of Special Amusement License Application – East Shore Tavern – Kyle Bancroft, owner

Motion to approve the special amusement license with contingencies of 6 month follow up cleaning and inspection and installation of no parking signs in 7 days for the leased parcel behind the building by Select Olsen. Seconded by Select Sadak.

Unanimously approved

Several citizens spoke up at this point to voice their displeasure that they were not given the opportunity to speak. Chair Bruno said all they had to do was raise their hand. He then allowed their comments.

Carrie Grant, former employee of Mr Bancroft, stated that the employees had not been properly paid, only paid tips. Back lot is used for parking and for dumpsters. She told of discrepancies with purchasing liquor and how much is sold. Cook consistently drinking on the job and bringing in a minor.

CEO Sirois has heard some of these complaints, none of which are land use related.

Courtney Ewards, from Windham, who spoke about a scenario with a neighbor who she said was overserved at East Shore Tavern.

Joe Grant spoke about the serving of underage kids and many police stops for drunk driving.

Mr Bancroft stated that Ms Grant was fired. Ms Grant spoke over Mr Bancroft. Liquor Inspector and Health Inspector found no issue when investigating Ms Grant's claims.

Chair Bruno asked Town Clerk Look to get reports from Dept of Liquor, Dept of Labor, Cumberland County Sheriff's Office, and State Police. Select Sadak will contact DHHS.

Motion to reconsider the liquor license and special amusement by Select Sadak. Seconded by Select Olsen.

Unanimously approved

Motion to table until the next meeting by Select Sadak. Seconded by Select Olsen.

Unanimously approved

5) New Business

- a) Consideration of Business License Application – Paul & Adelen Philippine Store – Paul Wells, owner

Asian grocery store where the gem/jewelry store was. There will be some cold prepared food. Planning to open Friday. If they add more equipment there will need to be an upgrade of circuits.

Motion to approve as presented by Select Olsen. Seconded by Select Gifford.

Unanimously approved

- b) Consideration of Business License Application – Camp Masters – Santino Tarsetti, owner

Camp maintenance business, docks, opening, closing, construction, landscaping, etc. It will be for display and office space.

Motion to approve as presented by Select Olsen. Seconded by Select Ray.

Unanimously approved

c) Consideration of Awarding Revaluation Contract to KRT Appraisal – Curt Lebel, Contract Assessor

We received 2 bids and the committee (Assessor's Agent Lebel, Select Ray, Finance Director Keach, CEO Sirois, and Interim Town Manager Look) unanimously agreed that KRT Appraisal is the company we would like to recommend.

Kevin Leen or KRT (who did Raymond's last revaluation) said that they will meet with town folks as long as necessary after the revaluation.

Motion to award the contract to KRT Appraisal by Select Olsen. Seconded by Select Sadak.

Unanimously approved

d) Consideration of Setting the FY 2023-2024 Mill Rate – Curt Lebel, Contract Assessor

	LAST YEAR (FY 2022-23)		PROPERTY TAX REVENUES		
			THIS YEAR (FY 2023-24) TAX RATE OPTIONS		
TAX RATE	\$	15.00	\$15.80	\$15.90	\$16.00
TAXABLE VALUATION	\$	1,061,314,380.00	\$ 1,071,991,940.00	\$ 1,071,991,940.00	\$ 1,071,991,940.00
COUNTY	\$	817,347.00	\$ 974,325.00	\$ 974,325.00	\$ 974,325.00
SCHOOL	\$	11,370,566.74	\$ 11,940,729.34	\$ 11,940,729.34	\$ 11,940,729.34
TIF AMOUNT	\$	266,042.93	\$ 270,483.28	\$ 272,195.20	\$ 273,907.12
MUNICIPAL	\$	3,406,942.82	\$ 3,711,906.50	\$ 3,810,043.02	\$ 3,908,179.53
OVERLAY	\$	58,816.21	\$ 40,028.53	\$ 47,379.29	\$ 54,730.05
TOTAL PROPERTY TAX	\$	15,919,715.70	\$ 16,937,472.65	\$ 17,044,671.85	\$ 17,151,871.04
Each 1 cent increment on the tax rate will affect overlay by apprx \$10,900					
NON PROPERTY TAX REVENUES USED TO REDUCE MUNICIPAL APPROPRIATION					
	\$	15.00			
HOMESTEAD REIMB	\$	(242,958.60)	\$ (244,584.95)	\$ (246,132.95)	\$ (247,680.96)
BETE REIMB	\$	(53,295.75)	\$ (49,845.84)	\$ (50,161.32)	\$ (50,476.80)
STATE REV SHARING	\$	(505,081.83)	\$ (464,259.71)	\$ (464,259.71)	\$ (464,259.71)
OTHER REVENUES	\$	(1,841,299.00)	\$ (2,015,400.00)	\$ (2,015,400.00)	\$ (2,015,400.00)
SELECT BOARD USE OF FUND BALANCE	\$	(200,000.00)	\$ (200,000.00)	\$ (100,000.00)	\$ -
MUNICIPAL APPROPRIATION	\$	6,249,578.00	\$ 6,685,997.00	\$ 6,685,997.00	\$ 6,685,997.00
TOTAL NON TAX REV	\$	(2,842,635.18)	\$ (2,974,090.50)	\$ (2,875,953.98)	\$ (2,777,817.47)
TOTAL MUNICIPAL TAX REV	\$	3,406,942.82	\$ 3,711,906.50	\$ 3,810,043.02	\$ 3,908,179.53

The Board will be asked to select an amount of fund balance to apply towards the municipal budget and approve a tax rate at its September 12, 2023 meeting. Upon approval of the rate, the necessary warrants and certificates may be completed for signatures by the board members the next day. I will be available at the meeting to answer any follow up questions the board may have. --Curt Lebel

Finance Director Keach said that based on her numbers we would be around 12% in undesignated fund balance (we have a policy to keep this around 15%) if we use \$100,000 to offset taxes. We have over expenditures on attorney fees and Worker's Compensation is over as is Solid Waste.

Motion to set the Mill Rate for FY 2023-2024 at \$15.90 per \$1,000 of valuation by Select Olsen. Seconded by Select Sadak.

Unanimously approved

- e) Consideration of update of the Post Issuance Compliance Policy – Charisse Keach, Finance Director

Town Clerk Look forgot to include the red-lined version in the ePacket, so this will be tabled until the October meeting.

Motion to table until the October regular meeting by Select Olsen. Seconded by Select Sadak.

Unanimously approved

- f) Consideration of Annual Update to General Assistance Ordinance – Sue Look, Interim Town Manager

Motion to approve as presented by Select Olsen. Seconded by Select Gifford.

Unanimously approved

6) Public Comment – none

7) Selectman Comment – none

8) Town Manager's Report and Communications

We have a new Librarian, Richard Dowe. It was unanimous agreement with the hiring committee (Select Olsen, Interim Town Manager Look, Deb Hutchinson – Chair of Friends of RVL, Rec Director Crocker).

The Town Office will be closing at noon on September 28th for a Town Picnic at Tassel Top.

a) Confirm Dates for Upcoming Regular Meetings

- October 10, 2023
- November 14, 2023

9) Executive Session

- a) Discussion of Personnel Issue - pursuant to 1 MRSA §405 (6) (A)

Motion to enter executive session at 7:25pm as noted above by Select Sadak. Seconded by Select Ray.

Unanimously approved

Motion to leave executive session at 7:52pm by Select Olsen. Seconded by Select Gifford.

Unanimously approved

Motion to go forward with the discussed recommendations by Select Olsen.
Seconded by Select Sadak.

Unanimously approved

10) Adjournment

Motion to adjourn at 7:53pm by Select Olsen. Seconded by Select Sadak.

Unanimously approved

Respectfully submitted,

*Susan L Look, Town Clerk
& Interim Town Manager*

East Shore Tavern - Liquor License Application



STATE OF MAINE
DEPARTMENT OF ADMINISTRATIVE AND FINANCIAL SERVICES
BUREAU OF ALCOHOLIC BEVERAGES AND LOTTERY OPERATIONS
DIVISION OF LIQUOR LICENSING AND ENFORCEMENT

Application for an On-Premises License

All Questions Must Be Answered Completely. Please print legibly.

Section I: Licensee/Applicant(s) Information; Type of License and Status

Division Use Only	
License No:	
Class:	By:
Deposit Date:	
Amt. Deposited:	
Payment Type:	
OK with SOS:	Yes <input type="checkbox"/> No <input type="checkbox"/>

Legal Business Entity Applicant Name (corporation, LLC):	Business Name (D/B/A):
BATAIS HOLDINGS LLC	EAST SHORE TAVERN
Individual or Sole Proprietor Applicant Name(s):	Physical Location:
	1248 ROOSEVELT TRAIL RAYMOND, ME
Individual or Sole Proprietor Applicant Name(s):	Mailing address, if different:
	P.O. BOX 896 RAYMOND, ME 04071
Mailing address, if different from DBA address:	Email Address:
	KJSBANCROFT@HOTMAIL.COM
Telephone # Fax #:	Business Telephone # Fax #:
207-807-0842	207-655-6481
Federal Tax Identification Number:	Maine Seller Certificate # or Sales Tax #:
85-1174601	1207642
Retail Beverage Alcohol Dealers Permit:	Website address:
	N/A

1. New license or renewal of existing license? ☐ New Expected Start date: _____

☒ Renewal Expiration Date: 8/19/21

2. The dollar amount of gross income for the licensure period that will end on the expiration date above:

Food: \$120,000.00 Beer, Wine or Spirits: \$110,000.00 Guest Rooms: 0

3. Please indicate the type of alcoholic beverage to be sold: (check all that apply)

☒ Malt Liquor (beer) ☒ Wine ☒ Spirits

4. Indicate the type of license applying for: (choose only one)

- | | | |
|--|---|---|
| <input type="checkbox"/> Restaurant
(Class I, II, III, IV) | <input checked="" type="checkbox"/> Class A Restaurant/Lounge
(Class XI) | <input type="checkbox"/> Class A Lounge
(Class X) |
| <input type="checkbox"/> Hotel
(Class I, II, III, IV) | <input type="checkbox"/> Hotel – Food Optional
(Class I-A) | <input type="checkbox"/> Bed & Breakfast
(Class V) |
| <input type="checkbox"/> Golf Course (included optional licenses, please check if apply)
(Class I, II, III, IV) | <input type="checkbox"/> Auxiliary | <input type="checkbox"/> Mobile Cart |
| <input type="checkbox"/> Tavern
(Class IV) | <input type="checkbox"/> Other: _____ | |
| <input type="checkbox"/> Qualified Caterer | <input type="checkbox"/> Self-Sponsored Events (Qualified Caterers Only) | |

Refer to Section V for the License Fee Schedule on page 9

5. Business records are located at the following address:

1252 ROOSEVELT TRAIL RAYMOND, ME 04071

6. Is the licensee/applicant(s) citizens of the United States? ☒ Yes ☐ No

7. Is the licensee/applicant(s) a resident of the State of Maine? ☒ Yes ☐ No

NOTE: Applicants that are not citizens of the United States are required to file for the license as a business entity.

8. Is licensee/applicant(s) a business entity like a corporation or limited liability company?

☒ Yes ☐ No If Yes, complete Section VII at the end of this application

9. For a licensee/applicant who is a business entity as noted in Section I, does any officer, director, member, manager, shareholder or partner have in any way an interest, directly or indirectly, in their capacity in any other business entity which is a holder of a wholesaler license granted by the State of Maine?

☐ Yes ☒ No

☐ Not applicable – licensee/applicant(s) is a sole proprietor

10. Is the licensee or applicant for a license receiving, directly or indirectly, any money, credit, thing of value, endorsement of commercial paper, guarantee of credit or financial assistance of any sort from any person or entity within or without the State, if the person or entity is engaged, directly or indirectly, in the manufacture, distribution, wholesale sale, storage or transportation of liquor.

☐ Yes ☒ No

If yes, please provide details: _____

11. Do you own or have any interest in any another Maine Liquor License? ☐ Yes ☒ No

If yes, please list license number, business name, and complete physical location address: (attach additional pages as needed using the same format)

Name of Business	License Number	Complete Physical Address

12. List name, date of birth, place of birth for all applicants including any manager(s) employed by the licensee/applicant. Provide maiden name, if married. (attach additional pages as needed using the same format)

Full Name	DOB	Place of Birth
KYLE J. BANCROFT	10/14/1985	PORTLAND, MAINE

Residence address on all the above for previous 5 years

Name	Address:
KYLE BANCROFT	244 MEADOW RD. RAYMOND, ME 04071
Name	Address:
Name	Address:
Name	Address:

13. Will any law enforcement officer directly benefit financially from this license, if issued?

☐ Yes ☒ No

If Yes, provide name of law enforcement officer and department where employed:

14. Has the licensee/applicant(s) ever been convicted of any violation of the liquor laws in Maine or any State of the United States? ☐ Yes ☒ No

If Yes, please provide the following information and attach additional pages as needed using the same format.

Name: _____ Date of Conviction: _____

Offense: _____ Location: _____

Disposition: _____

15. Has the licensee/applicant(s) ever been convicted of any violation of any law, other than minor traffic violations, in Maine or any State of the United States? ☐ Yes ☒ No

If Yes, please provide the following information and attach additional pages as needed using the same format.

Name: _____ Date of Conviction: _____

Offense: _____ Location: _____

Disposition: _____

16. Has the licensee/applicant(s) formerly held a Maine liquor license? ☐ Yes ☒ No

17. Does the licensee/applicant(s) own the premises? ☐ Yes ☒ No

If No, please provide the name and address of the owner:

WILLIAM HAM 142 DARRICK TERRACE HOLDS, ME

18. If you are applying for a liquor license for a Hotel or Bed & Breakfast, please provide the number of guest rooms available: N/A

19. Please describe in detail the area(s) within the premises to be licensed. This description is in addition to the diagram in Section VI. (Use additional pages as needed)

BAR, DINING AREA, DECK & PATIO AREA

20. What is the distance from the premises to the nearest school, school dormitory, church, chapel or parish house, measured from the main entrance of the premises to the main entrance of the school, school dormitory, church, chapel or parish house by the ordinary course of travel?

Name: LAKE REGION BAPTIST CHURCH

Distance: 0.2 MILES

Section II: Signature of Applicant(s)

By signing this application, the licensee/applicant understands that false statements made on this application are punishable by law. Knowingly supplying false information on this application is a Class D Offense under Maine's Criminal Code, punishable by confinement of up to one year, or by monetary fine of up to \$2,000 or by both.

Please sign and date in blue ink.

Dated: 7/1/23


Signature of Duly Authorized Person

Signature of Duly Authorized Person

KYLE BAWCROFT
Printed Name Duly Authorized Person

Printed Name of Duly Authorized Person

Section III: For use by Municipal Officers and County Commissioners only

The undersigned hereby certifies that we have complied with the process outlined in 28-A M.R.S. §653 and approve this on-premises liquor license application.

Dated: _____

Who is approving this application? ☒ Municipal Officers of Raymond

☐ County Commissioners of _____ County

- ☐ **Please Note:** The Municipal Officers or County Commissioners must confirm that the records of Local Option Votes have been verified that allows this type of establishment to be licensed by the Bureau for the type of alcohol to be sold for the appropriate days of the week. Please check this box to indicate this verification was completed.

Signature of Officials	Printed Name and Title
	Joseph Bruno, chair
	Rolf Olsen, Vice-Chair
	Teresa Sadak
	Samuel Gifford
	Derek Ray

**This Application will Expire 60 Days from the date of
Municipal or County Approval unless submitted to the Bureau**

Included below is the section of Maine's liquor laws regarding the approval process by the municipalities or the county commissioners. This is provided as a courtesy only and may not reflect the law in effect at the time of application. Please see <http://www.mainelegislature.org/legis/statutes/28-A/title28-Asec653.html>

§653. Hearings; bureau review; appeal

1. Hearings. The municipal officers or, in the case of unincorporated places, the county commissioners of the county in which the unincorporated place is located, may hold a public hearing for the consideration of applications for new on-premises licenses and applications for transfer of location of existing on-premises licenses. The municipal officers or county commissioners may hold a public hearing for the consideration of requests for renewal of licenses, except that when an applicant has held a license for the prior 5 years and a complaint has not been filed against the applicant within that time, the applicant may request a waiver of the hearing.

A. The bureau shall prepare and supply application forms.

B. The municipal officers or the county commissioners, as the case may be, shall provide public notice of any hearing held under this section by causing a notice, at the applicant's prepaid expense, stating the name and place of hearing, to appear on at least 3 consecutive days before the date of hearing in a daily newspaper having general circulation in the municipality where the premises are located or one week before the date of the hearing in a weekly newspaper having general circulation in the municipality where the premises are located.

C. If the municipal officers or the county commissioners, as the case may be, fail to take final action on an application for a new on-premises license or transfer of the location of an existing on-premises license within 60 days of the filing of an application, the application is deemed approved and ready for action by the bureau. For purposes of this paragraph, the date of filing of the application is the date the application is received by the municipal officers or county commissioners. This paragraph applies to all applications pending before municipal officers or county commissioners as of the effective date of this paragraph as well as all applications filed on or after the effective date of this paragraph. This paragraph applies to an existing on-premises license that has been extended pending renewal. The municipal officers or the county commissioners shall take final action on an on-premises license that has been extended pending renewal within 120 days of the filing of the application.

D. If an application is approved by the municipal officers or the county commissioners but the bureau finds, after inspection of the premises and the records of the applicant, that the applicant does not qualify for the class of license applied for, the bureau shall notify the applicant of that fact in writing. The bureau shall give the applicant 30 days to file an amended application for the appropriate class of license, accompanied by any additional license fee, with the municipal officers or county commissioners, as the case may be. If the applicant fails to file an amended application within 30 days, the original application must be denied by the bureau. The bureau shall notify the applicant in writing of its decision to deny the application including the reasons for the denial and the rights of appeal of the applicant.

2. Findings. In granting or denying an application, the municipal officers or the county commissioners shall indicate the reasons for their decision and provide a copy to the applicant. A license may be denied on one or more of the following grounds:

A. Conviction of the applicant of any Class A, Class B or Class C crime;

B. Noncompliance of the licensed premises or its use with any local zoning ordinance or other land use ordinance not directly related to liquor control;

C. Conditions of record such as waste disposal violations, health or safety violations or repeated parking or traffic violations on or in the vicinity of the licensed premises and caused by persons patronizing or employed by the licensed premises or other such conditions caused by persons patronizing or employed by the licensed premises that unreasonably disturb, interfere with or affect the ability of persons or businesses residing or located in the vicinity of the licensed premises to use their property in a reasonable manner;

D. Repeated incidents of record of breaches of the peace, disorderly conduct, vandalism or other violations of law on or in the vicinity of the licensed premises and caused by persons patronizing or employed by the licensed premises;

D-1. Failure to obtain, or comply with the provisions of, a permit for music, dancing or entertainment required by a municipality or, in the case of an unincorporated place, the county commissioners;

E. A violation of any provision of this Title;

F. A determination by the municipal officers or county commissioners that the purpose of the application is to circumvent the provisions of section 601; and

G. After September 1, 2010, server training, in a program certified by the bureau and required by local ordinance, has not been completed by individuals who serve alcoholic beverages.

3. Appeal to bureau. Any applicant aggrieved by the decision of the municipal officers or county commissioners under this section may appeal to the bureau within 15 days of the receipt of the written decision of the municipal officers or county commissioners. The bureau shall hold a public hearing in the city, town or unincorporated place where the premises are situated. In acting on such an appeal, the bureau may consider all licensure requirements and findings referred to in subsection 2.

A. Repealed

B. If the decision appealed from is an application denial, the bureau may issue the license only if it finds by clear and convincing evidence that the decision was without justifiable cause.

4. Repealed

5. Appeal to District Court. Any person or governmental entity aggrieved by a bureau decision under this section may appeal the decision to the District Court within 30 days of receipt of the written decision of the bureau.

An applicant who files an appeal or who has an appeal pending shall pay the annual license fee the applicant would otherwise pay. Upon resolution of the appeal, if an applicant's license renewal is denied, the bureau shall refund the applicant the prorated amount of the unused license fee.

Section IV: Terms and Conditions of Licensure as an Establishment that sells liquor for on-premises consumption in Maine

- The licensee/applicant(s) agrees to be bound by and comply with the laws, rules and instructions promulgated by the Bureau.
- The licensee/applicant(s) agrees to maintain accurate records related to an on-premise license as required by the law, rules and instructions promulgated or issued by the Bureau if a license is issued as a result of this application.
 - The licensee/applicant(s) authorizes the Bureau to obtain and examine all books, records and tax returns pertaining to the business, for which this liquor license is requested, and also any books, records and returns during the year in which any liquor license is in effect.
- Any change in the licensee's/applicant's licensed premises as defined in this application must be approved by the Bureau in advance.
- All new applicants must apply to the Alcohol and Tobacco Tax and Trade Bureau (TTB) for its [Retail Beverage Alcohol Dealers](https://www.ttb.gov/nrc/retail-beverage-alcohol-dealers) permit. See the TTB's website at <https://www.ttb.gov/nrc/retail-beverage-alcohol-dealers> for more information.

Section V: Fee Schedule

Filing fee required. In addition to the license fees listed below, a filing fee of \$10.00 must be included with all applications.

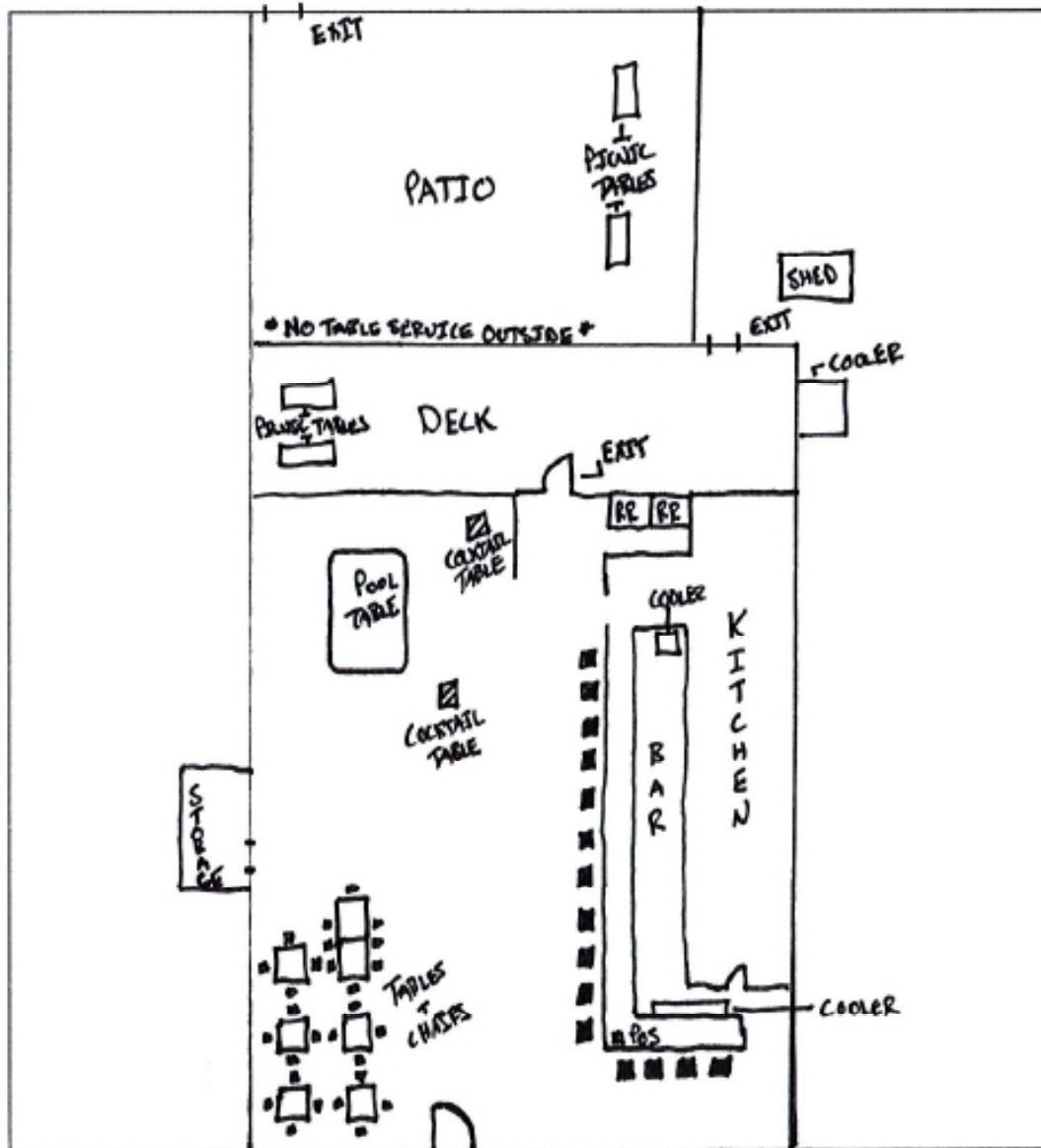
Please note: For Licensees/Applicants in unorganized territories in Maine, the \$10.00 filing fee must be paid directly to County Treasurer. All applications received by the Bureau from licensees/applicants in unorganized territories must submit proof of payment was made to the County Treasurer together with the application.

Class of License	Type of liquor/Establishments included	Fee
Class I	For the sale of liquor (malt liquor, wine and spirits) This class includes: Airlines; Civic Auditoriums; Class A Restaurants; Clubs with catering privileges; Dining Cars; Golf Courses; Hotels; Indoor Ice-Skating Clubs; Indoor Tennis Clubs; Vessels; Qualified Caterers	\$ 900.00
Class I-A	For the sale of liquor (malt liquor, wine and spirits) This class includes only hotels that do not serve three meals a day.	\$1,100.00
Class II	For the Sale of Spirits Only This class includes: Airlines; Civic Auditoriums; Class A Restaurants; Clubs with catering privileges; Dining Cars; Golf Courses; Hotels; Indoor Ice-Skating Clubs; Indoor Tennis Clubs; and Vessels.	\$ 550.00
Class III	For the Sale of Wine Only This class includes: Airlines; Civic Auditoriums; Class A Restaurants; Clubs with catering privileges; Dining Cars; Golf Courses; Hotels; Indoor Ice-Skating Clubs; Indoor Tennis Clubs; Restaurants; Vessels; Pool Halls; and Bed and Breakfasts.	\$ 220.00
Class IV	For the Sale of Malt Liquor Only This class includes: Airlines; Civic Auditoriums; Class A Restaurants; Clubs with catering privileges; Dining Cars; Golf Courses; Hotels; Indoor Ice-Skating Clubs; Indoor Tennis Clubs; Restaurants; Taverns; Pool Halls; and Bed and Breakfasts.	\$ 220.00
Class III and IV	For the Sale of Malt Liquor and Wine Only This class includes: Airlines; Civic Auditoriums; Class A Restaurants; Clubs with catering privileges; Dining Cars; Golf Courses; Hotels; Indoor Ice-Skating Clubs; Indoor Tennis Clubs; Restaurants; Vessels; Pool Halls; and Bed and Breakfasts.	\$ 440.00
Class V	For the sale of liquor (malt liquor, wine and spirits) This class includes only a Club without catering privileges.	\$ 495.00
Class X	For the sale of liquor (malt liquor, wine and spirits) This class includes only a Class A Lounge	\$2,200.00
Class XI	For the sale of liquor (malt liquor, wine and spirits) This class includes only a Restaurant Lounge	\$1,500.00

Section VI Premises Floor Plan

In an effort to clearly define your license premise and the areas that consumption and storage of liquor authorized by your license type is allowed, the Bureau requires all applications to include a diagram of the premise to be licensed.

Diagrams should be submitted on this form and should be as accurate as possible. Be sure to label the following areas: entrances, office area, coolers, storage areas, display cases, shelves, restroom, point of sale area, area for on-premise consumption, dining rooms, event/function rooms, lounges, outside area/decks or any other areas on the premise that you are requesting approval. Attached an additional page as needed to fully describe the premise.



Section VII: Required Additional Information for a Licensee/Applicant for an On-Premises Liquor License Who are Legal Business Entities

Questions 1 to 4 of this part of the application must match information in Section I of the application above and match the information on file with the Maine Secretary of State's office. If you have questions regarding your legal entity name or DBA, please call the Secretary of State's office at (207) 624-7752.

All Questions Must Be Answered Completely. Please print legibly.

1. Exact legal name: BATAIT HOLDINGS LLC
2. Doing Business As, if any: EAST SHORE TAVERN
3. Date of filing with Secretary of State: 5/26/2020 State in which you are formed: MAINE
4. If not a Maine business entity, date on which you were authorized to transact business in the State of Maine:
N/A
5. List the name and addresses for previous 5 years, birth dates, titles of officers, directors, managers, members or partners and the percentage ownership any person listed: (attached additional pages as needed)

Name	Address (5 Years)	Date of Birth	Title	Percentage of Ownership
KYLE BANCROFT	244 MEADOW RD. RAYMOND ME	10/14/85	MANAGER	100%

(Ownership in non-publicly traded companies must add up to 100%.)

East Shore Tavern - CUM County Calls 2022



Cumberland County Sheriff's Office

Calls for Service to East Shore Tavern

Year 2022



Nature of Incident	Total Incidents
911 Cell Hangup	1
Assault	1
Attempt to Locate	1
Citizen Assist	1
Information	7
Intoxication	1
Pedestrian Check	1
Traffic Offense	2

Report Total: **15**

Report Includes:

All dates between `00:00:01 01/01/22` and `23:59:59 12/31/22`
All agencies matching `0300`
All issuing officers
All areas matching **Raymond**
All violations

East Shore Tavern - CUM County Calls 2023



Cumberland County Sheriff's Office

Calls for Service to East Shore Tavern

January 1, 2023 - September 12, 2023



Nature of Incident	Total Incidents
911 Cell Hangup	1
911 Misdial	2
Attempt to Locate	1
Citizen Assist	1
Criminal Trespass	1
Intoxication	1
Theft	1
Traffic Offense	6

Report Total: **14**

Report Includes:

All dates between `00:00:01 01/01/23` and `23:59:59 09/12/23`

All agencies matching `0300`

All issuing officers

All areas matching `Raymond`

All violations

East Shore Tavern - Dept of Health Report

<input type="checkbox"/> Failed <input type="checkbox"/> Closed <input type="checkbox"/> IHH		State of Maine Health Inspection Report		Page 1 of 4	
Establishment Name CAFE SEBAGO		As Authorized by 22 MRSA § 2496		Critical Violations 2	Date 12/22/2022
		Non-Critical Violations 6		Time In 3:30 PM	
		Certified Food Protection Manager Y		Time Out 4:30 PM	
License Expiry Date/EST. ID# 7/10/2023 / 1052		Address 1248 ROOSEVELT TRL		City RAYMOND	Zip Code 04071
License Type EATING PLACE 30-75 SEATS		Owner Name BATALI HOLDINGS LLC		Purpose of Inspection Regular	Telephone 207-807-0842
				License Posted Yes	Risk Category

FOODBORNE ILLNESS RISK FACTORS AND PUBLIC HEALTH INTERVENTIONS					
Circle designated compliance status (IN, OUT, N/O, N/A) for each numbered item <small>IN=in compliance OUT=not in compliance N/O=not observed N/A=not applicable</small>			Mark "X" in appropriate box for COS and/or R <small>COS=corrected on-site during inspection R=repeat violation</small>		
Compliance Status			COS	R	
Supervision					
1	IN	PIC present, demonstrates knowledge, and performs duties			
Employee Health					
2	IN	Management awareness; policy present			
3	IN	Proper use of reporting, restriction & exclusion			
Good Hygienic Practices					
4	OUT	Proper eating, tasting, drinking, or tobacco use			
5	IN	No discharge from eyes, nose, and mouth			
Preventing Contamination by Hands					
6	IN	Hands clean & properly washed			
7	IN	No bare hand contact with RTE foods or approved alternate method properly followed			
8	IN	Adequate handwashing facilities supplied & accessible			
Approved Source					
9	IN	Food obtained from approved source			
10	IN	Food received at proper temperature			
11	IN	Food in good condition, safe, & unadulterated			
12	IN	Required records available: shellstock tags parasite destruction			
Protection from Contamination					
13	IN	Food separated & protected			
14	IN	Food-contact surfaces: cleaned and sanitized			
15	IN	Proper disposition of returned, previously served, reconditioned, & unsafe food			

GOOD RETAIL PRACTICES					
Good Retail Practices are preventative measures to control the addition of pathogens, chemicals, and physical objects into foods.					
Mark "X" in box if numbered item is not in compliance Mark "X" in appropriate box for COS and/or R COS=corrected on-site during inspection R=repeat violation					
Compliance Status			COS	R	
Safe Food and Water					
28	IN	Pasteurized eggs used where required			
29	IN	Water & ice from approved source			
30	IN	Variance obtained for specialized processing methods			
Food Temperature Control					
31	IN	Proper cooling methods used; adequate equipment for temperature control			
32	IN	Plant food properly cooked for hot holding			
33	IN	Approved thawing methods used			
34	X	Thermometers provided and accurate			
Food Identification					
35	IN	Food properly labeled; original container			
Prevention of Food Contamination					
36	IN	Insects, rodents, & animals not present			
37	X	Contamination prevented during food preparation, storage & display			
38	X	Personal cleanliness			
39	IN	Wiping cloths: properly used & stored			
40	IN	Washing fruits & vegetables			

GOOD RETAIL PRACTICES					
Good Retail Practices are preventative measures to control the addition of pathogens, chemicals, and physical objects into foods.					
Mark "X" in box if numbered item is not in compliance Mark "X" in appropriate box for COS and/or R COS=corrected on-site during inspection R=repeat violation					
Compliance Status			COS	R	
Proper Use of Utensils					
41	IN	In-use utensils: properly stored			
42	IN	Utensils, equipment, & linens: properly stored, dried, & handled			
43	IN	Single-use & single-service articles: properly stored & used			
44	IN	Gloves used properly			
Utensils, Equipment and Vending					
45	IN	Food & non-food contact surfaces cleanable, properly designed, constructed, & used			
46	IN	Warewashing facilities: installed, maintained, & used; test strips			
47	IN	Non-food contact surfaces clean			
Physical Facilities					
48	IN	Hot & cold water available; adequate pressure			
49	IN	Plumbing installed; proper backflow devices			
50	IN	Sewage & waste water properly disposed			
51	IN	Toilet facilities: properly constructed, supplied, & cleaned			
52	X	Garbage & refuse properly disposed; facilities maintained			
53	X	Physical facilities installed, maintained, & clean			
54	X	Adequate ventilation & lighting; designated areas used			

Person in Charge (Signature) <i>Luisa Stardella</i>		Date: 12/22/2022	
Health Inspector (Signature) <i>Stuart Leckie</i>			
Follow-up: <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		Date of Follow-up:	

State of Maine Health Inspection Report

Page 2 of 4

Establishment Name CAFE SEBAGO		As Authorized by 22 MRSA § 2496		Date 12/22/2022
License Expiry Date/EST. ID# 7/10/2023 / 1052	Address 1248 ROOSEVELT TRL	City / State RAYMOND / ME	Zip Code 04071	Telephone 207-807-0842

Temperature Observations

Location	Temperature	Notes
Dish machine	180	
3 Bay	112	Wash
Hot holding	167	Mac and cheese
Hot holding	165	Chili
Hot holding	165	Meatballs
Prep unit	40	Cheese
Freezer	0	
Prep unit	38	Blue cheese

Person in Charge (Signature)

Luisa Stardella

Date: 12/22/2022

Health Inspector (Signature)

STUART LECKIE

Stuart Leckie

HHE-601(a)Rev.01/07/10

State of Maine Health Inspection Report

Page 3 of 4

Establishment Name CAFE SEBAGO				Date 12/22/2022	
License Expiry Date/EST. ID# 7/10/2023 / 1052	Address 1248 ROOSEVELT TRL	City / State RAYMOND ME	Zip Code 04071		

Observations and Corrective Actions

Violations cited in this report must be corrected within the time frames below, or as stated in sections 8-405.11 and 8-406.11 of the Food Code

54: 6-303.11: N: Insufficient lighting provided.

INSPECTOR NOTES: Light is out in walk in. Replace bulb

53: 6-501.11: N: The physical facilities are in disrepair.

INSPECTOR NOTES: Missing tiles near dishwasher and utilities need fixing. Floors should be smooth, durable and easy to clean

52: 5-501.110: N: Refuse, Recyclables, and Returnables accessible to insects / rodents.

INSPECTOR NOTES: Dumpster lids should be closed at all times

38: 2-402.11: N: Food Employees not wearing effective hair restraints.

INSPECTOR NOTES: Kitchen employee needs an affective hair restraint

37: 3-305.11: N: Food not protected from contamination during storage.

INSPECTOR NOTES: Food on floor in walk in cooler. All food should be 6 inches off the floor

34: 4-204.112.(A): N: Temperature measuring device not properly located.

INSPECTOR NOTES: All coolers and refrigerators need to have a thermometer

20: 3-501.16.(A).(2): C: PHF not maintained at 41 F or less.

INSPECTOR NOTES: Salad dressings on shelf need to be refrigerated

4: 2-401.11: C: Food employee is eating, drinking, or using any tobacco where the contamination of exposed FOOD; clean EQUIPMENT, UTENSILS, and LINENS; unwrapped SINGLE-SERVICE and SINGLE-USE ARTICLES; or other items needing protection can result.

INSPECTOR NOTES: All beverages should be in cup with a lid and a straw or with a sippy cup

Person in Charge (Signature)

Luisa Stardella

Date: 12/22/2022

Health Inspector (Signature)

Stuart Leckie

STUART LECKIE

State of Maine Health Inspection Report

Page 4 of 4

Establishment Name CAFE SEBAGO				Date 12/22/2022	
License Expiry Date/EST. ID# 7/10/2023 / 1052	Address 1248 ROOSEVELT TRL	City / State RAYMOND ME	Zip Code 04071		

Inspection Notes

This inspection was conducted and reviewed on-site with Luisa Sbardella. (luisasbaard21@gmail.com) The report was entered in remote format and finalized off-site. The name of the PIC was printed in the signature block by the inspector with prior permission obtained from the PIC. The PIC's actual signature was not obtained. A copy of this report has been provided to the PIC via email.

Certified Food Protection Manager: Luisa Sbardella

Every eating establishment must employ on its staff a Certified Food Protection Manager (CFPM). Some establishments are exempt from this requirement. A CFPM certificate must accompany the application for a new establishment and change of ownership. A CFPM must be hired within 60 days of the departure of the last CFPM leaving employment. Eating establishments must post in a conspicuous area the certification of the CFPM(s), and the certificate must be made available to the Department upon request. For a list of CFPM courses and trainers go to <http://www.maine.gov/healthinspection/training.htm>. Please provide a copy of this certification(s) to Casandra Lavallee, Health Inspection Program, 286 Water St. 3rd Floor, Augusta, ME 04333, casandra.lavallee@maine.gov or faxing to 207-287-3165. Please include the name of your establishment and the establishment ID# with your certification(s).

Employee Health Policy

The Health Inspection Program implemented an educational public health initiative on Employee Health on March 1, 2017. The policy handouts will be provided to you by your inspector and reviewed during inspection for compliance. They are also available on the Program's website: <http://www.maine.gov/healthinspection>

Violation Correction Timeframe

Critical violations should be corrected on site, but in any event, within 10 days. The licensee must contact your inspector, Stuart Leckie when the critical violation has been addressed at (207)441-2798 or Stuart.Leckie@maine.gov. Non-critical violations must be corrected within 30 days. Failure to satisfactorily correct these violations before the follow-up inspection may result in enforcement proceedings by the Department to include fines and penalties. License renewals can be denied if violations are not corrected within the noted timeframes.

C= Critical violation and NC= Non-critical violation

"Critical violation" means a provision of the Food Code that, if in non-compliance, is more likely than other violations to contribute to food contamination, illness or environmental health hazard.

Additional Inspection Fee

License fees provide for two inspections per year. When additional inspections are required, the Department may charge an additional \$100 fee to cover the costs of each additional inspection or visit.

Document Retention/Posting

Pursuant to the Maine Food Code, the establishment's current license must be displayed. In addition, a sign or placard must be posted in a conspicuous area notifying consumers that a copy of the most recent inspection report is available upon request. If you have received your inspection report via email, please print and retain onsite. CFPM certificates must be posted in a conspicuous area and must be available to the Department upon request.

Person in Charge (Signature)

Luisa Sbardella

Date: 12/22/2022

Health Inspector (Signature)

Stuart Leckie

STUART LECKIE

East Shore Tavern - Fire Marshall's Report



INSPECTION SHEET
STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL

RECEIVED

JUL 31 2023

11 am

FIRE MARSHAL'S OFFICE ENTERTAINMENT LICENSING

LICENSE: DAN50726 - CAFE SEBAGO BAR & GRILL

Inspection Start : 07/11/2023 Req'd By: 08/11/2023 Status: INSPECTION HAS BEEN REQUESTED

Type: DANCE/THEATER/HAUNTED HOUSE PERMIT

Location: 1248 ROOSEVELT TRL
RAYMOND, ME 04071-6602

County: CUMBERLAND
Phone: +1 (207) 655-6481

Territory: BRITTANY WHITE

Req'd Insp Attributes:

Appl Rec'd Date: 07/11/2023

Field date: 07/11/2023

Attributes (General):

File Number: 87216

Contacts:

WILLIAM HAM II (BLDOWNER)
142 DARBICK TER, HOLLIS CENTER, ME 04042-3844
BATALI HOLDINGS LLC (KEY)
PO BOX 896, RAYMOND, ME 04071-0896
BATALI HOLDINGS LLC (OW)
PO BOX 896, RAYMOND, ME 04071-0896

Phone: +1 (207) 400-6057

Phone: +1 (207) 807-0842

Phone: +1 (207) 807-0842

Date/Insp.	Code	Violation

OK to Issue: ☒

Date of Inspection: 7/31/23

Plan of Correction required: ☐

Date of Revisit:

Revisit is required before approval: ☐

Exit Interview w/:

Inspector:

7/27/23 -

(signature of owner or rep.)

Date Printed: 07/12/2023



STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL
52 STATE HOUSE STATION
AUGUSTA, ME 04333-0052

No. 50726

In accordance with the provisions of M.R.S.A. Title 8, Sec. 161 license is hereby granted to the person named herein to use the premises named herein for dancing purposes. Any changes to the structure or layout of the building that affects exiting, seating layout, occupant capacities or safety of the occupants shall be submitted to this Office for approval at least 10 days prior to any scheduled change. The owner and/or operator of the facility must submit a request for renewal of this License at least 30 days prior to the expiration of this License.

Licensee: BATALI HOLDINGS LLC

Mailing Address: BATALI HOLDINGS LLC
PO BOX 896
RAYMOND, ME 04071-0896

Hall: CAFE SEBAGO BAR & GRILL

Hall Address: 1248 ROOSEVELT TRL, RAYMOND, ME 04071-6602

Permit Date: 09/09/2023

Expiration Date: 09/08/2024

8,217,998.00

0.00


COMMISSIONER OF PUBLIC SAFETY



STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL
52 STATE HOUSE STATION
AUGUSTA, ME 04333-0052



No. 50726

**CAFE SEBAGO BAR & GRILL
DANCE FLOOR**

The following limitations have been set for this facility and/or room as specified here:

Maximum Occupancy: 112

Maximum capacity with tables and chairs: 70

Maximum capacity without tables and chairs: 112

Any change of these limitations shall be applied for in writing and a new inspection may be required. This information shall be posted in a prominent location at the main entrance of the facility and/or room that has these limitations. These limitations are calculated by the use of specific formulas and do not reflect limitations set forth by other agencies or authorities having jurisdiction. Other entities may be more restrictive than the limitations set herein. Any violations of these limits may constitute a class E crime under MRSA 25 Subsection 2452.

Expiration Date: 09/08/2024



STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL
52 STATE HOUSE STATION
AUGUSTA, ME 04333-0052



No. 50726

CAFE SEBAGO BAR & GRILL
OUTSIDE PATIO AREA

The following limitations have been set for this facility and/or room as specified here:

Maximum Occupancy: 125

Maximum capacity with tables and chairs: 109

Maximum capacity without tables and chairs: 125

Any change of these limitations shall be applied for in writing and a new inspection may be required. This information shall be posted in a prominent location at the main entrance of the facility and/or room that has these limitations. These limitations are calculated by the use of specific formulas and do not reflect limitations set forth by other agencies or authorities having jurisdiction. Other entities may be more restrictive than the limitations set herein. Any violations of these limits may constitute a class E crime under MRSA 25 Subsection 2452.

Expiration Date: 09/08/2024



INSPECTION SHEET
STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL

RECEIVED
SEP 09 2022

BY:

FIRE MARSHAL'S OFFICE ENTERTAINMENT LICENSING

LICENSE: DAN58726 - CAFE SEBAGO BAR & GRILL

* 3591-1 *

Inspection Start : 08/09/2022 Req'd By: 09/09/2022 Status: INSPECTION HAS BEEN REQUESTED

Type: DANCE/THEATER/HAUNTED HOUSE PERMIT

Location: 1248 ROOSEVELT TRL
RAYMOND, ME 04071-6602

County: CUMBERLAND
Phone: +1 (207) 655-6481

Territory: BRITTANY WHITE

Req'd Insp Attributes:

Appl Rec'd Date: 08/09/2022

Field date: 08/09/2022

Attributes (General):

File Number: 87216

Contacts:

WILLIAM HAM II (BLDOWNER)
142 DARBICK TER, HOLLIS CENTER, ME 04042-3844
BATALLI HOLDINGS LLC (KEY)
PO BOX 896, RAYMOND, ME 04071-0896
BATALLI HOLDINGS LLC (OW)
PO BOX 896, RAYMOND, ME 04071-0896

Phone: +1 (207) 400-6057

Phone: +1 (207) 807-0842

Phone: +1 (207) 807-0842

Date/Ins.	Code	Violation
8/11/22		

OK to Issue: ☒

Date of Inspection: 8/11/22

Plan of Correction required: ☐

Date of Revisit: _____

Revisit is required before approval: ☐

Exit Interview w/: _____

Inspector: *[Signature]*

(signature of owner or rep.)

Kj.bancroft@hotmail.com
8/23/22 - emailed Kyle

Date Printed: 08/10/2022



STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL
52 STATE HOUSE STATION
AUGUSTA, ME 04333-0052

No. 50726

In accordance with the provisions of M.R.S.A. Title 8, Sec. 161 license is hereby granted to the person named herein to use the premises named herein for dancing purposes. Any changes to the structure or layout of the building that affects exiting, seating layout, occupant capacities or safety of the occupants shall be submitted to this Office for approval at least 10 days prior to any scheduled change. The owner and/or operator of the facility must submit a request for renewal of this License at least 30 days prior to the expiration of this License.

Licensee: BATALI HOLDINGS LLC
Mailing Address: BATALI HOLDINGS LLC
PO BOX 896
RAYMOND, ME 04071-0896
Hall: CAFE SEBAGO BAR & GRILL
Hall Address: 1248 ROOSEVELT TRL, RAYMOND, ME 04071-6602
Permit Date: 09/09/2022

Expiration Date: 09/08/2023

7,992,056.00

0.00


COMMISSIONER OF PUBLIC SAFETY



STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL
52 STATE HOUSE STATION
AUGUSTA, ME 04333-0052



No. 50726

**CAFE SEBAGO BAR & GRILL
DANCE FLOOR**

The following limitations have been set for this facility and/or room as specified here:

Maximum Occupancy: 112
Maximum capacity with tables and chairs: 70
Maximum capacity without tables and chairs: 112

Any change of these limitations shall be applied for in writing and a new inspection may be required. This information shall be posted in a prominent location at the main entrance of the facility and/or room that has these limitations. These limitations are calculated by the use of specific formulars and do not reflect limitations set forth by other agencies or authorities having jurisdiction. Other entities may be more restrictive than the limitations set herein. Any violations of these limits may constitute a class E crime under MRSA 25 Subsection 2452.

Expiration Date: 09/08/2023



STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL
52 STATE HOUSE STATION
AUGUSTA, ME 04333-0052



No. 50726

CAFE SEBAGO BAR & GRILL
OUTSIDE PATIO AREA

The following limitations have been set for this facility and/or room as specified here:

Maximum Occupancy: 125

Maximum capacity with tables and chairs: 109

Maximum capacity without tables and chairs: 125

Any change of these limitations shall be applied for in writing and a new inspection may be required. This information shall be posted in a prominent location at the main entrance of the facility and/or room that has these limitations. These limitations are calculated by the use of specific formulas and do not reflect limitations set forth by other agencies or authorities having jurisdiction. Other entities may be more restrictive than the limitations set herein. Any violations of these limits may constitute a class E crime under MRSA 25 Subsection 2452.

Expiration Date: 09/08/2023

Janet T Mills
Governor



**Maine Department of Public Safety
State Fire Marshal's Office
52 State House Station
Augusta, Maine 04333-0052**



Michael Sauschuck
Commissioner
Chief Joseph Thomas
State Fire Marshal
Phone: 207-626-3870
Fax: 207-287-6251

Statement of Deficiencies and Plan of Corrections

Facility Name: Café Sebago Bar & Grill Location: 1248 Roosevelt Trl Raymond, ME 04071 Facility Type: Entertainment License Telephone : 207-655-6481 Resource ID : File :	Owner Name: Address: Date:
During an inspection of your facility a certified State Inspector has found the following violations.	In this right hand column you are required to indicate how and when you will have these violations corrected. Complete this information and return this "Plan of Correction" to the above address within 10 days of receipt of this statement.

Maximum Capacity

DJ table, dance floor and bar stools – 112

Tables, chairs and bar stools – 70

Outside patio area with 6 picnic tables – 109

Outside patio area with 1 table – 125

*This report does not indicate violations, only capacity.

Pending P.O.C.

Date of Inspection: 8/26/21
Inspector: Brittany M. White
cc:

Owner/Occupant Signature:
Date:



STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL
52 STATE HOUSE STATION
AUGUSTA, ME 04333-0052

No. 50726

In accordance with the provisions of M.R.S.A. Title 8, Sec. 161 license is hereby granted to the person named herein to use the premises named herein for dancing purposes. Any changes to the structure or layout of the building that affects exiting, seating layout, occupant capacities or safety of the occupants shall be submitted to this Office for approval at least 10 days prior to any scheduled change. The owner and/or operator of the facility must submit a request for renewal of this License at least 30 days prior to the expiration of this License.

Licensee: BATALI HOLDINGS LLC
Mailing Address: BATALI HOLDINGS LLC
PO BOX 896
RAYMOND, ME 04071-0896
Hall: CAFE SEBAGO BAR & GRILL
Hall Address: 1248 ROOSEVELT TRL, RAYMOND, ME 04071-6602
Permit Date: 08/27/2021

Expiration Date: 08/26/2022


COMMISSIONER OF PUBLIC SAFETY



STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL
52 STATE HOUSE STATION
AUGUSTA, ME 04333-0052



No. 50726

**CAFE SEBAGO BAR & GRILL
DANCE FLOOR**

The following limitations have been set for this facility and/or room as specified here:

Maximum Occupancy: 112
Maximum capacity with tables and chairs: 70
Maximum capacity without tables and chairs: 112

Any change of these limitations shall be applied for in writing and a new inspection may be required. This information shall be posted in a prominent location at the main entrance of the facility and/or room that has these limitations. These limitations are calculated by the use of specific formulars and do not reflect limitations set forth by other agencies or authorities having jurisdiction. Other entities may be more restrictive than the limitations set herein. Any violations of these limits may constitute a class E crime under MRSA 25 Subsection 2452.

Expiration Date: 08/26/2022



STATE OF MAINE - DEPARTMENT OF PUBLIC SAFETY
OFFICE OF STATE FIRE MARSHAL
52 STATE HOUSE STATION
AUGUSTA, ME 04333-0052



No. 50726

**CAFE SEBAGO BAR & GRILL
OUTSIDE PATIO AREA**

The following limitations have been set for this facility and/or room as specified here:

Maximum Occupancy: 125

Maximum capacity with tables and chairs: 109

Maximum capacity without tables and chairs: 125

Any change of these limitations shall be applied for in writing and a new inspection may be required. This information shall be posted in a prominent location at the main entrance of the facility and/or room that has these limitations. These limitations are calculated by the use of specific formulars and do not reflect limitations set forth by other agencies or authorities having jurisdiction. Other entities may be more restrictive than the limitations set herein. Any violations of these limits may constitute a class E crime under MRSA 25 Subsection 2452.

Expiration Date: 08/26/2022

East Shore Tavern - Dept of Liquor and Labor



Susan L Look
Interim Town Manager

401 Webbs Mills Road
Raymond, Maine 04071

207-655-4742 x121

September 13, 2023

TO: Select Board
FROM: Sue Look, Interim Town Manager
RE: Phone Conversations Pertaining to Café Sebago/East Shore Tavern

I spoke with Larry Sanborn at the ME Dept of Liquor, and he said they have been in to inspect, and have sent in undercover officers, and have not seen evidence of wrongdoing. He did say that their inspections are a bit "hit or miss" since they can not send in officers often and in any establishment it may take several visits before any questionable activity is witnessed.

I also spoke with Bart Hutchinson at the ME Dept of Labor, and he said there was 1 complaint in 2021 about not paying employees (totaling \$2,200) that was not investigated. He said they would check into the current status of the business's labor practices.

East Shore Tavern - Special Amusement Application



Town of Raymond
401 Webbs Mills Road
Raymond, Maine 04071
207.655.4742

SPECIAL AMUSEMENT APPLICATION

Pursuant to the Town of Raymond Special Amusement Ordinance and 28-A MRSA §1054

1. Name of Applicant: BATALI HOLDINGS LLC
2. Address of Applicant: P.O. BOX 896 RAYMOND, ME 04071
3. Name of Business: EAST SHORE TAVERN
4. Business Street Address: 1248 ROOSEVELT TRAIL RAYMOND, ME 04071
5. Business Mailing Address: P.O. BOX 896 RAYMOND, ME 04071
6. Telephone – Cell: 207-807-0842 Business: 207-655-6481
7. List the names and addresses of all officers and their residency for the preceding 3 years.

KYLE BANCROFT P.O. BOX 896 RAYMOND, ME 04071

8. Have any of the officers been convicted of a Class A, B, or C crime in the last 3 years?
If so, who and describe the offense:

NONE

9. Please describe the premises including security measures being taken, size, seating, etc.

OPEN ROOM, PATIO AREA, SECURITY LATE / WEEKENDS

10. Has applicant ever had a license denied or revoked? If so, describe the circumstances.

NO

11. Please specify the type of entertainment in detail: [If extra space is required, please attach a separate piece of paper.]

DJ, LIVE MUSIC, OPEN MIC NIGHT

12. List the days and hours of entertainment:

8PM - 12AM

NOTE: "I understand that false statements made on this form are punishable by law. Knowingly supplying false information on this form is a Class D offense under the Criminal Code, punishable by confinement of up to one year or by monetary fine of up to \$500.00 for each offense or by both. Each day that a violation occurred shall be considered a separate offense."

13. The fee must be paid at the time of application. The application fee is \$50.00 plus all advertising costs if a public hearing is necessary.


Signature of Applicant

7/28/23
Date

NOTE: Special amusement permits expire at the same time as the liquor license.

Conditions of Approval: _____

Authorizing signatures:

Code Enforcement Officer: _____

Public Safety: _____

Town Manager: _____

Select Board: _____

Post Issuance Compliance Policy - Red-Lined

~~Town of Raymond~~
~~STATE OF MAINE~~
~~TOWN OF RAYMOND~~

POST ISSUANCE COMPLIANCE POLICY

The Town ~~of Raymond (the “Town”)~~ issues tax-exempt bonds, ~~notes, leases, and other obligations (“Obligations”)~~ from time to time to finance various capital improvements. As an issuer of such ~~tax-exempt bonds~~ ~~Obligations~~, the Town is required by the Internal Revenue Code of 1986, as amended, (the “Code”) and regulations promulgated by the United States Treasury Department to take certain actions subsequent to the issuance of such ~~Obligations~~ ~~bonds~~ to ensure their continuing tax-ex~~empt status.~~ ~~empt status of the bonds.~~

The Town recognizes that compliance with applicable provisions of the Code and Treasury Regulations is an on-going process, necessary during the entire term of a bond issue, and is an integral component of the Town's overall debt-management responsibilities. These requirements apply equally to capital leases. Accordingly, the implementation of these requirements will require on-going monitoring and consultation with Bond Counsel.

Issuance:

The Select Board shall approve the terms and structure of ~~bonds~~ ~~Obligations~~ issued by the Town. Such ~~bonds~~ ~~Obligations~~ shall be issued in accordance with United States Treasury Department Regulations, the Internal Revenue Code of 1986, as amended, and State statutes. Specific post-issuance compliance procedures are addressed below.

General Procedures:

The following guidelines will be used to monitor compliance with post-issuance requirements:

1. The Town Treasurer, or the Treasurer's designee, shall serve as the Compliance Officer and shall be the person primarily responsible for ensuring that the Town successfully carries out its post issuance responsibilities. The Compliance Officer shall be assisted by the following persons or entities:

- a. Bond Counsel
- b. Financial Advisor
- c. Paying Agent
- d. Rebate Specialist

The Compliance Officer shall be responsible for assigning post-issuance responsibilities to other staff, Bond Counsel, the Financial Advisor, the Paying Agent, and the Rebate Specialist, and shall utilize such other professional services as are necessary to ensure compliance with all post-issuance requirements.

2. The Compliance Officer shall verify that the following post-issuance actions have been

taken on behalf of the Town with respect to each issue of tax-exempt ~~bonds~~Obligations:

- a. Ensure that a full and complete record for the principal documents of each issue has been completed by Bond Counsel and the Financial Advisor;
- b. Ensure that the Internal Revenue Service (IRS) forms 8038 are properly filed with the IRS by Bond Counsel within the time limits imposed by Section 149(c) of the Code;
- c. Account for the allocation of the proceeds of the tax-exempt ~~bonds~~Obligations to expenditures as required by the Code;
- d. Coordinate receipt and retention of relevant books and records with respect to the investment and expenditures of the issue proceeds;
- e. Identify proceeds of tax-exempt ~~O~~bligations, in consultation with Bond Counsel and the Financial Advisor, that are yield-restricted and monitor the investments of any yield-restricted funds to ensure that the yield on such investments does not exceed the bond yield to which such investments are restricted;
- f. Determine, in consultation with Bond Counsel and the Financial Advisor, whether the Town is subject to the rebate requirements of Section 148(f) of the Code and related Treasury Regulations with respect to each issue of the Town.
The Compliance Officer shall contact a Rebate Specialist, as required, prior to the fifth anniversary of the date of issuance of each issue and each fifth anniversary thereafter until the obligation has matured to arrange for calculation of the rebate requirements, as needed, to be paid by the Town. If any rebate is required to be paid to the IRS, the Town Compliance Officer will file Form 8038-T, along with the required payment;
- ~~g.~~ Shall monitor the use of all financed facilities in order to determine whether private business uses of financed facilities have exceeded the de minimus limits set forth in Section 141(b) of the Code (generally a value or benefit equal to 10% of issue proceeds) that provide special legal entitlements to non-governmental persons; ~~and-~~
- ~~g-h.~~ Shall, with the assistance of professional services as needed, ensure that all nonqualified Obligations are remediated according to the requirements of the Code and relevant regulations.

3. The Compliance Officer shall collect and retain the following records with respect to each issue of tax-exempt ~~O~~bligations and with respect to the facilities financed with the proceeds of such Obligations:

- a. Audited financial statements of the Town;
- b. Appraisals, surveys, feasibility studies, if any, with respect to the facilities to be financed with issue proceeds;
- c. Trustee or Paying Agent statements;
- d. Records of all investments and the gains (or losses) from such investments;
- e. Expenditures reimbursed with the issue proceeds;
- f. Allocation of ~~issue~~Obligations proceeds to expenditures (including cost of issuance) and the dates and amounts of each expenditure (including requisitions, draw down schedules, invoices, bills, and canceled checks as related to each

- expenditure);
- g. Construction or renovation contracts for financed facilities or projects;
- h. Maintain an asset list of all tax-exempt financed depreciable property and sales of tax-exempt financed assets;
- i. Arbitrage rebate reports and records of rebate and yield reduction payments, if any;
- j. Orders, Resolutions, and other actions, if any, adopted by the Town subsequent to the date of issue of the ~~O~~bligations; and
- k. Relevant correspondence relating to such ~~bonds~~Obligations.

The records collected by the Town shall be stored in any format deemed appropriate by the Compliance Officer and shall be retained for a period equal to the life of the tax-exempt obligations, including the life of any obligations issued to refund obligations, plus three (3) years.

~~a. The Compliance Officer, with assistance from such other officers, employees, and agents of the Town as necessary, shall be informed of and review financial information and operating data to be filed with the MSRB pursuant to the CDAs, including, but not limited to, annual audited financial information and annual operating data as identified in documents offering the Town's security obligations for sale (the "Annual Filing");~~

~~b. The Compliance Officer shall file the Annual Filing with the MSRB through EMMA by the deadline established by law, regulation, and/or the CDAs;~~

4. Prior to the change in use, sale, lease, or rent of any bond-financed asset, the Compliance Officer shall be consulted in order to ensure compliance with applicable Code provisions and Treasury Regulations. In the event that an action is found to cause an issue to meet the private business tests or the private loan financing tests, the Compliance Officer and other necessary Town officials, in consultation with Bond Counsel, may undertake the remedial action steps listed in 26 C.F.R. § 1.141-12.

5. In the event of a violation of the applicable rules for tax-exempt Obligations, the Compliance Officer, and other necessary Town officials, in consultation with Bond Counsel, may participate in the Tax-Exempt Bonds Voluntary Closing Agreement Program in order to conclusively resolve the violation as expeditiously as possible.

6. In addition to its post-issuance compliance requirements under the Code and Treasury Regulations, the Town has agreed to provide Continuing Disclosure, such as annual financial and operating data and event notices ("Continuing Disclosure Documents") as required pursuant to law, regulation, and/or such Continuing Disclosure Agreements ("CDAs") into which the Town may enter. The Town has also agreed to file such Continuing Disclosure Documents with the Municipal Securities Rulemaking Board ("MSRB") through the Electronic Municipal Market Access System ("EMMA"). The continuing disclosure obligations are governed by the CDAs, the Continuing Disclosure Documents, and by the terms of Rule 15c2-12 under the Securities and

Exchange Act of 1934, as amended and officially interpreted from time to time. Among its Continuing Disclosure obligations, the Town shall undertake the following:

- a. In connection with the offering by the Town of any securities for sale on the public market, the Compliance Officer, with assistance from such other officers, employees, and agents of the Town as necessary, shall review any relevant offering documents, including but not limited to: preliminary official statements, final official statements, or investor presentations (“Offering Documents”), to ensure the material facts in the Offering Documents appear to be consistent with those known to the Town; and Offering Documents do not omit any material facts necessary to be included to prevent the Offering Documents from being misleading to investors;
- b. Prior to posting of a final official statement, the Town Board of Selectmen will review the same and **only after** their authorization **shall** the final official statement be posted;
- c. The Compliance Officer, with assistance from such other officers, employees, and agents of the Town as necessary, shall be informed of and review financial information and operating data to be filed with the MSRB pursuant to the CDAs, including, but not limited to, annual audited financial information and annual operating data (the “Annual Filing”), as identified in documents offering the Town’s security obligations for sale;
- d. The Compliance Officer shall file the Annual Filing with the MSRB through EMMA by the deadline established by law, regulation, and/or the CDAs;
- e. The Compliance Officer shall maintain a list of events, which if material to investors, the Town is required to provide notice of to the MSRB pursuant to law, regulation, and/or the CDAs (“Disclosure Event(s)”). Such Disclosure Events include, but are not limited to, failure to provide annual financial information on or before the date agreed to by the Town; principal and interest payment delinquencies; non-payment related defaults; unscheduled draws on debt service; reserves reflecting financial difficulties; unscheduled draws on credit enhancements reflecting financial difficulties; substitution of credit or liquidity providers, or their failure to perform; adverse tax opinions or events affecting the tax status of the security; modifications to rights of security holders; bond calls and tender offers; defeasances; release, substitution or sale of property securing repayment of the securities; rating changes; bankruptcy, insolvency or receivership; merger, acquisition or sale of all issuer assets; appointment of successor trustee; or incurrence of a material financial obligation;
- f. Upon the occurrence of a Disclosure Event the Compliance Officer shall involve such other officers, employees, and agents of the Town as necessary and shall: (1) assess the materiality of any Disclosure Event with the assistance of legal counsel and, if notice of the event must be given; (b) prepare an Event Notice giving notice of the event and file the same with EMMA;

- g. The Compliance Officer shall periodically review the Town's websites to ensure that: (a) material third-party information is not linked or referred to without appropriate disclaimers, is not hyperlinked, and is not included unless the Compliance Officer has reason to believe that it is reliable, and identifies the source of the information; (b) dated material information is removed from the websites or moved to a clearly labeled archives page; (c) all material financial and operating data is presented as of a specific date with appropriate disclaimers as to the currency of the data; (d) no material forward-looking statements (projections, forecasts, etc.) are included unless they are based on reasonable assumptions and are accompanied by a description of the substantial risks to achieving the forecasted results; and (e) the material information presented is consistent with the knowledge of such persons and not internally inconsistent; and
- h. The Compliance Officer shall undertake periodic disclosure training, which shall address the requirements of federal and state securities laws and the CDAs, the meaning of "material," and the duties of such officers, employees, and agents under this Policy.

Date of Town Board of Selectmen Adoption: _____, 2021

Post Issuance Compliance Policy - Clean

STATE OF MAINE TOWN OF RAYMOND POST ISSUANCE COMPLIANCE POLICY

The Town of Raymond (the “Town”) issues tax-exempt bonds, notes, leases, and other obligations (“Obligations”) from time to time to finance various capital improvements. As an issuer of such Obligations, the Town is required by the Internal Revenue Code of 1986, as amended, (the “Code”) and regulations promulgated by the United States Treasury Department to take certain actions subsequent to the issuance of such Obligations to ensure their continuing tax-exempt status.

The Town recognizes that compliance with applicable provisions of the Code and Treasury Regulations is an on-going process, necessary during the entire term of a bond issue, and is an integral component of the Town's overall debt-management responsibilities. These requirements apply equally to capital leases. Accordingly, the implementation of these requirements will require on-going monitoring and consultation with Bond Counsel.

Issuance:

The Select Board shall approve the terms and structure of Obligations issued by the Town. Such Obligations shall be issued in accordance with United States Treasury Department Regulations, the Internal Revenue Code of 1986, as amended, and State statutes. Specific post-issuance compliance procedures are addressed below.

General Procedures:

The following guidelines will be used to monitor compliance with post-issuance requirements:

1. The Town Treasurer, or the Treasurer's designee, shall serve as the Compliance Officer and shall be the person primarily responsible for ensuring that the Town successfully carries out its post issuance responsibilities. The Compliance Officer shall be assisted by the following persons or entities:
 - a. Bond Counsel
 - b. Financial Advisor
 - c. Paying Agent
 - d. Rebate Specialist

The Compliance Officer shall be responsible for assigning post-issuance responsibilities to other staff, Bond Counsel, the Financial Advisor, the Paying Agent, and the Rebate Specialist, and shall utilize such other professional services as are necessary to ensure compliance with all post-issuance requirements.

2. The Compliance Officer shall verify that the following post-issuance actions have been taken on behalf of the Town with respect to each issue of tax-exempt Obligations:
 - a. Ensure that a full and complete record for the principal documents of each issue has been completed by Bond Counsel and the Financial Advisor;
 - b. Ensure that the Internal Revenue Service (IRS) forms 8038 are properly filed with the IRS

by Bond Counsel within the time limits imposed by Section 149(c) of the Code;

- c. Account for the allocation of the proceeds of the tax-exempt Obligations to expenditures as required by the Code;
- d. Coordinate receipt and retention of relevant books and records with respect to the investment and expenditures of the issue proceeds;
- e. Identify proceeds of tax-exempt Obligations, in consultation with Bond Counsel and the Financial Advisor, that are yield-restricted and monitor the investments of any yield-restricted funds to ensure that the yield on such investments does not exceed the bond yield to which such investments are restricted;
- f. Determine, in consultation with Bond Counsel and the Financial Advisor, whether the Town is subject to the rebate requirements of Section 148(f) of the Code and related Treasury Regulations with respect to each issue of the Town.

The Compliance Officer shall contact a Rebate Specialist, as required, prior to the fifth anniversary of the date of issuance of each issue and each fifth anniversary thereafter until the obligation has matured to arrange for calculation of the rebate requirements, as needed, to be paid by the Town. If any rebate is required to be paid to the IRS, the Town Compliance Officer will file Form 8038-T, along with the required payment;

- g. Shall monitor the use of all financed facilities in order to determine whether private business uses of financed facilities have exceeded the de minimis limits set forth in Section 141(b) of the Code (generally a value or benefit equal to 10% of issue proceeds) that provide special legal entitlements to non-governmental persons; and
- h. Shall, with the assistance of professional services as needed, ensure that all nonqualified Obligations are remediated according to the requirements of the Code and relevant regulations.

3. The Compliance Officer shall collect and retain the following records with respect to each issue of tax-exempt Obligations and with respect to the facilities financed with the proceeds of such Obligations:

- a. Audited financial statements of the Town;
- b. Appraisals, surveys, feasibility studies, if any, with respect to the facilities to be financed with issue proceeds;
- c. Trustee or Paying Agent statements;
- d. Records of all investments and the gains (or losses) from such investments;
- e. Expenditures reimbursed with the issue proceeds;
- f. Allocation of Obligations proceeds to expenditures (including cost of issuance) and the dates and amounts of each expenditure (including requisitions, draw down schedules, invoices, bills, and canceled checks as related to each expenditure);
- g. Construction or renovation contracts for financed facilities or projects;
- h. Maintain an asset list of all tax-exempt financed depreciable property and sales of tax-exempt financed assets;
- i. Arbitrage rebate reports and records of rebate and yield reduction payments, if any;

- j. Orders, Resolutions, and other actions, if any, adopted by the Town subsequent to the date of issue of the Obligations; and
- k. Relevant correspondence relating to such Obligations.

The records collected by the Town shall be stored in any format deemed appropriate by the Compliance Officer and shall be retained for a period equal to the life of the tax-exempt obligations, including the life of any obligations issued to refund obligations, plus three (3) years.

- 4. Prior to the change in use, sale, lease, or rent of any bond-financed asset, the Compliance Officer shall be consulted in order to ensure compliance with applicable Code provisions and Treasury Regulations. In the event that an action is found to cause an issue to meet the private business tests or the private loan financing tests, the Compliance Officer and other necessary Town officials, in consultation with Bond Counsel, may undertake the remedial action steps listed in 26 C.F.R. § 1.141-12.
- 5. In the event of a violation of the applicable rules for tax-exempt Obligations, the Compliance Officer, and other necessary Town officials, in consultation with Bond Counsel, may participate in the Tax-Exempt Bonds Voluntary Closing Agreement Program in order to conclusively resolve the violation as expeditiously as possible.
- 6. In addition to its post-issuance compliance requirements under the Code and Treasury Regulations, the Town has agreed to provide Continuing Disclosure, such as annual financial and operating data and event notices (“Continuing Disclosure Documents”) as required pursuant to law, regulation, and/or such Continuing Disclosure Agreements (“CDAs”) into which the Town may enter. The Town has also agreed to file such Continuing Disclosure Documents with the Municipal Securities Rulemaking Board (“MSRB”) through the Electronic Municipal Market Access System (“EMMA”). The continuing disclosure obligations are governed by the CDAs, the Continuing Disclosure Documents, and by the terms of Rule 15c2-12 under the Securities and Exchange Act of 1934, as amended and officially interpreted from time to time. Among its Continuing Disclosure obligations, the Town shall undertake the following:
 - a. In connection with the offering by the Town of any securities for sale on the public market, the Compliance Officer, with assistance from such other officers, employees, and agents of the Town as necessary, shall review any relevant offering documents, including but not limited to: preliminary official statements, final official statements, or investor presentations (“Offering Documents”), to ensure the material facts in the Offering Documents appear to be consistent with those known to the Town; and Offering Documents do not omit any material facts necessary to be included to prevent the Offering Documents from being misleading to investors;
 - b. Prior to posting of a final official statement, the Town Board of Selectmen will review the same and only after their authorization shall the final official statement be posted;
 - c. The Compliance Officer, with assistance from such other officers, employees, and agents of the Town as necessary, shall be informed of and review financial information and operating data to be filed with the MSRB pursuant to the CDAs, including, but not limited to, annual audited financial information and annual operating data (the “Annual Filing”),

as identified in documents offering the Town's security obligations for sale;

- d. The Compliance Officer shall file the Annual Filing with the MSRB through EMMA by the deadline established by law, regulation, and/or the CDAs;
- e. The Compliance Officer shall maintain a list of events, which if material to investors, the Town is required to provide notice of to the MSRB pursuant to law, regulation, and/or the CDAs ("Disclosure Event(s)"). Such Disclosure Events include, but are not limited to, failure to provide annual financial information on or before the date agreed to by the Town; principal and interest payment delinquencies; non-payment related defaults; unscheduled draws on debt service; reserves reflecting financial difficulties; unscheduled draws on credit enhancements reflecting financial difficulties; substitution of credit or liquidity providers, or their failure to perform; adverse tax opinions or events affecting the tax status of the security; modifications to rights of security holders; bond calls and tender offers; defeasances; release, substitution or sale of property securing repayment of the securities; rating changes; bankruptcy, insolvency or receivership; merger, acquisition or sale of all issuer assets; appointment of successor trustee; or incurrence of a material financial obligation;
- f. Upon the occurrence of a Disclosure Event the Compliance Officer shall involve such other officers, employees, and agents of the Town as necessary and shall: (1) assess the materiality of any Disclosure Event with the assistance of legal counsel and, if notice of the event must be given; (b) prepare an Event Notice giving notice of the event and file the same with EMMA;
- g. The Compliance Officer shall periodically review the Town's websites to ensure that: (a) material third-party information is not linked or referred to without appropriate disclaimers, is not hyperlinked, and is not included unless the Compliance Officer has reason to believe that it is reliable, and identifies the source of the information; (b) dated material information is removed from the websites or moved to a clearly labeled archives page; (c) all material financial and operating data is presented as of a specific date with appropriate disclaimers as to the accuracy of the data; (d) no material forward-looking statements (projections, forecasts, etc.) are included unless they are based on reasonable assumptions and are accompanied by a description of the substantial risks to achieving the forecasted results; and (e) the material information presented is consistent with the knowledge of such persons and not internally inconsistent; and
- h. The Compliance Officer shall undertake periodic disclosure training, which shall address the requirements of federal and state securities laws and the CDAs, the meaning of "material," and the duties of such officers, employees, and agents under this Policy.

Given unto our hands on the 10th day of October, 2023:

Joseph Bruno, Chair

Samuel Gifford

Rolf Olsen, Vice-Chair

Derek Ray

Teresa Sadak

Liquor License Renewal - The Beacon



STATE OF MAINE
DEPARTMENT OF ADMINISTRATIVE AND FINANCIAL SERVICES
BUREAU OF ALCOHOLIC BEVERAGES AND LOTTERY OPERATIONS
DIVISION OF LIQUOR LICENSING AND ENFORCEMENT

Application for an On-Premises License

All Questions Must Be Answered Completely. Please print legibly.

Section I: Licensee/Applicant(s) Information; Type of License and Status

Division Use Only	
License No:	
Class:	By:
Deposit Date:	
Amt. Deposited:	
Payment Type:	
OK with SOS: Yes <input type="checkbox"/> No <input type="checkbox"/>	

Legal Business Entity Applicant Name (corporation, LLC): The Beacon, Inc.	Business Name (D/B/A): The Beacon
Individual or Sole Proprietor Applicant Name(s): Pamela & Robert Wing	Physical Location: 1233 Roosevelt Trail Unit 15
Individual or Sole Proprietor Applicant Name(s):	Mailing address, if different: PO Box 1063, Raymond, ME 04071
Mailing address, if different from DBA address:	Email Address: pwing2@maine.rr.com
Telephone # Fax #: (207) 232-9817	Business Telephone # Fax #: (207) 655-6432
Federal Tax Identification Number: 82-4788353	Maine Seller Certificate # or Sales Tax #: 1190974
Retail Beverage Alcohol Dealers Permit:	Website address:

1. New license or renewal of existing license? ☐ New Expected Start date: _____
☒ Renewal Expiration Date: **9/25/23**
2. The dollar amount of gross income for the licensure period that will end on the expiration date above:
Food: **\$400,000** Beer, Wine or Spirits: **\$5,000** Guest Rooms: **0**
3. Please indicate the type of alcoholic beverage to be sold: (check all that apply)
☒ Malt Liquor (beer) ☐ Wine ☐ Spirits

4. Indicate the type of license applying for: (choose only one)

- | | | |
|--|--|---|
| <input checked="" type="checkbox"/> Restaurant
(Class I, II, III, IV) | <input type="checkbox"/> Class A Restaurant/Lounge
(Class XI) | <input type="checkbox"/> Class A Lounge
(Class X) |
| <input type="checkbox"/> Hotel
(Class I, II, III, IV) | <input type="checkbox"/> Hotel – Food Optional
(Class I-A) | <input type="checkbox"/> Bed & Breakfast
(Class V) |
| <input type="checkbox"/> Golf Course (included optional licenses, please check if apply)
(Class I, II, III, IV) | <input type="checkbox"/> Auxiliary | <input type="checkbox"/> Mobile Cart |
| <input type="checkbox"/> Tavern
(Class IV) | <input type="checkbox"/> Other: _____ | |
| <input type="checkbox"/> Qualified Caterer | <input type="checkbox"/> Self-Sponsored Events (Qualified Caterers Only) | |

Refer to Section V for the License Fee Schedule on page 9

5. Business records are located at the following address:

1233 Roosevelt Trail, Raymond, ME 04071

6. Is the licensee/applicant(s) citizens of the United States? ☒ Yes ☐ No

7. Is the licensee/applicant(s) a resident of the State of Maine? ☒ Yes ☐ No

NOTE: Applicants that are not citizens of the United States are required to file for the license as a business entity.

8. Is licensee/applicant(s) a business entity like a corporation or limited liability company?

☒ Yes ☐ No If Yes, complete Section VII at the end of this application

9. For a licensee/applicant who is a business entity as noted in Section I, does any officer, director, member, manager, shareholder or partner have in any way an interest, directly or indirectly, in their capacity in any other business entity which is a holder of a wholesaler license granted by the State of Maine?

☐ Yes ☒ No

☐ Not applicable – licensee/applicant(s) is a sole proprietor

10. Is the licensee or applicant for a license receiving, directly or indirectly, any money, credit, thing of value, endorsement of commercial paper, guarantee of credit or financial assistance of any sort from any person or entity within or without the State, if the person or entity is engaged, directly or indirectly, in the manufacture, distribution, wholesale sale, storage or transportation of liquor.

☐ Yes ☒ No

If yes, please provide details: _____

11. Do you own or have any interest in any another Maine Liquor License? ☐ Yes ☒ No

If yes, please list license number, business name, and complete physical location address: (attach additional pages as needed using the same format)

Name of Business	License Number	Complete Physical Address

12. List name, date of birth, place of birth for all applicants including any manager(s) employed by the licensee/applicant. Provide maiden name, if married. (attach additional pages as needed using the same format)

Full Name	DOB	Place of Birth
Pamela Rene' Wing (Affhim)	10/27/1974	Portland, ME
Robert Patrick Wing	4/4/1970	Lewiston, ME

Residence address on all the above for previous 5 years

Name	Address:
Pamela Wing	5 Alfred Mann Dr. Raymond, ME 04071
Name	Address:
Robert Wing	5 Alfred Mann Dr. Raymond, ME 04071
Name	Address:
Name	Address:

13. Will any law enforcement officer directly benefit financially from this license, if issued?

☐ Yes ☒ No

If Yes, provide name of law enforcement officer and department where employed:

14. Has the licensee/applicant(s) ever been convicted of any violation of the liquor laws in Maine or any State of the United States? ☐ Yes ☒ No

If Yes, please provide the following information and attach additional pages as needed using the same format.

Name: _____ Date of Conviction: _____

Offense: _____ Location: _____

Disposition: _____

15. Has the licensee/applicant(s) ever been convicted of any violation of any law, other than minor traffic violations, in Maine or any State of the United States? ☐ Yes ☒ No

If Yes, please provide the following information and attach additional pages as needed using the same format.

Name: _____ Date of Conviction: _____

Offense: _____ Location: _____

Disposition: _____

16. Has the licensee/applicant(s) formerly held a Maine liquor license? ☒ Yes ☐ No

17. Does the licensee/applicant(s) own the premises? ☐ Yes ☒ No

If No, please provide the name and address of the owner:

SAMP 1233 LLC, 91 Sidney St. Suite 315 Cambridge, MA 02139

18. If you are applying for a liquor license for a Hotel or Bed & Breakfast, please provide the number of guest rooms available: _____

19. Please describe in detail the area(s) within the premises to be licensed. This description is in addition to the diagram in Section VI. (Use additional pages as needed)

Small dining room (seats 30 people)
Offer counter service & take out service
Small section w/ chips, soda, treats, (Beer behind counter)

20. What is the distance from the premises to the **nearest** school, school dormitory, church, chapel or parish house, measured from the main entrance of the premises to the main entrance of the school, school dormitory, church, chapel or parish house by the ordinary course of travel?

Name: Lake Region Baptist Church

Distance: 4 miles away

Section II: Signature of Applicant(s)

By signing this application, the licensee/applicant understands that false statements made on this application are punishable by law. Knowingly supplying false information on this application is a Class D Offense under Maine's Criminal Code, punishable by confinement of up to one year, or by monetary fine of up to \$2,000 or by both.

Please sign and date in blue ink.

Dated: 9/25/23

Pamela R. Wing
Signature of Duly Authorized Person

Robert F. Wing
Signature of Duly Authorized Person

Pamela R. Wing
Printed Name Duly Authorized Person

Robert F. Wing
Printed Name of Duly Authorized Person

Section III: For use by Municipal Officers and County Commissioners only

The undersigned hereby certifies that we have complied with the process outlined in 28-A M.R.S. §653 and approve this on-premises liquor license application.

Dated: _____

Who is approving this application? ☐ Municipal Officers of _____

☐ County Commissioners of _____ County

- ☐ **Please Note:** The Municipal Officers or County Commissioners must confirm that the records of Local Option Votes have been verified that allows this type of establishment to be licensed by the Bureau for the type of alcohol to be sold for the appropriate days of the week. Please check this box to indicate this verification was completed.

Signature of Officials	Printed Name and Title

**This Application will Expire 60 Days from the date of
Municipal or County Approval unless submitted to the Bureau**

Included below is the section of Maine's liquor laws regarding the approval process by the municipalities or the county commissioners. This is provided as a courtesy only and may not reflect the law in effect at the time of application. Please see <http://www.mainelegislature.org/legis/statutes/28-A/title28-Asec653.html>

§653. Hearings; bureau review; appeal

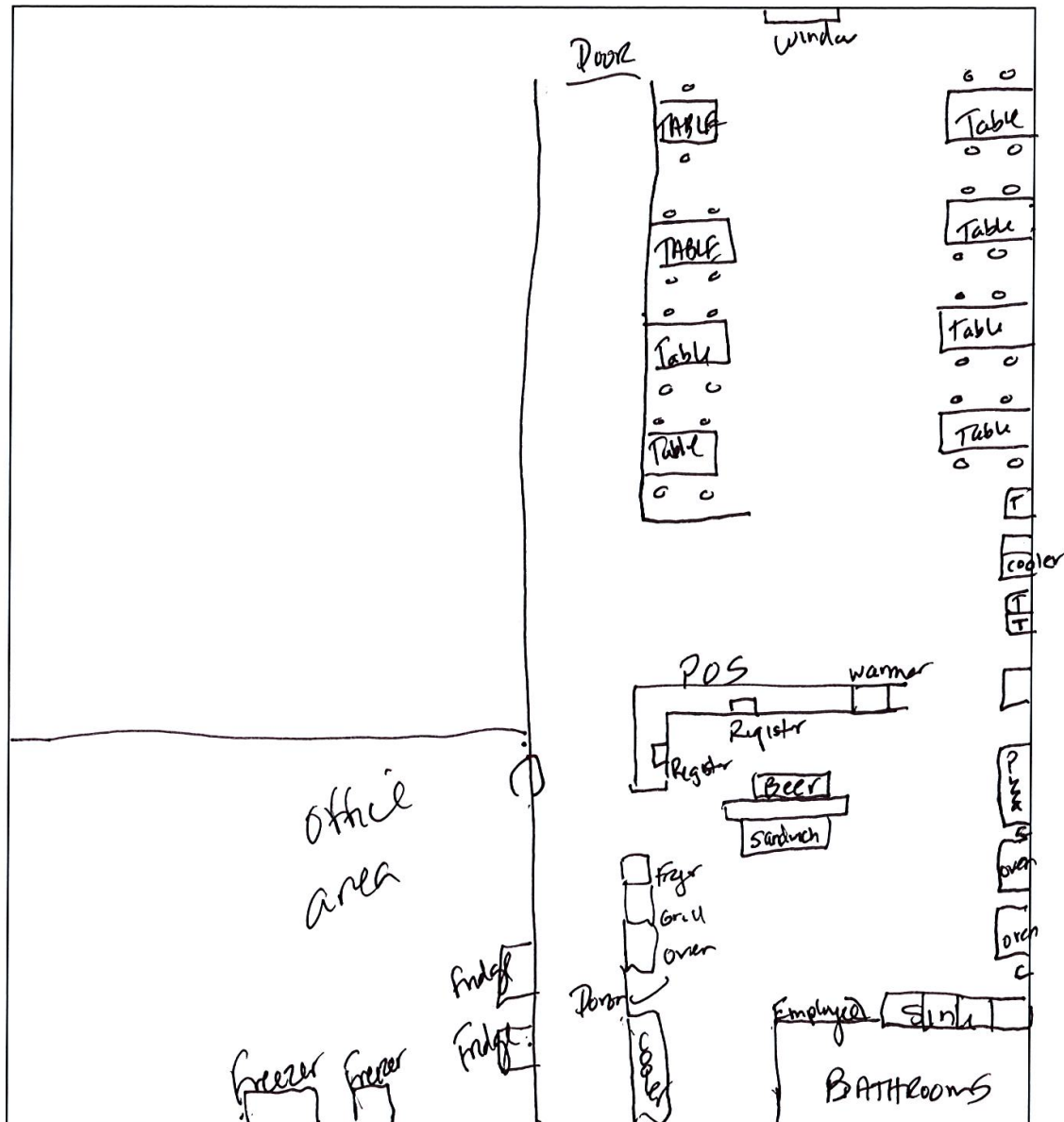
1. Hearings. The municipal officers or, in the case of unincorporated places, the county commissioners of the county in which the unincorporated place is located, may hold a public hearing for the consideration of applications for new on-premises licenses and applications for transfer of location of existing on-premises licenses. The municipal officers or county commissioners may hold a public hearing for the consideration of requests for renewal of licenses, except that when an applicant has held a license for the prior 5 years and a complaint has not been filed against the applicant within that time, the applicant may request a waiver of the hearing.

A. The bureau shall prepare and supply application forms.

Section VI Premises Floor Plan

In an effort to clearly define your license premise and the areas that consumption and storage of liquor authorized by your license type is allowed, the Bureau requires all applications to include a diagram of the premise to be licensed.

Diagrams should be submitted on this form and should be as accurate as possible. Be sure to label the following areas: entrances, office area, coolers, storage areas, display cases, shelves, restroom, point of sale area, area for on-premise consumption, dining rooms, event/function rooms, lounges, outside area/decks or any other areas on the premise that you are requesting approval. Attached an additional page as needed to fully describe the premise.



Section VII: Required Additional Information for a Licensee/Applicant for an On-Premises Liquor License Who are Legal Business Entities

Questions 1 to 4 of this part of the application must match information in Section I of the application above and match the information on file with the Maine Secretary of State's office. If you have questions regarding your legal entity name or DBA, please call the Secretary of State's office at (207) 624-7752.

All Questions Must Be Answered Completely. Please print legibly.

1. Exact legal name: The Beacon, Inc.
2. Doing Business As, if any: The Beacon
3. Date of filing with Secretary of State: 2018 State in which you are formed: Maine
4. If not a Maine business entity, date on which you were authorized to transact business in the State of Maine:

5. List the name and addresses for previous 5 years, birth dates, titles of officers, directors, managers, members or partners and the percentage ownership any person listed: (attached additional pages as needed)

Name	Address (5 Years)	Date of Birth	Title	Percentage of Ownership
Pamela René Wing	5A Alfred Mann Dr. Raymond, ME	10/27/1974	President	50%
Robert Patrick Wing	5A Alfred Mann Dr. Raymond ME	4/4/1970	Clerk	50%

(Ownership in non-publicly traded companies must add up to 100%.)

Email to Beacon from Fire Inspector

From: "Wayne Jones" <wayne.jones@raymondmaine.org>
To: "pwing2@maine.rr.com" <pwing2@maine.rr.com>, "rwing@yahoo.com" <rwing@yahoo.com>, "rwing84@yahoo.com" <rwing84@yahoo.com>, "Sue Look" <Sue.Look@raymondmaine.org>
Cc: "Wayne Jones" <wayne.jones@raymondmaine.org>
Date: 10/02/2023 12:53 PM
Subject: Re: Scheduling RFRD Fire & Life Safety Inspection for Liquor License Application - 2023

Dear Pam & Bob,

I wanted to reach out with this email in order to make this application process as seamless for you as possible. I was informed by the Town Office that you have submitted your Annual Liquor License Application

For the Life Safety inspection, there are a number of items that would need to be addressed prior to scheduling your inspection with us. I wanted to provide you with a bulleted list, allowing adequate time for you to complete them before your Liquor License expires with the State.

Here is the list of items to check on prior to scheduling the fire inspection.

- Current (2023) annual NFPA 72 Fire Alarm System Inspection, Testing & Maintenance Report conducted in June 2023 is currently on file with the RFRD. The business owner shall provide a copy of the NFPA 72 Inspection, Testing & Maintenance Report from the fire alarm company (including testing all initiation points, the Hood suppression system activation of the fire alarm system, and LP gas supply shuts-off operations). The NFPA 72 Inspection & Testing report will be submitted to the Raymond Fire Rescue Department (RFRD) for the file.
- Current (2023 annual Grease Hood Fire Suppression System Annual Inspection, Testing & Maintenance. The business owner shall provide copy of test report from the Testing Company for RFRD file.
- Current (2023) Grease Hood Semi-Annual cleaning with a copy of these semi-annual reports submitted for RFRD file.
- Current (2023) Fire Extinguisher Annual Inspection, Testing & Maintenance with current years Inspection Tag(s) in place.

Also please check to ensure these items from previous Inspection Reports have been corrected.

- Ensure all Exit Doors, Exit Signs and Emergency Lights are working properly.
- Ensure that there are no grease accumulations in the kitchen including walls and ceiling areas.
- The Exit that discharges into the rear Exit Foyer needs to maintain a clear, full width pathway (exit discharge), from the exit door out through the rear double Exit Doors, and down the rear stairs to the parking lot (with no obstructions in the Exit pathways).
- CO/Gas detection is installed and operating.
- Ensure all Exit Doors are unobstructed and working properly including the self-closers.
- Waste Grease is stored properly in waste grease dumpster(s) and is placed at least 10 feet from the building.
- Copy of Occupancy Load Certificate placed in readily visible location from the dining room.

Once you have determined that all these items are completed, we can proceed with scheduling your inspection. Please contact me with any questions.

Yours in Fire Safety,

Wayne C. Jones
Fire Inspector
Raymond Fire Rescue Department
207-894-4046

Business License Application - Moon Enterprises DBA Eclipse



Business License Application

Permit Fee: \$25.00

Application Date: _____

Map-Lot: _____

Zone: _____

Business Name: Moon Enterprises LLC DBA "Eclipse"

Business Location: 1259 Roosevelt Trail

Applicant: Tyler Monahan

Mailing Address: 9 Scott St

City State Zip: Portland, ME 04102

Home Telephone: 207-608-5983 Work Telephone: 207-383-3113

Email Address: tyler@eclipsemaine.com

Description of Business: Medical Cannabis Retail

Owners/Partners Names	Owners/Partners Address	Owners/Partners Phone #s
<u>Tyler Monahan</u>	<u>9 Scott Portland, ME 04102</u>	<u>207-608-5983</u>
Emergency Contact Names	Emergency Phone # 1	Emergency Phone # 2

I have secured or am in the process of securing all State and local licenses/permits required for my business to operate. Please list required licenses/permits:

CGR-27540

Have there been any public health, safety, or welfare problems occurring in the operation of the business or a similar business at the same location in the immediately preceding year, including but not limited to neighborhood complaints, disorderly customers, and excessively loud or unnecessary noise that initiated complaints to or required a response from the sheriff's department fire department or other municipal regulatory body or employee? ☐ Yes ☒ No

If Yes, please provide evidence of satisfactory resolution of any such complaint.

Applicant Signature: Tyler Monahan

Town fees, taxes and inspections, as well as compliant with all Town of Raymond Ordinances.

Code Enforcement Officer _____

Fire Inspector _____

Tax Collector _____

Conditions of Approval by Select Board:

☐ Application Approved

☐ Application Denied. Denial Reason:

Determination Date: _____

Expiration Date: March 1, _____

Select Board Signatures:

Joseph Bruno, Chair

Rolf Olsen, Vice Chair

Teresa Sadak

Samuel Gifford

Derek Ray



OFFICE OF CANNABIS POLICY

DEPARTMENT OF ADMINISTRATIVE AND FINANCIAL SERVICES

Maine Medical Cannabis Program Caregiver Retail Store Local Authorization Form

This Local Authorization Form must be completed by the host municipality where a caregiver registry identification card applicant intends to locate a caregiver retail store. The authorized local official responsible for completing this Form must return it to the Office of Cannabis Policy at Licensing.OCP@maine.gov or 162 State House Station, Augusta, Maine 04333.

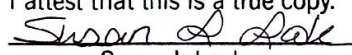
If the authorized local official in receipt of this Form has not recently met with the Office of Cannabis Policy to discuss the local authorization process and OCP's expectations for completion of this Form, please contact the Director of Licensing, at Licensing.OCP@maine.gov or (207) 624-7530, prior to filling it out.

Section 1: Caregiver Information. Information to be completed by the caregiver applicant.			
Section 1(a): Required information for all applicants for caregiver registry identification cards.			
Caregiver's Legal Name Tyler Mamban		Doing Business As Name Eclipse	Primary Phone 207-608-5923
Physical Address of the Proposed Caregiver Retail Store 1259 Roosevelt Trail		City Raymond	State Maine
Caregiver Mailing Address 9 Scott Street		City Portland	State Maine
		Zip 04102	
Section 2: Medical Cannabis Caregiver and Local Authorization Information. This section to be completed by the Municipality in receipt of request for Local Authorization.			
Physical Location of Caregiver Retail Store (include unit number) 1259 Roosevelt Trail		Municipality Raymond	State ME
Tax Map # 55		Zip 04071	
Owner of Record of the Physical Location Listed Above JTM Properties		Tax Lot # 22	
Date Local Authorization Form Presented to the Municipality 10/3/2023		Date Local Authorization Form Approved by Municipality	
Section 3: Local Authorization of Caregiver Retail Store within Municipalities. This section to be completed by the Municipality in receipt of request for approval of Local Authorization.			
Section 3(a): Request for approval of local authorization to operate a registered caregiver retail store in municipality prohibited unless authorized by municipal ordinance or warrant article, or unless in operation with municipal approval prior December 13, 2018. A person operating a medical caregiver retail store within a municipality may not request approval of local authorization to operate the medical caregiver retail store, and a municipality may not accept as complete the person's request for approval of local authorization, unless the municipality permits, by ordinance or warrant article, the operation of registered caregiver retail stores within the municipality, or unless the caregiver retail store was operating with municipal approval in the municipality prior December 13, 2018.			
1. Is an ordinance or warrant article in effect that allows the operation of a registered caregiver retail store within the municipality?			
2. <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No			
3. Is a copy of the ordinance or warrant article attached to this form?			
4. <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No			
5. Was the caregiver retail store operating with municipal approval in the municipality prior to December 13, 2018?			
6. <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No			
Section 3(b): Local authorization required for operation of a registered caregiver retail store within municipality. A person may not to operate a registered caregiver retail store within a municipality unless the following question is answered in the affirmative.			
1. Has the person obtained all applicable municipal approvals, permits, or licenses that are required by the municipality for the operation of a registered caregiver retail store? By selecting "yes" below, the municipality is affirming that no further action by the municipality is required prior to the Office of Cannabis Policy's approval of the applicant's registry identification card. The Office of Cannabis Policy encourages the municipality to coordinate the issuance date of a local license with the Office when appropriate. Please attach a copy of all applicable approvals, permits or licenses, including dates of issuance and expiration to this form.			
2. <input type="checkbox"/> Yes <input type="checkbox"/> No			
Statutory Guidance for Municipalities			
Pursuant to 22 MRS § 2429-D, a municipality may regulate registered caregiver retail stores within that municipality, and may not permit a registered caregiver retail store to operate within that municipality unless the municipal legislative body has voted to adopt or amend an ordinance or warrant article allowing the operation of a registered caregiver retail store within that municipality, or unless that registered caregiver retail store has been continuously operating, as a registered caregiver retail store, by the same caregiver, within that municipality since before December 13, 2018.			
The completed Maine Medical Cannabis Program Caregiver Retail Store Local Authorization Form can be emailed to the Office of Cannabis Policy at Licensing.OCP@maine.gov or sent to Office of Cannabis Policy, 162 State House Station, Augusta, ME 04333-			

0162.	
Municipality	
Legal Name and Title of Authorized Municipal Official:	City:
I hereby affirm and acknowledge that the information above is truthful and complete to the best of my knowledge.	
Signature of Municipal Official: (Do not sign until witnessed by notary):	Date:
Notarization	
The foregoing instrument was acknowledged before me this day of , 20 , at , Maine, by to be the free act and deed of the above named municipal official.	
Name of Notary Public (Printed)	Signature of Notary Public
Notary Public, State of Maine	<p style="text-align: center;">STAMP/SEAL</p>
My commission expires:	

Initials of Signing Municipal Official: _____
OCP_CGR_LAF - Rev. 09/28/2023 - Page 1 of 2

I attest that this is a true copy.


Susan L. Look
Town Clerk of Raymond Maine

Town of Raymond

August 15, 2023

SPECIAL TOWN MEETING MINUTES

TO: Don McClellan, a resident of the Town of Raymond, in the County of Cumberland and State of Maine.

GREETINGS:

In the name of the State of Maine, you are hereby required to notify and warn the inhabitants of the Town of Raymond, qualified by law to vote in Town affairs, to meet at the Broadcast Studio at 423 Webbs Mills Road in said town on Tuesday, August 15, 2023, at 5:30 P.M., then and there to act on Articles 1 through 2 as set out below.

ARTICLE 1: To elect a moderator to preside at said meeting.

Nomination made and seconded for Joe Bruno. Call for nominations to cease.
Voted 3-0

Mr Bruno was sworn in by Town Clerk Look

ARTICLE 2: To see if the Town will authorize medical cannabis retail store locations operating with municipal approval as of December 13, 2018, to operate pursuant to a medical cannabis dispensary registration or a caregiver registration, in compliance with all applicable state and local requirements?

NOTE OF EXPLANATION: *This change in no way allows any sale of recreational use cannabis in the Town of Raymond. It does allow the 2 medical use sites currently grandfathered to operate in Raymond to register with the State of Maine as either a medical caregiver or a medical dispensary.*


The Maine State Statues (Title 22, Chapter 558-C: Maine Medical Use of Cannabis Act) §2422. Definitions include the following:

1-F. Caregiver retail store. "Caregiver retail store" means a store that has attributes generally associated with retail stores, including, but not limited to, a fixed location, a sign, regular business hours, accessibility to the public and sales of goods or services directly to a consumer, and that is used by a registered caregiver to offer cannabis plants or harvested cannabis for sale to qualifying patients.

6. Registered dispensary or dispensary. "Registered dispensary" or "dispensary" means an entity registered under section 2425-A that acquires, possesses, cultivates, manufactures, delivers, transfers, transports, sells, supplies or dispenses cannabis plants or harvested cannabis or related supplies and educational materials to qualifying patients and the caregivers of those patients.

Motion to approve as presented by Mrs Sadak. Seconded by Mr Olsen.
Vote 9-0

Motion to adjourn at 5:35pm by Mrs Sadak. Seconded by Mr Olsen.
Unanimously approved

Respectfully submitted,

Susan L Look, Town Clerk

New Street Name - Sheila's Way

Road Name Approval Application

Applicant/Owner of Road (if private) DAVID + Sheila BAKER
Map 12 Lot 4

Proposed Road Name Sheila's Way

Location (street number at intersection) and Length of Road (left or right off existing road)

Em Lane 124 off RT 85, Driveway is about 1/2
mile long

Reason for Name Building on lot

If this is a private road you will be responsible for maintaining a Road Sign at the intersection of your road and the public way, if the road sign is demolished or stolen it will have to be replaced within 30 days, after notification that the sign must be replaced you shall be liable for a civil penalty of no less than \$10.00 or no more than \$50.00 for each violation.

Signature of Applicant D Baker Date 9/18/23

Office Use Only

Public Safety _____ Code Enforcement/ Addressing Officer _____

Town Planner _____ Assessor _____

Public Works _____

Comments: _____

Selectmen Approval _____

Date _____

MOU Correction - Raymond PFFA IAFF Local 5278

Town of Raymond, Maine

The Raymond Professional Fire Fighters of Maine, IAFF Local 5278

Memorandum of Understanding Amending Article (1) – Recognition Clause

This Memorandum of Understanding [MOU] is entered into by the Town of Raymond, Maine, and the Raymond Professional Fire Fighters Association, IAFF Local 5278.

Background: In September 2023, the full-time employees, included in the Windham-Raymond Professional Fire Fighters Association, IAFF Local 4095's bargaining unit who are employed by the Town of Raymond, petitioned the IAFF to establish their own IAFF Local. To this end, the IAFF approved their request for a standalone IAFF Local and issued them a charter. The Raymond full-time employees are now associated with and represented by the Raymond Professional Fire Fighters Association, IAFF Local 5278.

Purpose: The purpose of this MOU is for the Parties to amend Article 1 of their current Collective Bargaining Agreement (CBA) to change the name of the exclusive bargaining agent from IAFF Local 4095 to IAFF Local 5278 without changing the structure of the current bargaining unit.

Action: The parties agree to amend Article 1 of the current CBA to make the necessary changes to recognize the Raymond Professional Fire Fighters Association, IAFF Local 5278 as the exclusive bargaining agent. To this end, the Parties agree to amend Article 1 of their current agreement to read as follows:

Article 1-Recognition

The Town of Raymond hereby recognizes the Professional Fire Fighters Association, IAFF Local 5278 AFL-CIO-CLC as the sole and exclusive bargaining agent for all Full-time Firefighters/EMS personnel who are public employees as defined by 26 M.R.S.A. §962 (6) excluding the Fire Chief and Assistant Fire Chief.

This MOU is effective upon its execution and will remain in full force and effect unless otherwise agreed to by the parties.

Michael J Crouse, President
PFFA Maine, Representative for
IAFF Local 5278

Date: _____

Susan L Look, Interim Town Manager
Town of Raymond

Date: _____

For the Union [IAFF Local 5278]
Initials _____ Date _____

For the Employer [Town of Raymond]
Initials _____ Date _____

Town of Raymond Maine

Comprehensive Information Technology

Policies, Procedures and Standards

Handbook

Adopted this 10th day of October 2023, by the Raymond Select Board:

Joseph Bruno, Chair

Rolf Olsen, Vice Chair

Teresa Sadak

Samuel Gifford

Derek Ray

Version 2023-10-04 13:13:13

Table of Contents

Introduction	5
1.1 Purpose and Scope.....	5
1.2 Definitions	6
1.3 Revision History	7
2 IT Policies	8
2.1 Acceptable Use Policies.....	8
2.1.1 Appropriate Use of Technology Policy.....	8
2.1.2 Access Control Policy	11
2.1.3 Remote Access Policy.....	13
2.1.4 BYOD Policy.....	15
2.1.5 Password Policy.....	17
2.1.6 Email Policy	18
2.1.7 Social Media Policy.....	20
2.1.8 Compliance Policy.....	21
2.1.9 Fire and Rescue Vehicle Shared Accounts Policy.....	23
2.1.10 Privileged Access Policy.....	24
2.1.11 Approved End User Application Software Policy.....	25
2.2 General Policies.....	26
2.2.1 IT Standards and Procedures Compliance Policy	26
2.2.2 IT Documentation Standards Policy	27
2.2.3 Change Management Policy	28
2.2.4 Business Continuity and Disaster Recovery Policy.....	29
2.2.5 IT Policy Manual Responsibilities	30
2.2.6 GIS Policy.....	31
2.3 Systems Management Policies	32
2.3.1 IT Asset Inventory	32
2.3.2 Hardware Documentation Policy.....	33
2.3.3 Software Documentation Policy	34
2.3.4 Network Monitoring Policy	35
2.3.5 Hardware Monitoring Policy	36
2.3.6 Network Documentation Policy	37
2.3.7 Access Provisioning and Deprovisioning Policy	38
2.3.8 Software Update Policy	39
2.3.9 User Provisioning and Deprovisioning Policy.....	40
2.4 Data Management Policies	41
2.4.1 Data Classification Policy.....	41
2.4.2 Data Retention and Destruction Policy.....	43
2.4.3 Backup and Retention Policy.....	44
2.4.4 Archival Policy	45
2.4.5 Document Management Policy.....	46
2.4.6 Cloud Computing Services Policy.....	47
2.4.7 Customer/Client Data Protection Policy.....	48
2.4.8 Data Labeling and Handling Policy.....	49
2.4.9 Signed Legal Documents Storage Policy.....	50
2.5 IT Policies Affecting HR	51

2.5.1 General Staff Hiring Policy	51
2.5.2 General Staff Termination Policy	52
2.5.3 IT Training Policy	53
2.5.4 General Staff Technology Training Policy	54
2.5.5 IT Procurement Policy	55
2.5.6 Equipment Checkout Policy	56
2.6 Communications Policies	57
2.6.1 Department Email Addresses Policy	57
2.6.2 IPTV Policy	58
2.6.3 IPTV Multimedia Presentation Policy	60
2.6.4 Electronic Signage Policy	63
2.6.5 Public Website Policy	64
2.6.6 Public Social Media Policy	65
2.6.7 Integration with Local FEMA Plans	66
2.6.8 Municipal Meetings Policy	67
2.7 Security Policies	68
2.7.1 Encryption Policy	68
2.7.2 Network Security Policy	69
2.7.3 Vendor Management Policy	70
2.7.4 Teleworking Policy	71
2.7.5 Secure Password Storage Policy	72
2.7.6 Mobile Device Management Policy	73
2.7.7 Vulnerability Management Policy	74
2.7.8 Central Credentials Repository Policy	75
2.7.9 Electronic Signature Policy	76
2.7.10 Remote Vehicle Monitoring Policy	77
2.7.11 Internet Proxy Policy	78
2.7.12 Credit Card Payment Policy	79
2.7.13 Removable Media and Storage Device Usage Policy	80
2.7.14 Vulnerability Disclosure Policy	81
2.7.15 IT Forensics and Legal Investigations Policy	82
2.8 Infrastructure Policies	83
2.8.1 Resilient Network Policy	83
2.8.2 Building Automation Policy	84
2.8.3 VoIP Server Policy	85
2.8.4 E-Mail Server Policy	86
2.8.5 Physical IT Infrastructure Access Control Policy	87
2.8.6 Building Security and Alarm Policy	88
2.8.7 Website Server Policy	89
2.8.8 Intranet Server Policy	90
2.8.9 Video Surveillance Infrastructure Policy	91
3 IT Standards	92
3.1 Open Source Software Standards	92
3.2 IPv6 Adoption Standards	93
3.3 Firewall Standards	94
3.4 Network Infrastructure Standards	95
3.4.1 Wired LAN Standards	95
3.4.2 Wireless LAN Standards	96

3.4.3 WAN Connectivity Standards	97
3.5 Workstation Configuration Standards	98
3.6 Server Standards	99
3.7 Server Room and Data Center Standards	100
3.8 Equipment Racks and Cabinets	101
3.9 Access Control and Authentication Standards	102
3.9.1 Access Control Standards	102
3.9.2 Authentication Standards	103
3.9.3 Network Access Standards	104
3.10 VoIP Infrastructure Standards	105
3.11 Video Surveillance Standards	106
3.12 Cellular Device Standards	107
3.13 Cloud Computing Standards	108
3.14 Database Server Standards	109
3.15 Email Server Standards	110
3.16 Directory Services Standards	111
4 IT Procedures	112
4.1 Asset Management Procedures	112
4.2 Change Management Procedures	113
4.3 Incident Response Procedures	114
4.4 Disaster Recovery Procedures	115
4.5 Backup and Restore Procedures	116
5 IT Security	117
5.1 Acceptable Encryption Standards	117
5.2 Password Security Standards	118
5.3 Access Control Standards	119
5.4 Network Security Standards	120
6 Compliance and Audits	121
6.1 Compliance Requirements	121
6.2 Information Security Audits	122
7 Appendix	123
7.1 Glossary of Terms	123
7.2 References	126
7.3 IT Forms and Templates	128

Introduction

1.1 Purpose and Scope

The purpose of this comprehensive IT policies, procedures and standards manual is to establish standardized guidelines, protocols, and best practices for the management, administration, and security of information technology resources within our municipal government. This manual will serve as the primary reference for all acceptable and prohibited uses of IT assets by municipal employees, contractors, volunteers, and constituents.

This provides a framework that will be used to incrementally migrate, update, and audit existing IT assets, software, technologies, controls and processes to comply with these documented standards over the next 3-5 years. The transition plan will be designed to minimize disruption to operations while bringing infrastructure modernization and maturity improvements that align with organizational objectives. Compliance requirements will be adapted appropriately for legacy systems based on associated risks and lifespans.

This manual applies to all personnel who access or utilize the municipal's IT infrastructure, systems, software, hardware, data, devices, networks and facilities. This includes full-time and part-time staff, contractors, consultants, partners, elected officials, volunteers, and authorized third parties. All users must comply fully and without exception.

This manual aims to:

- Provide clear guidelines and requirements for appropriate use of municipal IT assets
- Standardize IT configurations, processes, controls and methodologies
- Define required security controls and protocols to safeguard information resources
- Outline technology acquisition protocols and life cycle management
- Ensure IT policies and governance align with municipal goals and initiatives
- Reduce risk of disruptions, legal liability, data loss and non-compliance

The scope covers:

- Servers, computers, mobile devices, network infrastructure
- Software platforms, databases, licensing and permit systems
- Websites, cloud services, geospatial systems and applications
- Records, documents and data stored or transmitted electronically
- Internet access, email, telecoms, radios, and peripheral devices
- Physical facilities and infrastructure housing IT equipment

The scope includes all municipal-owned and managed technology, as well as any personal devices authorized for government business. This manual governs resources located on-premises and remotely. All users must comply fully.

1.2 Definitions

To ensure clarity across policies, the following key terms are defined:

Information Technology (IT) - All municipal computer systems, hardware, software, services, infrastructure, and other information processing technologies.

Policy - High level municipal requirements mandating or prohibiting actions to meet municipal government objectives.

Standard - Technical configurations and specifications for systems, software, and devices based on municipal best practices.

Procedure - Instructions outlining steps to complete tasks or processes in line with municipal policies.

Personal Information - Any data related to an individual which could potentially identify them. Examples include name, address, Social Security number, etc.

Confidential Information - Sensitive municipal data accessible only to authorized personnel including citizen records, personnel files, strategic plans, etc.

Third Party - Any external entity such as a vendor, contractor, partner, or other agency that interacts with the municipal government.

Service Account - User account created for a specific software program or service instead of an individual.

Mobile Device - Portable computing equipment such as smartphones, tablets, laptops.

User - Any authorized person including employees, officials, contractors, volunteers who utilize municipal IT resources.

1.3 Revision History

This IT Policies, Standards and Procedures Manual will be updated periodically to account for changes to municipal IT infrastructure, systems, statutory requirements, government processes, and industry best practices.

The Municipal IT Department will review and approve any revisions prior to release of an updated version. The revised manual will be submitted to the municipal governing entity. Upon final approval, the revised manual will be formally communicated and accessible to all municipal employees, contractors, officials, and relevant external entities.

The revision history will document the following for each update:

- Version number (date and time)
- Summary of changes
- Approving department and authority

Historical versions will be archived for reference. The current approved manual will supersede any prior revisions.

All users of municipal IT resources are responsible for adhering to the current version. The Municipal IT Department will maintain the revision history and provide access to archived versions if required.

Version	Changes	Approved By
2023-10-04 13:12:41	Initial draft containing only Introduction and IT Policies sections	

2 IT Policies

Purpose: Establishes required governance policies and guidelines spanning across areas of IT acceptable use, general practices, systems administration, data privacy, security, infrastructure, and communications to direct technology initiatives, inform decision-making, maintain regulatory compliance, and manage risk.

2.1 Acceptable Use Policies

Purpose: Establishes policies and guidelines spanning appropriate usage, access control, passwords, email, social media, compliance, accounts, and other areas to inform municipal workforce technology utilization, protect government systems and data, and meet statutory obligations.

2.1.1 Appropriate Use of Technology Policy

Purpose: Establishes guidelines and requirements for the acceptable and responsible use of municipal government information technology resources including systems, hardware, software, applications, networks, and data. It aims to ensure use of technology aligns with government business needs, complies with laws and policies, protects confidential citizen data, maintains productivity, and prohibits unauthorized activities. This policy applies to all municipal employees, contractors, volunteers, and authorized users granted access to government IT resources.

General Use Requirements:

- General Requirements:
- IT resources are provided exclusively for authorized municipal government business purposes. Any personal use requires department head approval.
- Users must comply with all applicable federal, state and municipal laws, regulations, and policies when using IT resources.
- Users have no reasonable expectation of privacy when using municipal systems or networks, which may be monitored and logged at any time.
- Access to confidential citizen data and municipal records is limited to the minimum necessary to carry out assigned job duties.
- Downloading unauthorized software, applications, files or connecting unauthorized personal devices requires IT approval.
- When working remotely, personnel must maintain the same security controls and usage standards as when on municipal premises.
- Accounts, devices, software, data and outputs generated on municipal IT systems remain municipal government property.
- Resources may not be used to pursue discriminatory, harassing or unethical purposes.
- Violations may result in prosecution, termination of employment/contract, and/or legal prosecution.

Acceptable Use Examples:

- Accessing municipal-provided software, applications, and systems necessary to carry out job duties
- Communicating with colleagues, officials, partners, and citizens regarding municipal matters
- Reviewing work-related websites, online resources, and training materials
- Occasional brief personal browsing, email or chat during breaks in compliance with HR policy
- Downloading work documents to municipal-owned devices assigned to user
- IT support staff performing authorized system maintenance, upgrades and troubleshooting
- Municipal record backup, archiving and authorized data sharing for business needs
- Limited ad-hoc use of external drives for municipal files where scanned and encrypted

Prohibited Use Activities:

- Any illegal activities under local, state, or federal laws
- Accessing, distributing, or storing inappropriate, abusive, or obscene content
- Online gambling, unauthorized business activities, or other unauthorized personal use
- Attempts to circumvent security controls or access systems/data outside of authorization
- Unauthorized vulnerability scanning, hacking, or security testing of municipal systems
- Installing unapproved or pirated software, applications, or media files
- Launching malware, keyloggers, viruses or carrying out other disruptive attacks
- Sending spam, phishing emails, or other unauthorized communications
- Disclosing confidential citizen data or strategic municipal information without approval
- Saving or transmitting sensitive municipal data to personal accounts or unauthorized services
- Unauthorized recording of phone calls, video, or other surveillance within municipal facilities
- Using municipal resources for discrimination, harassment, stalking or other unethical acts
- Excessive personal use that interferes with municipal productivity and operations
- Any other activities deemed inappropriate per municipal policies and standards
- Failing to report known violations, breaches, or suspicious system activities

Compliance:

- Violations of this policy may result in disciplinary action up to and including termination of employment, contract, or access privileges.
- Severe or repeated violations that break local, state or federal laws will be referred for criminal prosecution.
- Department heads and supervisors are responsible for enforcing this policy within their divisions. They must promptly address any violations observed or reported.
- The Municipal IT Department will monitor systems on an ongoing basis to ensure compliance and investigate any suspected violations.
- Annual policy attestation and training is mandatory for all personnel. Access may be suspended until requirements are met.
- Temporary access may be granted to personal devices during a declared emergency to facilitate remote work by critical employees, provided they agree to and follow standard security protocols.

- Any exceptions to this policy must be approved in writing by the Municipal IT Director and Town Manager.

To maintain access privileges, all municipal government workforce members must understand and comply with this policy. Disciplinary procedures will be impartially carried out based on the severity and frequency of violations.

2.1.2 Access Control Policy

Purpose: Institutes requirements and protocols for managing access to municipal government IT infrastructure, systems, applications, databases, and confidential data based on the principles of least privilege and need-to-know. It seeks to grant access to technology resources strictly according to assigned job functions, implement layered access controls, actively monitor access, and promptly revoke access following personnel termination or status changes. This access control policy applies across the municipality's IT environment and to all government workforce members requiring technology access.

Policy Directives:

- All IT systems and applications must implement role-based access control (RBAC) with user privileges restricted based on job functions.
- Access must be granted according to the principle of least privilege, allowing only required user rights.
- Shared or generic user accounts are prohibited. All accounts must be traceable to a single named user.
- Account creation must involve a formal access request process with management approval.
- Upon employee or contractor termination, all access must be revoked immediately.
- Privileged administrator and service accounts must be segregated, closely monitored, and limited to essential personnel.
- Multifactor authentication (MFA) is required for all remote system access and for accounts with elevated privileges.
- Strong passwords, password vaulting, and rapid rotation must be implemented in line with municipal standards.
- Password sharing, improper storage, and circumvention of controls is prohibited.
- Access to confidential citizen data requires additional authorization and audit logging.
- Role-based permissions must be reviewed by system owners at least quarterly and modified appropriately.
- Automatic account lockout after a defined number of incorrect login attempts is required.
- Active monitoring of unauthorized access attempts, privilege escalation, and suspicious insider activities must be performed.

Compliance:

- Department heads and managers are responsible for enforcing access policies within their divisions and ensuring alignment with personnel changes.
- The Municipal IT Department will conduct periodic access reviews and audits to identify any policy violations or unnecessary access.
- Any unauthorized or inappropriate access by personnel will result in escalating disciplinary action up to and including termination based on severity.

- For severe violations that constitute a criminal offense such as data breach or computer misuse, the Municipal IT Department will refer the incident for criminal investigation and prosecution by law enforcement.
- Annual mandatory cybersecurity training will be required covering access control policies, protocols and responsibilities before network access is granted.
- Proof of policy compliance will be required during audits and technology acquisition approvals. Non-compliance may impact funding or result in decommissioning of systems.
- Exceptions to the policy must be submitted in writing and approved by the Municipal IT Director and City Manager with compensating controls documented.

2.1.3 Remote Access Policy

Purpose: Defines secure remote access requirements, protocols, cybersecurity controls and acceptable use standards for municipal government employees, contractors, vendors and third parties connecting remotely to internal networks, systems and other IT resources. It aims to enable remote work while maintaining rigorous protections against unauthorized remote system access.

Policy Requirements:

- The Municipal IT Department must provision secure remote access technologies and capabilities to facilitate remote work by authorized personnel.
- All remote access sessions must utilize multi-factor authentication, including for third parties like contractors and partners.
- Remote access traffic must leverage encryption as specified in municipal security standards, such as VPNs, SSH, SFTP, TLS, etc.
- Access must only be granted on a least privilege basis according to specific job duties and deactivated promptly upon employee termination or status change.
- Personnel must comply with all organizational cybersecurity policies and take reasonable precautions when accessing municipal networks remotely.
- Connecting to municipal networks directly from public systems or unauthorized personal devices is strictly prohibited.
- Activity logs from remote access technologies will be monitored regularly to detect anomalies and potential breaches.
- Personal mobile devices used for remote access must utilize approved security applications and configurations.
- Ad hoc exceptions for emergency remote access from unmanaged systems must be pre-approved in writing by Municipal IT.

Compliance:

- The Municipal IT Department is responsible for providing and maintaining secure remote access technologies, options and support to enable remote work for authorized personnel.
- Department heads and managers must ensure compliance with remote access policies within their divisions. This includes revoking access promptly for employees who are terminated or change roles.
- Employees and contractors are required to report any potential unauthorized or suspicious remote access to municipal networks to the IT Helpdesk immediately.
- Any users found to be in violation of the remote access policy may have their remote access privileges revoked and also face disciplinary action per municipal codes.
- Annual cybersecurity training provided by Municipal IT will include education on proper remote access protocols for personnel. Failure to complete training may result in remote access being denied.
- The Municipal IT Department will regularly audit logs from remote access technologies to identify any potential security risks or policy violations requiring investigation.

- External audits of compliance to remote access policies will be conducted during annual risk assessments. Lack of compliance may impact municipal insurance coverage.

2.1.4 BYOD Policy

Purpose: Establishes mobile device management requirements, security controls, and acceptable use standards for personal devices used to access municipal government emails, data, networks, and other restricted resources. It seeks to enable flexibility of bring your own device (BYOD) access models while safeguarding government systems, maintaining regulatory compliance, and protecting sensitive information.

Policy Requirements:

- Only municipal-approved mobile platforms, operating systems, and applications may be used for BYOD access.
- Personal mobile devices must be encrypted using municipal-standard methods such as BitLocker, FileVault, etc.
- Passwords/passcodes used to unlock devices must meet complexity standards as defined in the Password Policy.
- Municipal data should only be accessed on BYOD devices through approved, official apps provided by the Municipal IT Department. Local storage or copying of municipal data is prohibited.
- Jailbreaking, rooting, disabling security features, or using compromised devices is strictly forbidden for BYOD usage.
- Current anti-malware and anti-virus software must be installed and maintained on devices.
- The Municipal IT Department reserves the right to remotely wipe BYOD devices that become lost, stolen or compromised.
- Users have no reasonable expectation of privacy over any municipal data stored on personal devices. The municipal may monitor and restrict access.
- Users must promptly report any lost or compromised devices with municipal data to the IT helpdesk.
- Non-compliant devices may have their network access revoked until they are in compliance.

Compliance:

- The Municipal IT Department will maintain a list of approved device types, operating systems, and applications for BYOD access. This list will be updated as technology and security needs evolve.
- Users must immediately report any lost or compromised personal devices used for municipal BYOD access to the IT helpdesk. Failure to report may result in disciplinary action.
- The Municipal IT Department reserves the right to remotely wipe lost or compromised BYOD devices to ensure municipal data is secure.
- BYOD devices found to be non-compliant with this policy may have their network access temporarily revoked until compliance is achieved.

- The Municipal IT Department will monitor and regulate access from BYOD devices to ensure adherence to data management laws and policies. Any unauthorized access attempts may be subject to investigation.
- Department heads are responsible for ensuring personnel are aware of and understand this BYOD policy as part of cybersecurity training.
- Violations of this policy may result in disciplinary procedures in accordance with municipal codes.

2.1.5 Password Policy

Purpose: Institutes requirements and standards for the creation, protection, storage, and lifecycle management of passwords, credentials, and multifactor authentication mechanisms used to control access to municipal government IT systems and data. It aims to maintain security by enforcing strong password complexity rules, maximum expiration times, history tracking, secure transmission and storage, and protocols to revoke compromised credentials.

Policy Requirements:

- All IT systems and applications require secure password authentication for access. Anonymous or default logins are prohibited.
- Passwords must meet complexity standards defined by Municipal IT, including minimum length, use of upper/lowercase letters, numbers and special characters.
- Password maximum age must be set requiring users to change passwords regularly, with previous passwords tracked to prevent reuse per Municipal IT guidelines.
- Passwords must not be shared between users or systems for any reason. Vendor-supplied default passwords must be changed immediately.
- Multifactor authentication (MFA) must be implemented wherever available to provide an additional layer of security beyond passwords.
- Privileged administrator, service, and management account passwords require additional controls, rotation frequency, and secure storage/access per Municipal IT standard.
- Plaintext password storage is prohibited. Hashed storage with salting is required where technically feasible.
- Any exceptions for embedded devices/systems with limited password capabilities require Municipal IT approval with compensating controls.

Compliance:

- The Municipal IT Department will provide training and guidance to personnel on strong password hygiene practices and controls.
- Department heads and managers are responsible for overseeing compliance with this password policy within their divisions and teams.
- Any sharing of passwords or use of weak passwords may result in access revocation and/or disciplinary action per municipal codes.
- At least annually, Municipal IT will require password resets across all systems to ensure compliance is maintained.
- Security audits will assess password controls across systems for alignment with this policy. Lack of compliance may impact technology funding or lead to decommissioning of systems.
- Proof of password policy adherence will be required as part of any new system procurement or deployment process.
- Exceptions must be submitted in writing to Municipal IT with compensating control measures for review and approval by the IT Director and Town Manager.

2.1.6 Email Policy

Purpose: Provides appropriate use guidelines, retention rules, and security protocols for the municipal government email system. It seeks to promote proper security, data protection, public records compliance, email hygiene, and productivity for government workforce communications and collaboration. This email policy applies to all municipal employees, contractors, officials and other email account holders.

Policy Requirements:

- Municipal email accounts should only be used for official municipal business communications and not personal purposes.
- Any personal use of municipal email should be incidental, kept to a minimum, and not interfere with employee productivity or operations.
- Users should exercise caution in opening email attachments or clicking links to avoid malware infections. Attachments should be scanned using municipal IT-provided tools when possible.
- Large file attachments should be stored and shared from municipal network drives or cloud storage instead of email when feasible.
- Emails considered municipal records must be retained and archived as required by open records laws and municipal retention schedules.
- Confidential citizen or internal information being transmitted via email must be labeled and encrypted as per data protection standards.
- The Municipal IT Department reserves the right to monitor, filter and access municipal email accounts at any time for security purposes.
- Email accounts may not be used for unlawful discrimination, harassment, or other unethical activities prohibited by municipal policies.

Compliance:

- The Municipal IT Department will provide ongoing training to personnel on proper security, retention and use of municipal email.
- Department heads are responsible for ensuring compliance with the email policy within their divisions through awareness and enforcement.
- Any use of email deemed excessive for personal reasons may result in warnings and access restrictions.
- Violations of records retention by failing to properly archive emails may lead to disciplinary action per municipal codes.
- Confirmed incidents of harassment, discrimination, or unlawful use may also trigger disciplinary procedures.
- The Municipal IT Department will perform monitoring for security purposes and provide tools for retention and discovery of emails as needed for open records requests, legal holds and eDiscovery purposes.

- Annual audits will assess municipal email use practices and technical controls for compliance to regulations and this policy.

2.1.7 Social Media Policy

Purpose: Establishes allowed usage, public communications standards, security protocols, and administration rules for official municipal government social media accounts on approved platforms. It also governs personal social media usage by government employees and officials. This policy aims to enable social media citizen engagement while maintaining information security, protecting the government's reputation, and following ethics/appropriateness standards.

Policy Requirements:

- Official municipal social media accounts must be approved, created and managed by designated staff from the Municipal Communications Department.
- Content published on official municipal social media must maintain a professional tone, follow branding standards, and protect confidential citizen data or records.
- Personal social media accounts of municipal employees should not claim to officially represent the municipal government without authorization.
- Excessive use of personal social media during municipal work hours that interferes with duties is prohibited.
- Social media, whether official municipal accounts or employees' personal accounts, may not be used to harass, discriminate, or threaten others, or otherwise violate laws/policies.
- Personnel are prohibited from sharing copyrighted or proprietary municipal information on unauthorized social media channels.
- Job postings and recruitment must utilize approved official social media accounts and go through the HR Department.

Compliance:

- The Municipal Communications Department is responsible for overseeing, monitoring and maintaining all official social media accounts representing the municipal government.
- Department heads and managers must ensure personnel are aware of and comply with social media policies, and avoid excessive personal use during work time.
- Violations of the policy, such as harassment online or sharing confidential information, may result in disciplinary procedures as per municipal codes up to termination.
- The HR Department will investigate any complaints related to employee social media misconduct and refer criminal matters to the appropriate authorities.
- Municipal IT can monitor social media traffic on municipal networks and systems and restrict unauthorized platforms if needed.
- Annual social media policy training will be required for all employees to support policy awareness and compliance.

2.1.8 Compliance Policy

Purpose: Mandates that municipal government information technology systems, infrastructure, controls, data collection and usage practices comply with all required federal and state of Maine laws, regulations, and statutes covering areas such as accessibility, public records, surveillance, cybersecurity, telecommunications, procurement, information handling, and data privacy. This policy seeks to ensure ongoing governance, management and operations of IT adhere to the complex and evolving regulatory compliance landscape.

Required Compliance Areas:

- Data Privacy and Security - Laws related to confidentiality, privacy, and security of sensitive data, including HIPAA, FERPA, GLBA, and breach notification laws.
- Surveillance and Wiretapping - Laws governing electronic monitoring, recording, and surveillance such as wiretap statutes.
- Public Records and Transparency - Laws providing public access to municipal records and information.
- Accessibility - Regulations requiring accessible design of electronic information and services, including Americans with Disabilities Act.
- Information Handling - Laws covering information reproduction, copyright, trademarks, and licensing.
- Telecommunications - Regulations around telecom services, communications, and infrastructure.
- Cybersecurity - Laws and regulations addressing cybersecurity practices for government agencies.
- Procurement - Regulations related to fair and open software/hardware procurement and licensing.
- Family Educational Rights and Privacy Act (FERPA) - student education record privacy
- Health Insurance Portability and Accountability Act (HIPAA) - healthcare information security and privacy
- Fair Credit Reporting Act (FCRA) - governs background check information
- Maine Notice of Risk to Personal Data Act - requires breach notification
- Maine Criminal History Record Information Act - regulates criminal records access
- Maine Insurance Information and Privacy Protection Act - governs confidentiality of insurance records
- Maine Public Records Law - provides public access to municipal records
- Maine Uniform Information Practices Act - privacy protections for public records
- Maine Archives and Records Management Law - records retention and disposition
- Federal Communications Commission (FCC) - telecoms regulation and accessibility
- U.S. Copyright Act - governs software licensing and information reproduction

Responsibilities:

- IT Leadership must keep abreast of current and emerging regulations impacting municipal IT.
- IT Security must ensure compliant safeguarding and handling of protected data.
- All personnel must comply with required laws and regulations when utilizing municipal IT resources and systems.

2.1.9 Fire and Rescue Vehicle Shared Accounts Policy

Purpose: Permits the controlled usage of shared generic accounts on fire, EMS and other emergency response vehicle mobile data terminals (MDTs) to provide required multi-user access to dispatch data, hazmat databases, building preplans, patient information and other systems necessary for crisis response. This policy aims to balance practical operational needs during incidents with appropriate access controls and auditing.

Applicability:

This applies to all shared accounts configured on MDTs installed in fire trucks, ambulances, battalion chief vehicles and other emergency response units with a legitimate need to access data from multiple users.

Policy Statements:

- Shared generic accounts may be configured on MDTs where use of individual user accounts is impractical.
- Shared accounts should only grant access to IT systems, applications, and datasets required for the specific vehicle type and emergency function.
- Shared vehicle MDT accounts are exempt from password expiration policies but must have complex passwords changed at least annually.
- MDT access privileges should be limited to authenticated emergency vehicles through firewall rules except for required public safety broadcasts.
- All MDT connection logs and shared account usage must be recorded and regularly audited to identify any unauthorized access.
- Any personnel misuse, abuse or unauthorized access of shared MDT accounts constitutes a policy violation subject to disciplinary action.

Compliance:

- The IT department is responsible for configuring secure shared accounts on MDTs according to the principle of least privilege.
- Fire and rescue leadership must ensure personnel understand appropriate MDT account usage and prohibitions on misuse.

2.1.10 Privileged Access Policy

Purpose: Institutes controls, restrictions, reviews, and monitoring mechanisms for privileged administrator, service, and management accounts across municipal government IT systems. It seeks to limit standing highly privileged access only to essential personnel, enforce multifactor authentication, closely track activity, regularly rotate shared passwords, and block standard users from privilege escalation.

Scope:

This policy applies to all IT staff, contractors, vendors or third parties who access the organization's systems using accounts with administrator privileges.

Policy Statements:

- Privileged accounts must only be granted to authorized IT staff members with a legitimate business need for elevated access to maintain and support systems.
- Multi-factor authentication (MFA) using a one-time-password (OTP) token or biometric method is required for all privileged account access.
- Privileged access sessions must utilize dedicated privileged access workstations isolated from the corporate network or laptops with hard disk encryption.
- Just-in-time dynamic privileged credentials should be used where technically feasible instead of standing static accounts.
- All privileged access usage must be logged and monitored to detect anomalies and abuse.
- Credentials for privileged accounts must be securely stored in an encrypted password vault or manager with access strictly limited based on roles.
- Privileged accounts should be periodically audited and validated at least quarterly to ensure proper management.
- Shared privileged accounts are prohibited whenever possible. If required, usage must be tightly restricted and tracked to individual users.

Enforcement:

- Any misuse, unauthorized access, or policy violations related to privileged accounts may lead to disciplinary measures up to termination.

2.1.11 Approved End User Application Software Policy

Purpose: This policy establishes the approved applications and software available for installation and use on municipal government end user workstations and devices. It aims to maintain standard configurations, efficient support, licensing compliance and security.

Scope: This policy applies to all municipal employees, contractors, officials and other end users issued computers, laptops, smartphones or tablets by the government entity. It allows installation of software applications from both the standard suite and an approved catalog.

Policy Statements:

- All workstations will have a standard suite of productivity software installed by IT including operating system, web browser, email client, office suite, PDF reader and security tools.
- An approved software catalog maintained by IT lists additional applications available for on-demand installation by end users for purposes aligned with municipal business needs.
- End users may submit requests for additions to the approved catalog, which will be evaluated based on need, licensing, costs and security considerations.
- Applications not included in the standard suite or approved catalog are prohibited from use on municipal devices without explicit authorization by IT.
- Software metering and auditing tools will monitor for any unauthorized applications resulting in access restrictions until unapproved installations are removed.
- Application whitelisting restrictions will be implemented where feasible to only allow installation and execution of approved software titles.
- Shareware, adware, trial versions and outdated unsupported applications are expressly prohibited without approval.
- Licensed commercial business applications take priority over unlicensed free/open source alternatives with vendor support availability preferred when possible.

Compliance:

- IT is responsible for managing the standard suite and approved application catalog available to end users based on requests.
- End users must not download or install unapproved applications without permission or attempt to circumvent restrictions.
- Violations may result in removal of software, access revocation and/or disciplinary action.

2.2 General Policies

Purpose: Defines cross-functional municipal government information technology policies covering standards/procedures compliance, documentation, planning, risk management, and geographic information systems to institute consistent governance.

2.2.1 IT Standards and Procedures Compliance Policy

Purpose: Establishes a requirement for municipal government IT teams and users to fully comply with documented IT standards and procedures in order to maintain consistency, enhance security, improve efficiency and promote stability across the technology environment. It requires submitting formal risk-based exceptions for any deviations from mandated configurations, processes or protocols.

Scope:

This policy covers all IT infrastructure, systems, software, services, platforms, and data usage throughout the organization as documented in Sections 3 through 6 of the IT Policy and Procedures Manual. It applies to any internal or external teams, vendors, contractors and third parties that manage, access or support the organization's technology.

Policy Statements:

- All hardware and software must be configured according to the organization's documented architecture and product standards outlined in Section 3.
- Any variance from approved configurations or architectures requires a formal waiver process including risk analysis and approval from IT leadership.
- All defined procedures for system availability, change management, incident response, audits and maintenance in Sections 4 through 6 must be followed.
- Non-compliance with procedures requires management approval along with risk acknowledgement and mitigation plans.
- IT vendors, contractors and partners must agree to comply with applicable standards and procedures.
- Routine internal audits will measure compliance levels across infrastructure against standards and procedures.
- Lack of compliance may result in project delays or cancellations, withholding of funding, or removal of unauthorized systems.
- Compliance reports will be reviewed by IT leadership on a quarterly basis.

2.2.2 IT Documentation Standards Policy

Purpose: Mandates comprehensive documentation and maintaining up-to-date records covering municipal government IT infrastructure, systems, software, policies, processes, procedures, configurations and architecture diagrams. It seeks to preserve institutional knowledge, enable troubleshooting, speed incident response, facilitate audits, and support disaster recovery scenarios and new/temporary employee onboarding through availability of accurate IT documentation.

Policy Statements:

- All IT systems, hardware, software, configurations, processes and procedures must be thoroughly documented.
- Documentation must be kept updated as changes occur and reviewed annually.
- Documentation should be stored in a centralized repository with access controlled based on job roles.
- Operating procedures should be developed for critical IT processes.
- Information security policies and controls must be documented for regulatory compliance.
- Physical topology diagrams are required for network infrastructure.
- Logical network diagrams must be maintained for critical systems.
- Data flow and application architecture diagrams should illustrate system interactions.
- Vendor-supplied documentation should be maintained for all purchased hardware/software.
- Project documentation and technical specifications are required for development efforts.
- Disaster recovery plans must document processes to restore critical systems and data.

2.2.3 Change Management Policy

Purpose: Institutes a structured and controlled IT change management process for modifications to municipal government systems, networks, databases, hardware, software and data center facilities. It aims to reduce business disruptions, maintain IT stability, systematically implement needed technology upgrades and enhancements, provide oversight and meet user community needs through standardized submission, review, approval, scheduling, testing, implementation and post-change validation procedures.

Policy Statements:

- All changes to IT systems must follow defined change management procedures. This includes software, hardware, network, and data center infrastructure.
- A change management process with associated tools should be established to track requests, approvals, scheduling, testing, implementation and verification of changes.
- Change requests must describe the change, justification, implementation plan, rollback plan, and expected impact.
- A change advisory board of stakeholders should review and approve/deny high risk or impactful change requests.
- Changes should be scheduled during approved change windows and adhere to established freeze periods.
- Proper communication of approved changes and maintenance windows must be made to impacted users/groups.
- Testing and staging environments should be provisioned to adequately test changes prior to production implementation.
- All application, system, network and device configuration changes must be tracked and documented in a central change repository.
- Implemented changes must be reviewed post-deployment to confirm proper functioning and stability.

2.2.4 Business Continuity and Disaster Recovery Policy

Purpose: Requires regular development, reviewing, testing and updating of business continuity and disaster recovery plans to restore essential municipal government IT operations and systems following minor disruptions, major outages or catastrophic events. It seeks to mitigate business disruption and data loss risks while maintaining continuity of government operations and services during a crisis.

Policy Statements:

- The organization must develop and maintain business continuity and disaster recovery plans to restore critical operations in the event of a outage or catastrophe.
- A business impact analysis must be conducted to identify critical systems, acceptable downtime, and recovery priorities.
- Recovery time objectives (RTOs) should be defined for essential systems and processes.
- Plans should delineate procedures for failover to alternate facilities or cloud infrastructure when warranted by the severity of an incident.
- Regular DR testing and exercises should be conducted to validate recovery capabilities, identifying gaps.
- Continuity and DR responsibilities should be defined for IT teams, departments and vendors.
- Critical equipment must have redundancies and fault-tolerant configurations.
- Offsite backups must be maintained with ability to restore essential data quickly.
- Succession planning should ensure qualified personnel are ready to manage continuity events.
- Emergency communications protocols are required to keep staff, customers, and stakeholders informed.

2.2.5 IT Policy Manual Responsibilities

Purpose: Defines clear accountability and requirements for routine maintenance, periodic reviews and updates, and version controls of the comprehensive municipal government IT policy manual between the government entity and any contracted IT services provider. It aims to keep this foundational IT governance and compliance document current based on evolving technologies, statutory obligations, risks, audits, and organization learning.

Policy Statements:

- When IT services are contracted, the municipal department responsible for oversight must designate an employee to be accountable for the manual.
- The responsible municipal employee will coordinate policy review and updates with the contracted IT service provider.
- The contracted IT Director holds overall accountability for routine maintenance and updates of the manual.
- Proposed policy changes must be reviewed and approved by both municipal and provider IT leadership.
- Municipal legal/compliance review should occur for policy updates when deemed necessary.
- Policy reviews and updates should occur annually at minimum.
- A policy change log must be maintained tracking updates.
- Updated manual must be accessible to both municipal and provider staff.

2.2.6 GIS Policy

Purpose: Outlines allowable usage, accuracy, data sensitivities, access controls and security obligations related to municipal government geographic information systems (GIS), geospatial data, digital maps, and location intelligence platforms. It aims to balance open government data publication, citizen privacy rights, supporting day-to-day operations, enabling strategic decisions based on location data while meeting regulatory compliance mandates.

Policy Statements:

- All GIS data utilized by municipal departments must be properly classified according to sensitivity and made accessible to personnel based on least privilege principles.
- GIS systems acquisition, usage, data accuracy, and data imports must comply with relevant state and federal regulations.
- A centralized enterprise GIS platform should be maintained as the authoritative repository with controlled access, monitoring, backups, disaster recovery, and cybersecurity controls.
- GIS datasets deemed confidential must have additional access restrictions and utilize encryption both at rest and in transit.
- A designated municipal GIS data steward will be responsible for administering the central platform, ensuring proper data classification, providing access, maintaining data quality and integrity, enforcing information security, and ensuring compliance.
- Any external sharing or distribution of GIS data must be approved by the data steward based on classification.
- GIS systems and data stores will be included in enterprise IT risk assessments, vulnerability scanning and penetration testing activities.
- GIS documentation will include up-to-date architectural diagrams, data models, schemas, flows, interfaces and inventories.

2.3 Systems Management Policies

Purpose: Outlines policies related to administering municipal government technology infrastructure including asset inventory, system documentation, monitoring, provisioning/deprovisioning, maintenance, and security update processes to optimize lifecycle management.

2.3.1 IT Asset Inventory

Purpose: This policy mandates maintaining a frequently updated, accurate and comprehensive centralized inventory of all municipal government information technology hardware and software assets. It seeks to support IT lifecycle management, security, acquisitions planning, budgeting, safeguarding of equipment, compliance, and technology decision-making through maintaining detailed inventory records and tracking of IT assets.

Policy Statements:

- Centralized inventory of all IT hardware and software must be maintained with assignment details, criticality, end of life/support status, and configuration specifications.
- Asset inventory must be validated annually at minimum through discovery scanning, manual audits and department input.
- Inventory records must track purchase date, cost, licensing, warranty/support status, approved uses, and end of life estimates.
- Asset inventory should integrate with procurement, change management and provisioning systems where feasible.
- Unique municipal asset tags must be assigned and remain affixed to inventoried equipment.
- Changes in asset status must trigger inventory updates in near real-time or via daily scheduled synchronizations.

2.3.2 Hardware Documentation Policy

Purpose: Requires thoroughly documenting all municipal government IT infrastructure devices, components, configurations, topology schematics, infrastructure interconnections, cabling, network addresses, console/management interfaces, and other technical specifications. It aims to create a complete reference source to enable incident troubleshooting, disaster recovery, forensic investigations, internal audits and effective infrastructure management.

Policy Statements:

- Detailed network topology diagrams must document all hardware interconnectivity, cabling, traffic routing and flows between network devices.
- Standards should outline required fields and conventions for inventory spreadsheets, asset management system data, and asset tag label formats.
- Photographic and/or video documentation should catalog physical hardware installations, cabling and device interfaces.
- Network addresses, configuration files, and equipment settings must be documented for disaster recovery purposes.
- Asset documentation should note space, power, and cooling requirements for equipment.
- Maintenance schedules and life cycle replacement timelines should guide proactive asset lifecycle management.
- Documentation process should detail required information to collect for new hardware deployment vs ongoing change maintenance.
- Process and automation should enable linking inventory systems with procurement records and shipment tracking.
- Rollback documentation is required when replacing or decommissioning hardware detailing return to previous state.

2.3.3 Software Documentation Policy

Purpose: Mandates comprehensive documentation of all municipal government-installed software titles, versions, licensing details, configurations, customizations, systems integrations, workflows, data flows, networking, accessible interfaces, privileges, vulnerabilities and operating procedures. It seeks to maintain software inventory, licensing, inform business continuity planning, comply with intellectual property restrictions, enable audits, and support new user training.

Policy Statements:

- Centralized records must be maintained of all software titles, versions, license details (terms, usage rights), renewal/maintenance dates, and proof of purchase.
- Documentation must cover the extent of software installations, customizations, configurations, integrations between systems, and operating procedures.
- All source code repositories, scripts, databases, configuration files, schemas, and API documentation must be kept current.
- Software change management logs must capture version history, updates, bug fixes, patches, and feature additions applied over time.
- Data flow and application architecture diagrams must outline relationships and interfaces between software systems, applications, databases, operating systems, and dependencies.
- Standard operating procedures must provide usage instructions for municipal personnel to follow for critical software programs.
- Software user manuals, technical specifications, training materials, administrator guides must be maintained.
- Compliance with software terms of service, licenses, copyrights and intellectual property must be ensured.
- Vulnerabilities, flaws, or unpatched versions identified in software applications must be documented, risk assessed, and updated.

2.3.4 Network Monitoring Policy

Purpose: Requires continuous proactive automated monitoring of municipal government networks for performance metrics, utilization patterns, availability, latency, errors and other key indicators. It aims to facilitate rapid problem identification, dynamic capacity planning, security analytics, and baseline trend analysis.

Policy Statements:

- Continuous network monitoring must include bandwidth utilization, latency, uptime and key performance metrics based on technology.
- Threshold-based alerts must notify IT staff of issues such as outages, congestion and abnormal traffic patterns.
- Troubleshooting mechanisms must allow network traffic analysis and tools to identify root cause.
- Monitoring systems must retain historical network operations data and generate reports on availability, utilization and health metrics.

2.3.5 Hardware Monitoring Policy

Purpose: Mandates continuous automated monitoring of essential municipal government IT infrastructure components and devices for availability, utilization, performance, errors, and other key health/telemetry data points based on technology type. It seeks to detect problems proactively, identify inadequate capacity, improve preventive maintenance, provide outage alerting, and collect data to improve future infrastructure designs.

Policy Statements:

- Systems must be instrumented to monitor availability, utilization and health data points relevant to each hardware device/platform.
- Monitoring must alert on conditions indicative of failure or degraded performance for proactive maintenance.
- Threshold-based alerts should notify support staff of issues like storage capacity, RAM exhaustion, I/O bottlenecks.
- Data from hardware monitoring allows analysis of growth patterns and informs capacity planning.

2.3.6 Network Documentation Policy

Purpose: Maintains updated diagrams, topology mappings, data flows, configurations, addressing schemas, credentials rosters, cabling schematics, and inventory listings fully documenting municipal government network components, logical connectivity and physical relationships. It aims to support incident response, troubleshooting, disaster recovery, infrastructure changes, technology upgrades and day-to-day administration by keeping accurate network documentation accessible only to authorized IT staff.

Policy Statements:

- Documentation must be maintained covering overall network architecture, data flows, topology and components.
- Network diagrams must outline LANs, WANs, subnets, VLANs, routing schemes, and traffic flows between networks.
- Detailed diagrams are required for critical infrastructure and key systems and services.
- An inventory of all networking equipment must be kept current including makes, models, configurations, IPs, and purpose.
- Schema documentation should define network addressing, DHCP scopes, NAT setups, WiFi networks, and VPN configurations.
- Network credentials, passwords, infrastructure cabling and telecom circuits must remain securely stored.
- Changes to networks must trigger documentation updates along with diagrams of before and after states.
- Network documentation must remain accessible to authorized IT staff in electronic repositories with role-based access controls.
- Physical copies of network documentation must have limited distribution and be marked confidential.

2.3.7 Access Provisioning and Deprovisioning Policy

Purpose: Standardizes and controls processes for timely requesting, reviewing, approving, fulfilling and revoking user access to municipal government information technology resources. It seeks to appropriately provision and deprovision access based on assigned job duties, need and principles of least privilege. This policy aims to integrate provisioning workflows with human resources systems and offboarding processes, effectively monitor access changes, and prevent unauthorized access especially following personnel departures.

Policy Statements:

- Formal user access request and approval workflows must be followed for granting access to IT systems and data.
- Access should be granted based on job role utilizing the principle of least privilege.
- A centralized identity and access management system should be used to fulfill access requests where possible.
- Access to confidential data requires additional approval by data owners.
- Access for third parties like vendors must be limited to required systems through time-bound accounts.
- Upon employee, contractor or third party termination or transfer, all access must be deactivated within 24 hours.
- Manager attestation should be required confirming deprovisioning after offboarding.
- Periodic access reviews by system owners must validate proper entitlements are assigned.
- Provisioning and deprovisioning activity should be monitored to detect delays or violations.

2.3.8 Software Update Policy

Purpose: Requires keeping software on all municipal government systems maintained at current versions and promptly patched with relevant fixes to mitigate vulnerabilities, align to vendor support levels, resolve platform bugs/defects, and take advantage of improved capabilities, performance, compatibility, and security features. It aims to optimize system stability, interoperability, compliance and security through up-to-date software while minimizing business disruptions from testing/deploying updates.

Policy Statements:

- Software on all municipal systems must be kept up-to-date with the latest security patches, updates, and versions supported by vendors.
- Automated patch management solutions should be deployed where possible for operating systems and software applications.
- Risk-based prioritization should determine installation order and deadlines for critical versus lower-risk updates.
- Change management procedures will govern process for testing and installing updates.
- Impacted departments and personnel must receive timely notification of pending updates and maintenance windows.
- Workstations, laptops, and mobile devices connecting remotely must maintain current endpoint security.

2.3.9 User Provisioning and Deprovisioning Policy

Purpose: Mandates that all municipal government employee, contractor and third party user account provisioning and deprovisioning strictly follow established protocols for access requests, reviews, approvals, fulfillment and revocation. It seeks to automate fulfillment and removal of access where feasible, integrate with HR systems, prevent standing excessive access especially after terminations, and routinely verify correct entitlements to computing resources.

Policy Statements:

- Formal request and approval workflows must be followed for granting new user accounts or modifying access to IT resources.
- Access should be granted based on assigned job duties and the principle of least privilege.
- Access to confidential information requires additional justification and manager approval.
- Upon employee termination or transfer, all access must be revoked within 24 hours.
- Manager attestation should be required to confirm deprovisioning.
- Access must be reviewed quarterly to ensure entitlements remain appropriate for each user's current role.
- Provisioning and deprovisioning activity should be logged and monitored to detect delays.
- Shared accounts are prohibited whenever possible. If created, usage must be strictly audited.
- Role-based permissions should be utilized rather than assigning access individually.

2.4 Data Management Policies

Purpose: Specifies policies around classifying data, establishing retention rules, securing backups, archiving historical records, utilizing document management systems, assessing third-party services, and protecting customer information to comply with legal obligations and protect sensitive data.

2.4.1 Data Classification Policy

Purpose: Requires classification of all municipal government information into defined sensitivity tiers based on data contents, level of risk if compromised, and required protection levels. It aims to determine approved location storage locations, access permissions, encryption requirements, retention rules, handling procedures and protection controls based on how the data is classified. Proper classification is foundational for compliant data management according to content and risk.

Policy Statements:

- All municipal electronic data must be categorized into defined classification levels based on the sensitivity and criticality of the data.
- Specific handling rules, usage permissions, storage locations, transmission methods, retention periods, and protection controls will be defined for each classification level per municipal standards.
- Data owners are responsible for appropriately classifying data resources under their management based on the risk assessment of the data.
- Data must be clearly labeled according to its classification where possible, such as marking file share directories or database columns.
- Sharing municipal data with external third parties requires verifying the recipient's clearance level and authority to receive the classification of data being shared.
- Unclassified data should be labeled and protected at a minimum level according to Municipal IT guidance.

Compliance:

- The Municipal IT Department will provide training and guidance to personnel on proper data classification and handling according to the municipal's standards.
- Department heads are accountable for enforcing the data classification policy and ensuring data under their purview is properly categorized and protected.
- Any unauthorized access, sharing or mishandling of confidential municipal data by personnel may result in disciplinary action per municipal codes.
- The Municipal IT Department will conduct periodic audits to identify any improper classification or unsecured confidential data requiring remediation.
- Annual policy attestation will be required by all employees to promote awareness and compliance. Failure to complete attestation may result in system access revocation.

- Policy adherence will be monitored as part of any new system procurement, development or data sharing initiative. Lack of compliance may impact budgetary approvals.

2.4.2 Data Retention and Destruction Policy

Purpose: Defines consistent data retention schedules and secure destruction methods to comply with municipal government records requirements, minimize unnecessary storage costs, and prevent unauthorized access or retrieval from decommissioned equipment and media. It aims to maintain information availability for required retention duration while permanently purging data no longer needing preservation based on classification.

Policy Statements:

- Formal data retention schedules must be defined and followed consistently across systems and storage locations.
- Minimum and maximum retention periods should comply with all legal, regulatory, audit and business retention requirements.
- Data stewards should work with legal/compliance to update retention schedules as requirements change.
- Data destruction procedures must be environmentally responsible and render data unrecoverable.
- Retention tags or classification metadata should identify retention periods within systems.
- System and backup purging processes must adhere to defined retention periods.
- Registered documents set for destruction should follow secure digital shredding techniques.
- Physical documents must be crosscut shredded, pulped, burned or chemically destroyed when no longer retained.
- Certificates of destruction should be obtained from vendors disposing of retired physical media and paper records.

2.4.3 Backup and Retention Policy

Purpose: Outlines municipal government backup frequency, retention duration, restoration testing procedures, offsite physical storage security, and data recovery objectives based on resource criticality and acceptable downtime. It seeks to provide properly secured backups/retention enabling complete data restoration and system recovery within defined time frames to support business continuity at optimized storage costs.

Policy Statements:

- Backup schedules, retention, and media must adhere to State of Maine statutes including:
- Title 10, §945 - Requiring regular backup of business electronic records
- Title 5, §131 - Continuing duty to keep records through required retention periods
- Frequency of backups, rotation schedules, retention periods and offsite storage must align to recovery objectives defined in the disaster recovery plan.
- Strict chain of custody, access controls, and physical security must be maintained for offsite backup media as per Title 5, §131.
- Annual documented restoration testing from backups must validate ability to meet recovery time objectives, as per Title 5, §131.
- Encryption meeting Maine statute Title 10, §1350-E must be applied to any backups containing confidential or sensitive information.
- Maximum allowable backup cycles must account for medium life expectancy and data degradation over defined retention timeframes.
- Secure destruction procedures for expired backups must render data non-recoverable while maintaining confidentiality obligations.
- Robust inventory tracking, logging, and reporting must account for all backup media locations through destruction.
- Documented backup administration processes must delineate assigned roles, responsibilities and controls.

2.4.4 Archival Policy

Purpose: Establishes procedures, handling protocols, security controls, integrity verification processes and environmental requirements for the long-term storage, preservation, and accessibility of historical municipal government records deemed to have enduring legal, administrative, fiscal or historical value. It aims for proper identification, retention and protection of permanent records over decades.

Scope: This policy covers the archival of paper documents, physical media, electronic records, and digital data designated for permanent retention per municipal records retention schedules.

Policy Statements:

- The Municipal Clerk's office shall maintain and enforce a master records retention schedule defining archival designations and periods.
- Paper documents shall be inventoried, packaged and transferred to the secure municipal archives facility using proper handling procedures to avoid damage or loss.
- Physical media such as recordings and photographic materials shall be professionally archived to prevent deterioration.
- Digital records designated for archival shall have verified backups created and transferred to highly secure archival systems maintained by IT.
- Archived information must remain fully accessible to authorized requestors as per freedom of access laws.
- Environmental conditions shall be maintained within target thresholds to prevent deterioration.
- Digital archives shall be periodically verified for integrity and migrated to current formats and media before systems are retired or upgraded.
- Archived records may only be disposed of after defined retention periods with proper approval per policy.

2.4.5 Document Management Policy

Purpose: Requires mandatory utilization of the centralized electronic document management system for properly classifying, indexing, storing, retaining, and enabling discovery of official municipal government documents based on defined metadata standards, taxonomies, access controls, and content lifecycles. It aims to preserve documents in appropriate repositories, automate retention, consistently apply access restrictions, and facilitate eDiscovery.

Scope: This policy covers all official final versions of municipal documents including policies, reports, meeting minutes, project files, departmental records, forms, and any other documents requiring retention. It applies to all municipal employees, contractors and system users.

Policy Statements:

- All final official versions of municipal documents must be stored in the document management system with appropriate metadata attached for classification and searchability.
- Naming conventions, folder structures and retention rules must be consistently followed organization-wide.
- Access controls will be implemented to restrict confidential documents only to authorized personnel based on role.
- The current official version of documents must be clearly identified if multiple revisions exist. Outdated versions should be moved to archive folders.
- Documents must be retained within the system to meet municipal records retention requirements, allowing for legal holds.
- Regular backups of the document repository must occur to safeguard from data loss.
- Prior to any system migration or decommissioning, all files and metadata must be successfully migrated to a new platform.
- The IT department is responsible for system administration, access controls, and managing backups and migrations.

2.4.6 Cloud Computing Services Policy

Purpose: Outlines assessment, risk evaluation, and security control responsibilities when adopting cloud computing models, platforms and services to process or store municipal government data based on sensitivity levels. It aims to enable prudent cloud adoption to achieve benefits like scalability, resilience and efficiency while maintaining oversight, managing risks, and protecting sensitive information stored externally.

Policy Statements:

- Use of cloud computing services must go through an approval process based on data sensitivity and security requirements.
- Contract terms must give the organization sufficient control over data and termination rights.
- Vendor risk assessments are required to validate security posture, resiliency and compliance controls.
- Data classification must dictate allowable cloud deployment models: IaaS, PaaS, SaaS.
- Sensitive data usage in cloud environments requires encryption both at rest and in transit.
- Ongoing security monitoring of cloud resources must be performed for breach detection.
- Incident response plans must cover data breaches or outages involving cloud services.
- Business continuity and disaster recovery plans must incorporate cloud-based systems.
- Access controls for cloud services must align with internal identity management policies.
- Cloud administrators must adhere to privileged access management policies.

2.4.7 Customer/Client Data Protection Policy

Purpose: Establishes standards and controls for properly classifying, limiting access, encrypting and safeguarding any customer or client data stored and processed within municipal government systems to maintain information security. It seeks to ensure compliance with privacy regulations, prevent unauthorized exposure, demonstrate due care, uphold public trust and maintain strict data stewardship even when external parties entrust the government with information.

Policy Statements:

- All customer or client data stored or processed by the organization must be properly classified and protected.
- Data classification should dictate approved storage locations, access controls, encryption requirements, retention and disposal methods.
- Access to customer data must be limited to personnel who require it for authorized business purposes only.
- Sharing data externally must be approved by legal and information security teams.
- Strong encryption (256-bit AES minimum) must be applied to customer data both at rest and in transit over networks.
- Breaches involving customer or client data must be reported to leadership within 1 hour of detection.
- Data protection requirements must be formally defined in vendor contracts.
- Consent procedures must govern use of data for secondary purposes like analytics or marketing.
- Customers should have accessible methods to update preferences and restrict data usage.
- Ongoing audits will validate proper policy compliance related to customer information safeguards.

2.4.8 Data Labeling and Handling Policy

Purpose: Requires properly labeling municipal government information to clearly indicate sensitivity level on reports, dashboards, databases, and displays containing restricted or confidential data. It further mandates adhering to defined handling procedures and protections based on the associated label such as encryption, storage, transmission, destruction and personnel access controls. This policy aims to prevent improper exposure or modification of sensitive information through compliant use of classification labels.

Policy Statements:

- All municipal data must be categorized and labeled according to the defined classification system.
- Labels should clearly identify sensitivity level on reports, files, database columns and screens displaying data.
- Handling procedures for access, storage, transmission and disposal must adhere to the controls required for each classification tier.
- Personnel must protect labeled data commensurate with classification scheme requirements.
- Confidential data at rest must require strong encryption. Confidential data in motion must require secure transmission protocols.
- Only authorized users should have access to restricted or confidential data based on job duties.
- External sharing of restricted information must follow published protocols.
- Confidential labeled data must maintain metadata identifying owners, custodians and approved usages.
- Regular assessments will audit data handling practices for compliance with labeling and controls.

2.4.9 Signed Legal Documents Storage Policy

Purpose: Dictates secure centralized storage locations, defined backup procedures, version controls, access protocols, decryption capabilities and retention rules for signed legal agreements, contracts and other official documents executed on behalf of and binding the municipal government. It aims to safeguard critical documents with long-term legal significance against loss, destruction or expiration.

Policy Statements:

- All finalized legal agreements, contracts, and documents bearing official municipal signatures must be stored in the official Document Management System (DMS) to enable proper backups, archival, and records retention.
- If a DMS has not yet been procured and implemented, signed hardcopy documents must be stored in a fireproof safe onsite with an additional physical copy stored offsite.
- Once a DMS is operational, all hardcopy signed documents will be digitized and uploaded with appropriate metadata applied based on records management procedures. The hardcopies will be destroyed after digitization.
- The Documents Management System must meet data security controls as per municipal IT policies, with access limited based on job function.
- Backup and retention periods will comply with statutory requirements for legal documents and records.

2.5 IT Policies Affecting HR

Purpose: Establishes municipal government information technology policies related to personnel management processes including hiring practices, staff training, procurement controls, equipment checkout, and offboarding procedures to integrate with human resources systems.

2.5.1 General Staff Hiring Policy

Purpose: Establishes required municipal government pre-employment screening, identity verification, background checks, onboarding controls, security training, and policy acknowledgement processes for information technology staff and any personnel requiring access to sensitive systems. It seeks to validate character and qualifications prior to enabling access to technology resources and trusted roles.

Policy Statements:

- Candidates must undergo mandatory background checks including criminal history, education, employment and reference verification.
- Applicable licenses and certifications related to IT claimed during hiring must be validated.
- New staff must acknowledge receiving this policy manual and sign agreement to comply with Section 2.1 Acceptable Use Policies.
- Orientation will review key organizational IT policies related to conduct, ethics, discrimination, and security.
- Signed policy compliance agreement must be on file prior to start date.
- Applicable access provisioning will only occur once policy commitment is documented.
- IT systems access, equipment, and communication channels must be provisioned on start date as per on-boarding procedures.

2.5.2 General Staff Termination Policy

Purpose: Defines access revocation, account deactivation, device return, policy re-acknowledgement, and data protection procedures comprising the employee and contractor separation and offboarding processes. It aims to rapidly eliminate access while underscoring limitations on appropriating municipal government information, intellectual property or technology.

Policy Statements:

- As part of off-boarding process, staff must re-acknowledge Section 2.1 Acceptable Use Policies related to ongoing data protection responsibilities.
- Access revocation includes termination of rights to utilize or retrieve any municipal data, resources, and systems as per signed IT policies.
- Exit interviews will reaffirm limitations on appropriation of municipal intellectual property, resources, and information.
- Immediately revoking access to systems and facilities upon termination.
- Conducting exit interviews upon voluntary departures.
- Collecting all company-issued equipment and assets.
- Disabling accounts across all systems including SaaS apps.
- Changing system credentials the former employee had access to.
- Communicating termination to internal teams and external vendors.

2.5.3 IT Training Policy

Purpose: Requires ongoing skills development, education, and certification maintenance for municipal government information technology staff to stay updated on evolving technologies, cybersecurity threats, regulatory obligations, and solution capabilities. It seeks to enhance IT competencies, service quality and cost efficiencies through motivated knowledgeable personnel equipped with current expertise.

Policy Statements:

- All IT staff must complete a minimum of 40 hours of technical training annually.
- Training needs assessments will be conducted annually and may be incorporated into performance reviews.
- IT staff are encouraged to pursue relevant professional certifications with policy covering exam fees and study resources.
- A department training budget will be maintained to cover registration fees for conferences, classes, workshops, and e-learning materials.
- When feasible, internal knowledge sharing events will be conducted to cross-train team members.
- Training completion will be tracked with records maintained by the IT department.
- Failure to meet required training hours may impact performance evaluations and job advancement opportunities.

2.5.4 General Staff Technology Training Policy

Purpose: Necessitates ongoing general security awareness and role-based training covering proper usage, data protection, incident response and specific municipal government software systems for all personnel. It aims to empower employees to support cyber defense, compliance, technology innovations and appropriate data handling through applied knowledge.

Policy Statements:

- All staff must complete annual security awareness training covering topics such as:
 - Identifying and reporting phishing attempts
 - Importance of strong passwords and multi-factor authentication
 - Proper handling and storage of sensitive data
 - Detecting social engineering attacks
 - Securing workstations and mobile devices
 - Responding to security incidents and policy violations
- Role-specific training will be provided on proper security controls and acceptable use policies for systems and applications that staff interact with.
- Training needs assessments will identify required skills and knowledge gaps related to use of municipal technologies.
- In-depth classroom or hands-on training sessions will be provided following new system implementations or upgrades.
- IT will maintain a training curriculum covering both general security topics and system-specific training areas.
- Departments heads are responsible for ensuring staff complete assigned security awareness and technology training activities.
- Training completion will be tracked and reinforced through periodic knowledge assessments.

2.5.5 IT Procurement Policy

Purpose: Establishes procurement planning, budgeting, vendor selection, contracting, purchasing authorization controls and approval workflows for municipal government information technology projects and acquisitions. It seeks to ensure IT investments optimally achieve departmental objectives and community needs while proactively managing costs and risks.

Policy Statements:

- All purchases of IT equipment, software, and services must follow defined procurement processes and policies.
- Procurement requirements should define competitive bidding thresholds, capital expenditure approvals, and purchasing authorization levels.
- Purchase requests must provide details on business need, options evaluation, and cost analysis.
- An IT architecture review should occur for purchases above a defined dollar amount to ensure compatibility and standardization.
- Software license agreements must be reviewed by legal counsel with restrictions on non-disclosure, intellectual property, and liability.
- Major system purchases should have a project implementation plan including testing, training, support, and post-implementation review stages.
- Equipment must be received and validated against orders prior to payment along with appropriate documentation.
- Vendor master data must be kept current including banking details, remittance addresses, and contact information.
- Procurement status reports should track purchasing volume, spend, and vendor distribution.

2.5.6 Equipment Checkout Policy

Purpose: Outlines procedures, liabilities, security responsibilities and use restrictions for municipal government employees temporarily assigned mobile laptops, tablets, phones or other portable computing devices necessary for remote work or business travel. It aims to enable flexibility while securing devices and information when accessed externally.

Policy Statements:

- All IT equipment designated for temporary employee checkout must be properly inventoried and tracked.
- Equipment must be approved for checkout use with any restrictions documented.
- Employees checking out equipment must submit a request identifying pickup date, duration needed, and business justification.
- Equipment will be signed out indicating name, department, contact information, and expected return date.
- Extensions on duration require re-approval by IT.
- Employees are responsible for safeguarding equipment while in their possession and will be liable for loss or damage.
- Equipment must be returned in acceptable working condition with all accessories and carrying cases.
- Checkout period may not exceed 60 days without justification.
- Upon return, equipment will be inspected, data securely wiped, and any issues documented before redeployment.

2.6 Communications Policies

Purpose: Defines policies specific to managing public-facing communications channels utilized by the municipal government including email systems, TV studios, electronic signage, websites and social media accounts to effectively engage citizens.

2.6.1 Department Email Addresses Policy

Purpose: Requires establishing and maintaining published generic department and function email addresses for each municipal government division that persist through staff turnover. It aims to provide consistent constituent contact points and simplify routing of messages to appropriate current personnel.

Policy Statements:

- Each municipal government department will be assigned a generic email address using the department name, e.g. finance@municipality.gov, hr@municipality.gov.
- The department email account will be separate from any individual staff accounts.
- The account credentials will be managed by the department head and shared with relevant staff required to access the inbox.
- Emails sent to the department address will be received and handled by appropriate staff rather than sitting with a single person.
- During staff transitions, the department email access will transfer to the new department head.
- Department email addresses will be published as the primary contact details on the municipal website and materials.
- Individual staff should use their personal municipal email for day-to-day business as usual communications.

2.6.2 IPTV Policy

Purpose: Outlines municipal government requirements, programming standards, system capabilities, legal prerequisites, and community access rules for the Institutional Network (I-Net) public, education and government cable television channels and video on demand platforms. It aims to maintain compliance with state statutes and Federal Communications Commission regulations for public media.

Policy Statements:

- The official legal record of municipal board and committee meetings shall be the unedited video recordings.
- Meeting videos will be made available on-demand within 3 business days or prior to the next scheduled meeting, whichever comes first.
- The full unedited meeting videos will remain accessible to the public online for a minimum of 2 years.
- Video metadata will include recording date, meeting name, agenda topics, and time stamps.
- Closed sessions which are not public will not be recorded or made accessible. Only open public sessions are recorded.
- The Municipal Clerk's office is responsible for posting meeting recordings and maintaining the video archives.
- The municipal IPTV channel shall follow Federal Communications Commission (FCC) public, educational, and government (PEG) access cable television requirements.
- PEG programming shall be segregated from commercial channels and content.
- The IPTV channel shall serve the needs and interests of the local community.
- Reasonable time must be allocated for each programming category: public, education, and government.
- Rules for priority access consideration shall be fairly applied to municipal departments, public schools, community organizations and individuals.
- Editorial control rests with the individual program producer rather than the cable operator.
- Complaints related to FCC PEG compliance shall be directed to the municipal clerk's office and cable advisory board.
- Reasonable time slots and channel capacity must be allocated for public content not produced by the municipal government or schools.
- Community organizations and individuals may request time slots for public content on a first-come, first-served basis.
- Requests must describe the general content or subject matter without need to submit full productions prior to allocation.
- Public content must meet community standards and may not include commercial promotions, illegal activity, copyright violations or obscene material.
- A maximum 30 minute time slot may be allocated per week for ongoing public content from an individual or group.
- Preferred prime time slots will be distributed equitably when demand exceeds available capacity.

- Complaints of unfair time slot allocations will be reviewed by the cable board to ensure policies are applied consistently.

2.6.3 IPTV Multimedia Presentation Policy

This policy supersedes:

Town of Raymond Policy - Raymond IPTV Content Display Policy - Adopted January 10, 2023

Purpose: Defines requirements, quality standards, testing procedures, technical specifications, accessibility mandates, and legal disclaimers for creating and presenting video programming intended for broadcast on the municipal government Institutional Network (I-Net) public, education and government cable television channels.

Policy Statements:

Presenters must be authorized by one of the following:

- Official Raymond Board Chair
- Raymond Town Manager
- Raymond Town Department Manager

Responsibilities:

- General public presenting content
 - Correctly formatted and supported content type
 - Manipulation of content before or during the meeting
 - List of website URL's that might be used in the presentation
 - Notifying the Communications Director of the presentation and the content type to be displayed. This notification should be at least 4 business days before the presentation.
 - Arriving at least 30 minutes before the meeting to test the presentation
 - Display of content during the presentation
- Municipal employee with Windows domain account presenting content
 - Signon to raymondmaine.int with their Windows domain account
 - Correctly formatted and supported content type
 - Manipulation of content before or during the meeting
 - List of website UR L's that might be used in the presentation
 - Notifying the Communications Director of the presentation and the content type to be displayed. This notification should be at least 4 business days before the presentation
 - Arriving at least 30 minutes before the meeting to test the presentation
 - Display of content during the presentation
- IPTV Videographer
 - Signing on the iptv.guest account for general public presenters
 - Setting the IPTV displays so the content may be tested before the meeting
 - Supply the password for the IPTV public WiFi when the presenter uses their own laptop
- Communications Director
 - Notifying the IPTV Videographer and Tech support of any presentations and content to be displayed at least 2 business days before the presentation
 - Test access to the websites that the presenter may try to access
- IPTV Tech Support

- Answer questions about supported Content Types and Content Access

Supported Content Types:

- The IPTV laptop is Windows 10 based with the listed software installed for display of content.
- All software and the Windows OS are kept current with service. Content types are supported if they can be displayed by the following software:
 - Microsoft Office 365 Pro including Word, Excel, PowerPoint
 - LibreOffice including Draw, Writer, Calc and Impress
 - Internet Browsers including Chrome, Firefox, Edge
 - Multimedia AudioVideo support with VLC media player (check www.videolan.org for supported file types)
 - Google Earth Pro Desktop
 - Adobe Acrobat Reader

Supported Content Access Methods:

- IPTV Laptop
 - The IPTV laptop is connected to the Internet and the Intranet. It has USB, USB-C ports allowing for USB attachable media storage devices and an SD card reader.
 - Devices that are natively supported by Windows 10 are supported. No devices that require non-native Windows 10 drivers will be supported.
 - The laptop is equipped with Webroot Endpoint and DNS Protection. This may block some websites so a list of websites to be used in a presentation should be forwarded to the Communications Director with the presentation notification.
- Presenter Supplied Laptop
 - The laptop can access the public WiFi at the IPTV station to display content. The Videographer will supply the password.
 - The laptop must have an external video display port with one of the following interface types and resolutions:
 - USB-C - 1080p
 - VGA - 720p
 - HDMI - 1080p
 - mini HDMI - 1080p
 - Display Port - 1080p
 - mini Display Port - 1080p
- Audio is only supported through the HDMI interface

All video, audio, and slide presentations produced for public broadcast on the municipal IPTV channel must follow defined standards.

- Presentations by municipal employees must comply with municipal branding, style, and logo guidelines.
- Narration and slides must contain appropriate disclaimers indicating they are not official legal documents.
- Presentations covering sensitive topics require additional review and approval prior to broadcasting.

- Presenters must have sufficient rights, consents, and licenses for any third party materials utilized in productions.
- Background music or media requires licensing appropriate for broadcast use.
- Presentations must meet TV closed captioning and other multimedia accessibility requirements.
- Presentation files and transcripts will be archived according to records retention policies post-broadcast.
- Presenters must arrive sufficiently early before broadcast to test their presentations and any required technology in the studio.
- Presentations must be tested to identify any compatibility issues or unsupported file formats needing correction.
- Proper cables and adapters must be confirmed available in advance if presenting from personal devices.
- Presenters should have technical rehearsals in the studio prior to live broadcasts when feasible.
- Presentation slides and embedded videos must be formatted at appropriate resolutions and aspect ratios suited for broadcast.
- Adequate transition and timing rehearsals should occur to smooth delivery and transitions.
- Broadcast equipment and software must be tested to ensure reliable audio levels and signal quality.
- Contingency plans should be in place for technical failures during live presentations or loss of connectivity.

2.6.4 Electronic Signage Policy

This policy supersedes:

Town of Raymond – Electronic Sign Policy - Adopted 1/9/2018

Purpose: Establishes appropriate usage guidelines, content standards, placement criteria, administration roles, and system security requirements for digital signage displays located within municipal government facilities. It seeks to effectively communicate with the public while preventing unauthorized access or abuse of signage systems.

Policy Statements:

- The primary purpose of the Town of Raymond’s electronic signs is to promote the Town of Raymond’s meetings, events and services.
- Additionally, the signs will:
 - Enhance Town communications and transparency.
 - Help Raymond be a more welcoming place for the public.
 - Recognize achievements and events within the Town of Raymond.
 - Promote safety awareness in the community.
- All electronic signage display screens located in municipal facilities are for official use only.
- Signage must be located in appropriate public areas with approval from department heads.
- Content displayed must meet branding guidelines and have educational, public service or administrative purposes.
- Emergency messaging takes precedence over standard content when necessary.
- Commercial advertising, political endorsements and inappropriate material are prohibited.
- The communications department will manage and approve content with input from stakeholders.
- Technical specifications will ensure accessibility for citizens and comply with laws.
- Remote device management capabilities must secure signage endpoints and software.
- The Town Manager may delegate sign management responsibilities as necessary.
- Priority will be given to Town departments, elected committees, and Selectmen-appointed boards and committees.
- Postings will be based upon space availability at the discretion of the Town Manager.
- The Town Manager reserves the right to deny use of the sign, alter the contents and the design of information, and post/remove messages as he/she sees fit.
- Exceptions may be granted by the Town Manager on an as needed basis at his/her sole discretion.
- How to Request a Posting
 - An application must be received by the Town Office at least 10 days prior the desired date of posting.
 - Applications will be available at the Town Office and on www.raymondmaine.org.
 - The application will include:
 - Contact information for the requestor
 - The nature of the event to be posted and how this event benefits the citizens of the Town of Raymond

- The desired text, and any desired pictures

2.6.5 Public Website Policy

Purpose: Defines requirements for architecture, administration, emergency contingency provisions, accessibility, cybersecurity, public records compliance and continuity planning for the primary official municipal government public-facing website and any affiliated domains. It aims to maintain a secure, current, usable public information portal representing the government entity.

Policy Statements:

- The municipal website and any affiliated domains must be managed by the communications department or an approved vendor.
- Website content must follow policies covering branding, accessibility, language, and ethical standards.
- Appropriate disclaimers and privacy policies must be published.
- Web hosting providers and technologies must meet security, resilience, and regulatory compliance standards.
- Web traffic, usage patterns and analytics must be monitored to enhance services.
- Web vulnerable code scanning, penetration testing, and remediation are required according to security policies.
- Webmaster roles, change approval processes, and access controls must be maintained.
- Content must be routinely backed up with contingencies for defacement or data loss scenarios.
- The public website will serve as the central public information portal with social media as supplemental outreach channels.

2.6.6 Public Social Media Policy

Purpose: Outlines approved usage, accessibility, public communications, security protocols and content standards for official social media accounts formally representing the municipal government across social media platforms. It seeks to effectively expand citizen outreach and engagement through social channels while safeguarding information and aligning to the government brand.

Policy Statements:

- The municipality's official social media accounts must be managed and maintained by the communications department.
- Accounts should be created only on approved platforms based on target audiences, demographics and municipal branding.
- Content must be accessible, professional, politically neutral and adhere to applicable laws and policies.
- Social media managers must be trained on privacy, security, accessibility and records retention requirements.
- Security controls like multi-factor authentication must be enabled to prevent unauthorized access.
- Social media posts may require public records retention, e-discovery and legal holds.
- Comments and messaging must be monitored consistently and inappropriate content removed promptly.
- Disclaimers should state that third-party content does not reflect municipal opinions or endorsements.

2.6.7 Integration with Local FEMA Plans

Purpose: Enables prudent sharing and coordination of municipal government information technology assets, systems, data and personnel as dictated by Federal Emergency Management Agency (FEMA) incident response plans activated within the locality during major emergencies or disasters. It aims to integrate IT capabilities into community-wide emergency preparation, readiness and response efforts.

Policy Statements:

- The municipality will collaborate with the county office of emergency management and FEMA to integrate IT capabilities into emergency operations plans.
- IT will designate staff roles aligned to the incident command system (ICS) for responding to disasters and emergencies declared by FEMA.
- Technology resources including computers, mobile devices, radios, networks, and satellite communications will be made available to the emergency operations center (EOC) as required.
- Municipal IT policies will enable sharing appropriate data with authorized FEMA response teams during incidents to coordinate efforts.
- IT will maintain and periodically test contingency plans invoked upon activation of FEMA emergency response plans for the locality.
- Any gaps identified in IT resources or capabilities to support the community's FEMA plan will be addressed in collaboration with emergency management leadership.

2.6.8 Municipal Meetings Policy

This policy supersedes:

Town of Raymond - Municipal Meetings Policy - Adopted 10/8/2019

Purpose: Standardizes rules, accessibility requirements, parliamentary procedures, public participation and records handling for open meetings of municipal boards, committees, commissions and government bodies. It seeks to maintain transparency, consistency, order, legal compliance and productive outcomes across public meetings.

Policy Statements:

- All municipal boards, committees and commissions shall conduct meetings following the latest edition of Robert's Rules of Order for parliamentary procedures, except where overridden by local, state or federal laws.
- Electronic video recordings shall be considered the official primary record of municipal meetings when available. Written minutes shall be considered supplemental records.
- Meeting videos shall be made publicly accessible on the municipal website or YouTube within 3 business days or before the next scheduled meeting, whichever comes first.
- Written minutes must identify all video timestamp ranges corresponding to agenda items, motions, votes, and key discussions, in addition to supplemental details.

2.7 Security Policies

Purpose: Prescribes cybersecurity and information protection policies covering technologies, controls, awareness, vendor management, and risk mitigation planning to guard municipal government systems and data against internal and external threats.

2.7.1 Encryption Policy

Purpose: Outlines requirements for layered network security defenses incorporating monitored firewalls, intrusion detection/prevention systems, segmentation, regular vulnerability scanning, wireless controls, remote access restrictions and current endpoint security to protect municipal government networks from compromises and cyberattacks initiated both internally and externally.

Policy Statements:

- Acceptable encryption algorithms, protocols, and minimum key lengths must adhere to industry standards and best practices.
- Encryption should be utilized for data at rest and in transit wherever technologically feasible.
- Highly sensitive data must require encryption when stored, accessed, or transmitted.
- Policies must balance end user experience and usability when applying encryption controls.
- A secure key management process is required covering generation, distribution, storage, rotation, and destruction of keys.
- Access to encryption keys should be logged and tightly restricted based on roles.
- Encryption deployment must align with data classification scheme and regulatory compliance obligations.
- Standards should outline approved technologies, configurations, and implementation practices.
- Encryption requirements should be formally defined for vendors, contractors and other third parties.
- Periodic audits must validate correct encryption usage, key management and policy compliance.

2.7.2 Network Security Policy

Purpose: Outlines requirements for layered network security defenses incorporating monitored firewalls, intrusion detection/prevention systems, segmentation, regular vulnerability scanning, wireless controls, remote access restrictions and current endpoint security to protect municipal government networks from compromises and cyberattacks initiated both internally and externally.

Policy Statements:

- Network perimeter controls like firewalls, IDS/IPS must follow documented standards for secure configuration and maintenance.
- Network segmentation should isolate and restrict traffic between subnets based on data classification levels.
- Wireless networks must incorporate authentication, encryption and access control best practices.
- Network infrastructure security logging and monitoring is required to detect potential attacks and anomalies.
- Ports and services should be disabled if not explicitly required for approved business use.
- Network vulnerability scanning must regularly test defenses and identify gaps or misconfigurations.
- Patch management processes must maintain currency of network device software and firmware.
- Change management procedures are required for network changes or reconfigurations.
- Network diagrams and data flows must be kept updated and aligned with infrastructure.
- Networks carrying payment card data must adhere to PCI DSS wireless guidelines

2.7.3 Vendor Management Policy

Purpose: Defines security controls, risk assessment requirements, access restrictions and contract clauses when allowing external vendor, contractor, partner and consultant connections to municipal government networks, systems and data. It seeks to enable prudent third party business relationships while ensuring accountability, layered defenses and protections govern all remote and onsite vendor access.

Policy Statements:

- Formal risk assessments must be conducted for all third party vendors processing, storing or accessing the municipality's confidential data.
- Risk levels should be determined based on data classification and vendor assigned trust levels.
- Legal agreements must document security expectations, liability, failure reporting, and right-to-audit clauses.
- All vendor accounts accessing municipal resources must utilize strong multifactor authentication and least privilege restrictions.
- Vendor remote access must route through isolated network segments with additional inline controls.
- Valid vendor certificates must be installed to securely authenticate any external connections.
- Vendor credentials and passwords should be regularly rotated and immediately revoked after engagements.
- Change management procedures must be followed when modifying vendor access privileges.
- Timely deprovisioning of access must occur for vendor personnel no longer assigned to municipal projects.
- Periodic review of vendor entitlements is required to ensure appropriate and timely deprovisioning.

2.7.4 Teleworking Policy

Purpose: Extends existing municipal government information technology security policies, protocols, employee awareness responsibilities and acceptable use standards to remote work and telecommuting situations. It seeks to maintain effective safeguards, access restrictions and data protections for government networks, systems and information when accessed externally.

Policy Statements:

- Employees approved for telework must adhere to all security, acceptable use, and general HR policies when working remotely.
- Required hardware, software, and networking equipment will be provided by IT to facilitate secure remote access.
- Teleworkers are prohibited from connecting to internal networks directly from personal or public systems.
- Multifactor authentication must be utilized for any remote access connections to internal resources.
- Teleworkers must ensure confidential data is not transmitted or stored on unauthorized systems.
- Regular anti-malware scanning and prompt application of system updates is required for remote endpoints.
- Teleworkers must take precautions to prevent unauthorized access to work devices or materials within home environments.
- Secure VPN must be utilized when accessing internal applications and data remotely.
- Remote desktop access to internal systems should employ strong session encryption algorithms.

2.7.5 Secure Password Storage Policy

Purpose: Prohibits plaintext storage or transmission of municipal government user credentials or passwords. It requires properly hashing passwords, limiting access to hashes, utilizing salted hashes, and encrypting passwords for transmission across networks. This policy seeks to prevent password compromise, theft and misuse through technical protections and restricted access.

Policy Statements:

- User credentials and passwords must not be stored or transmitted in plaintext.
- Passwords must be hashed using secure cryptographic algorithms before persistence.
- Hashed passwords should leverage salting with a unique, random salt per user.
- Secure password stores such as password management systems must be used to securely store credentials.
- Access to password stores must require multifactor authentication aligned to privilege requirements.
- The use of authorized password stores must be audited regularly by IT security.
- Shared account credentials must only be stored in approved central, encrypted stores with access limited to required personnel.
- Administrative passwords must follow defined complexity standards and rotation frequency.
- Passwords or access keys for encrypted data stores should be kept separate from the data.
- Compromised credentials must be changed immediately across all systems.

2.7.6 Mobile Device Management Policy

Purpose: Defines requirements for central enrollment, configuration, encryption, remote wipe capabilities, access controls, allowable applications and acceptable use standards for all municipally-issued smartphones, tablets, laptops and mobile devices based on data sensitivity levels. It aims to maintain appropriate mobile security, data protection and operational control irrespective of device location.

Policy Statements:

- All municipality-issued mobile devices must be enrolled in the central mobile device management (MDM) system.
- MDM capabilities should include inventory tracking, configuration control, remote wiping, app management, and automated policy enforcement.
- Passcode complexity, data encryption, remote wipe, installed app restrictions, and antenna control policies will be implemented based on data risk levels.
- Jailbreaking, rooting, unlocking bootloaders, or otherwise circumventing built-in device security controls is strictly prohibited.
- Required MDM agents must not be uninstalled, disabled or worked around without explicit authorization from IT.
- Remote wipe of municipal data will be performed if a device is lost or stolen.
- Mobile devices must be kept secure when traveling and not left unattended in public.
- Any loss or theft of municipal mobile devices must be reported immediately to IT and management.

2.7.7 Vulnerability Management Policy

Purpose: Mandates continuous vulnerability identification, risk-based prioritization, centralized tracking and remediation of security weaknesses discovered within municipal government information systems, software applications, and network infrastructure following established practices. It seeks to systematically find and mitigate risks thereby measuring and enhancing organizational cyber resilience.

Policy Statements:

- An inventory of all IT assets and software must be maintained, along with assignment to data owners.
- New systems must have vulnerabilities identified prior to production deployment through static or dynamic analysis testing.
- Automated vulnerability scanning tools will be configured to perform periodic scans of networks, servers, endpoints, applications, databases, and other systems.
- Detected vulnerabilities will be classified and risk rated based on severity, exploitability, and potential impact.
- Asset owners will be provided with vulnerability reports, and expected to remediate issues within defined timelines based on severity risk rating.
- Vulnerability remediation will follow change management processes and incorporate compensating controls if immediate patching is infeasible.
- IT security team approval is required for exemptions or acceptance of any vulnerabilities deemed high risk.
- External penetration tests will be performed annually to identify vulnerabilities through simulated attacks against the environment.

2.7.8 Central Credentials Repository Policy

Purpose: Requires use of an approved centralized password vault or secure digital wallet for storage, access controls and management of credentials necessary for administering municipal government systems, data and devices. It aims to reduce standing access while improving password strength, periodic rotation and revocation when employees are off-boarded or transition between roles.

Policy Statements:

- All credentials and passwords necessary for administering municipal systems and hardware must be securely stored in an approved central password management repository.
- This includes passwords for server operating systems, network devices, workstations, system administrator accounts, software logins, and hardware/firmware passwords.
- The central password repository must utilize encryption and multifactor authentication for access.
- Only IT staff with an essential administrative job function may be granted access to the repository.
- Passwords must be programmatically generated with sufficient complexity and rotated at appropriate intervals.
- Repository permissions and access must be reviewed quarterly to ensure only authorized users have continued access.
- Logging and auditing capabilities must track all password viewing, access and usage.
- Onboarding/offboarding processes must immediately grant or revoke access for IT administrators.

2.7.9 Electronic Signature Policy

Purpose: Enables, establishes legal validity, and governs the permitted use and required controls when accepting electronic signatures on municipal government records, forms, registrations, contracts and other documents requiring execution or approvals. It aims to improve efficiency and continuity while still maintaining integrity, non-repudiation, and legal compliance.

Policy Statements:

- Electronic signatures should meet requirements to be legally binding and enforceable.
- An electronic signature policy and process must be defined covering how they are used, technologies enabled, access controls, and signature validity.
- Acceptable electronic signature methods may include username/passwords, PINs, digital signatures, or third party signing services.
- Multifactor authentication should be utilized where possible for identity assurance.
- Signed records must maintain authenticity, integrity, non-repudiation, and audit log traceability.
- All uses of electronic signatures should follow records management policies for retention requirements.
- Procedures must ensure continued verifiability of signatures over long term records retention.

2.7.10 Remote Vehicle Monitoring Policy

Purpose: Allows tracking, telematics and driver monitoring on municipal government vehicles to cost-effectively improve fleet safety, fuel efficiency, routing, and asset security balanced by restrictions preventing unauthorized personal location tracking or data misuse. It aims to enhance municipal operations through vehicle telemetry data while recognizing and mitigating privacy concerns.

Policy Statements:

- GPS tracking and telematics systems installed on municipal vehicles are for official purposes only related to fleet management, safety, and asset protection.
- Detailed locational tracking and reporting of official municipal vehicles may occur without notice. Personal use vehicles will be excluded.
- Drivers may be monitored for speed, acceleration, braking, seat belt usage and idle times to improve safety and economy.
- Alerts may be configured to detect unauthorized usage during off hours or geographical restrictions.
- Vehicle telemetry systems and collected data will be adequately secured against unauthorized access or tampering.
- Collected vehicle usage statistics, geospatial data, and reports will be protected appropriately per data classification.
- Any driver privacy concerns related to vehicle telematics monitoring should be raised to the Fleet program manager.

2.7.11 Internet Proxy Policy

Purpose: Requires routing all municipal government employee computer and mobile device external internet traffic through an authorized network proxy server to enforce content filtering, logging, threat protection, bandwidth management and access controls aligned to acceptable use policies. It aims to securely manage internet usage, prevent inappropriate activities, and protect government resources.

Policy Statements:

- All employee internet access must route through the authorized web proxy server on the municipal network.
- The proxy will perform content filtering to restrict access to prohibited or inappropriate websites in accordance with Acceptable Use Policies.
- Websites categorized as blocked will be inaccessible to standard users. Whitelist exceptions require IT approval.
- The proxy will log all internet access including sites visited, files downloaded, and user attribution. Logs will be retained per regulatory requirements.
- Encrypted HTTPS traffic may be decrypted at the proxy for logging, filtering, and malware prevention where legally permissible. Employees receive a warning upon policy acknowledgement at hiring.
- Prohibited activities including accessing illegal content, torrents/P2P, malicious sites will be blocked and reported via alerts.
- The proxy must load balance web requests across internet connections and provide denial of service attack mitigation.

2.7.12 Credit Card Payment Policy

Purpose: Establishes network segmentation, system security, key handling, physical controls, and strict access restrictions when processing, storing or transmitting payment card data to maintain compliance with mandated payment card industry data security standard (PCI DSS) requirements. It aims to enable secure digital payment capabilities while preventing unauthorized card data exposure.

Policy Statements:

- All credit card payment activities must comply with the Payment Card Industry Data Security Standard (PCI DSS).
- Cardholder data includes the full card number, expiration date, CVV code, and name. This information must be protected.
- Only approved municipal payment systems and methods may be used to process payments.
- Any new payment technologies or services must be assessed and approved to ensure PCI compliance.
- Cardholder data may only be used for processing payments and must not be stored in municipal systems unmasked.
- Secure mechanisms must tokenize/mask data at point of transaction.
- Physical media containing card data must be securely stored with strict access controls if permitted under policy.
- Personnel accepting payments must complete annual PCI DSS awareness training.
- Quarterly network and application scans must validate PCI compliance. Any gaps or policy violations must be remediated urgently.

2.7.13 Removable Media and Storage Device Usage Policy

Purpose: Outlines approved usage, data restrictions, maintenance processes and prohibited activities related to memory sticks, flash drives, external drives, optical discs and other removable media devices within the municipal government environment. It seeks to prevent data loss, malware infections and inappropriate information access through controlled portable media.

Policy Statements:

- Use of removable media such as USB drives, external hard drives, CD/DVDs is only permitted for authorized purposes. Personal use is prohibited.
- Storage devices must be scanned for malware before use and encrypted as per data protection standards.
- Confidential data should not be stored on removable media except for essential backup or transfer operations with approval.
- Removable media containing municipal data should be physically secured when not in use.
- IT asset management records should track assignment of USB drives to users and device inventories.
- Removable media should be permanently erased or destroyed prior to disposal according to data sanitization standards.
- Writing confidential data to consumer cloud drives, email platforms or exchange via unauthorized services is prohibited.
- IT approval is required for connecting unauthorized devices like personal phones or storage devices to municipal systems.

2.7.14 Vulnerability Disclosure Policy

Purpose: Defines secure policies and procedures including communications channels, coordinated disclosure timelines and legal safe harbor that govern external security researchers ethically reporting discovered vulnerabilities within internet-accessible municipal government digital systems, services and applications. It aims to enable improved security and citizen trust through responsible disclosure protocols.

Policy Statements:

- This policy provides guidelines for security researchers and third parties to responsibly report vulnerabilities discovered in municipal systems.
- Discovered vulnerabilities should be reported via encrypted email to security@municipality.gov which will create a security event ticket.
- Sufficient details should be provided to reproduce and validate the vulnerability, along with a suggested severity rating based on impact.
- Public disclosure of vulnerabilities by the researcher should not occur until reasonable time for remediation has passed after notification.
- Subject to verification, individuals or organizations who follow this policy will not face negative consequences for discovering and reporting vulnerabilities responsibly.
- After mitigation, credits and acknowledgement may be provided to reporters at their discretion.
- Confirmed significant vulnerabilities will be addressed based on severity within the following response timeframes:
 - Critical - 7 days
 - High - 30 days
 - Moderate - 90 days
 - Low - 180 days
- An encrypted public key will be made available for securely communicating vulnerability details.

2.7.15 IT Forensics and Legal Investigations Policy

Purpose: Establishes prudent requirements for proactive security logging, regular baseline backups, chain of custody, evidence preservation, accountability and data recovery to support municipal government investigations, litigation responses and court proceedings involving electronically stored information. It aims to balance security, privacy and compliance obligations.

Policy Statements:

- This policy establishes procedures to support legal investigations and e-discovery requests involving municipal IT systems and data.
- Formal information requests must be validated and approved by the City Attorney prior to IT assistance.
- IT will maintain baseline forensic images of critical systems to expedite investigation or recovery needs.
- Forensic tools will utilize write-blocking to preserve digital evidence integrity during analysis.
- Chain of custody will be followed when handling and transferring evidence media.
- Collected evidence will be securely stored in a manner allowing for admission as exhibits in legal proceedings.
- Documents and electronic records designated as responsive to an investigation will be comprehensively identified and preserved.
- Redaction of privileged, confidential or non-responsive data will occur prior to release.
- The City Attorney will coordinate the review and release of electronic records to parties in litigation.
- IT security will ensure all exported records are properly authenticated.

2.8 Infrastructure Policies

Purpose: Provides policies guiding management of municipal government networks, systems environments, buildings, electronic access controls and other technology infrastructure to maintain reliability, business continuity, and physical security.

2.8.1 Resilient Network Policy

Purpose: Requires architects to design municipal government networks with redundancy, fault tolerance, traffic engineering and failover capabilities that maximize availability and eliminate single points of failure. It aims to sustain reliable connectivity, prevent outages, and maintain business continuity through intentional resilient network characteristics.

Policy Statements:

- The municipal network will be architected to maximize resilience and redundancy.
- A fiber optic backbone ring will be implemented utilizing redundant connections between locations.
- In the event of a fiber cut or node failure, traffic will automatically reroute in the opposite direction on the ring.
- Critical network availability zones will be established served by redundant fiber rings.
- 10Gbps minimum ring capacity will prevent outages during peak demand. Self-healing 1Gbps rings can serve standard locations.
- Rings will incorporate automatic failover to redundant paths based on open shortest path first (OSPF) routing.
- Ring connections will utilize a compatible framing architecture like SONET/SDH.
- Network operations staff will be trained to rapidly isolate and bypass failed ring segments.
- Requirements like diversity, distance, and quality will apply for new fiber installations.

2.8.2 Building Automation Policy

Purpose: Defines physical, logical and administrative security safeguards required for building automation systems controlling lighting, HVAC, energy management, physical access and other capabilities that enable smart energy efficient municipal government facilities. It seeks to prevent unauthorized access or manipulation of automated environmental systems.

Policy Statements:

- Building automation systems controlling HVAC, lighting, electrical, and security must be properly secured against unauthorized access.
- Access will be limited to facilities management staff with least privilege permissions. Multifactor authentication should be enforced.
- Systems must be isolated from the corporate network and other high risk assets.
- Monitoring will detect abnormal equipment behavior and failures. Alerting will notify staff of issues.
- Disaster recovery plans will cover rebuilding system programming and restoring configs from backups.
- Change management procedures will be followed for any modifications to equipment or automation programming.
- Systems will undergo periodic pentesting to validate the effectiveness of security controls. Vulnerabilities will be remediated.
- Equipment should receive timely firmware updates to fix known holes and maintain warranty coverage.
- Physical controls will prevent unauthorized access to automation controllers, wiring and networked components.

2.8.3 VoIP Server Policy

Purpose: Outlines installation, configuration, authentication, availability redundancy, encryption, access restrictions and network security precautions required when deploying Voice over IP (VoIP) phone systems to provide enterprise telephony capabilities across municipal government locations and personnel. It aims to enable unified communications with security, resiliency and compliance.

Policy Statements:

- The municipal VoIP phone system must be secured against unauthorized access and abuse.
- The PBX will be configured to use complex passwords, IP address whitelisting, and limit remote login.
- Voicemail PINs will enforce complexity standards and be distributed separately from phone extension assignments.
- Automated remote alerts will notify on detected attacks, breaches, or outages impacting the VoIP system.
- Network traffic will be encrypted between the PBX, phones, and voice gateway using TLS/SRTP.
- Vulnerability scans will assess any risks, misconfigurations, or unpatched PBX components.
- The PBX and phones will reside on an isolated network segment to restrict traffic.
- QoS prioritization will ensure optimal voice quality on the network.

2.8.4 E-Mail Server Policy

Purpose: Establishes architecture, storage, backup, redundancy, security hardening, anti-spam, continuity provisions and access control measures required to ensure availability, integrity and data protection for municipal government email platforms, data stores and mailbox accounts. It seeks to balance communication capabilities supporting operations with appropriate safeguards.

Policy Statements:

- E-mail servers enabling staff mailboxes must be secured against unauthorized access.
- Servers will have unnecessary services disabled, utilize TLS encryption, and be kept updated.
- Mailboxes will require strong passwords that expire periodically.
- Server logs will feed into security information and event management (SIEM) systems for centralized analysis.
- Boundary defenses like spam filtering and attachment sandboxing will detect malicious emails.
- Mail flow will incorporate mechanisms to block phishing attempts and graymail.
- E-mail continuity and retention capabilities will meet policy and statutory requirements.
- Mail server access controls will follow least privilege principles and access will be monitored.

2.8.5 Physical IT Infrastructure Access Control Policy

Purpose: Manages physical access to restricted areas containing sensitive municipal government information technology infrastructure through defined electronic access control requirements, multifactor authentication, video surveillance, visitor protocols, access reviews and revocations aligned to security roles. It aims to allow necessary physical proximity while preventing unauthorized entry.

Scope: This policy applies to controlled areas including data centers, network closets, server rooms, telecom facilities, and areas specially designated to house sensitive IT assets. It covers all employees, contractors and third parties who require physical access to these restricted facilities.

Policy Statements:

- Electronic access control systems using badge readers or biometric scanners must be installed on entry points to restricted IT facility areas.
- Physical access to restricted areas will be granted only to personnel with designated job roles requiring proximity to sensitive infrastructure for tasks like hardware maintenance, cabling, monitoring or repair.
- Security teams will administer access control permissions and maintain a definitive up-to-date roster of authorized staff needed in these areas.
- Any new access requests or adjustments to access must go through an approval workflow including the asset owner and security manager.
- Comprehensive physical access logs will be maintained and regularly reviewed to identify anomalies.
- Electronic locks must default to failing closed if the access control system or power source is disrupted.
- All physical access points must have updated video surveillance with 90 days retention to correlate access logs and events.
- Annual audits will validate that electronic lock access to sensitive facilities aligns with least privilege principles.

Compliance: Facility managers and asset owners are responsible for requesting appropriate access for their teams. Security managers must approve requests and ensure adherence to this policy. Violations may result in disciplinary action.

2.8.6 Building Security and Alarm Policy

Purpose: Establishes integrated electronic, network and physical security controls required to detect unauthorized entry, tampering or threats to municipal government facilities while enabling rapid, effective incident response. It seeks to protect infrastructure, information and occupants through layered defenses.

Policy Statements:

- Physical access controls must secure municipal buildings, offices, and facilities housing IT infrastructure or sensitive data.
- Security controls will include door access card readers, CCTV cameras, duress/panic buttons, motion detectors, glass break sensors and tamper alarms as appropriate.
- Card reader access must be integrated with IT user account management and provisioning systems.
- Alarms must notify security personnel and systems must create audit logs of all access and events.
- Warning signage will be posted making unauthorized entrants aware of monitoring and alarm systems.
- Contingency plans must cover alarm failures, communication disruptions, and duress scenarios preventing card use.
- Technical controls will aim to channel and restrict access, detect intrusions, delay breach progress and respond rapidly to incidents.
- All physical security systems must be included in backup routines, redundancy configurations and disaster recovery plans.

2.8.7 Website Server Policy

Purpose: Defines secure configuration, redundancy, backup, access restrictions, vulnerability management, and continuity provisions needed to keep public-facing municipal government web servers available and protected from compromise. It aims to maintain ongoing uptime and availability of online services that citizens rely on.

Policy Statements:

- The website server environment must adhere to system hardening standards based on best practices.
- Operating systems, applications, and content management systems must utilize security capabilities and receive regular patches/updates.
- Unnecessary ports, protocols, and services will be disabled to reduce the attack surface.
- Network firewall rules will restrict traffic to only required ports.
- Web application firewalls or filtering devices will provide additional security layers against attacks.
- User access to backend website management interfaces will require multifactor authentication.
- Server logging will be centralized and monitored for signs of unauthorized access or abuse.
- Minimum TLS version for web traffic will meet cryptography standards.
- Backup and disaster recovery provisions must allow restoration of servers and website content.
- Default credentials on websites, applications, and devices will be changed.
- Server user access will be limited based on the principle of least privilege.
- File and folder permissions will be properly configured according to approved standards.
- Input validation and sanitization will help prevent website application attacks.
- Source code will be reviewed for vulnerabilities prior to deployment to production.
- Continuous security and vulnerability scanning will identify risks for remediation.

2.8.8 Intranet Server Policy

Purpose: Outlines access control rules, traffic restrictions, security hardening, web encryption, and availability measures required for internal employee-only municipal government intranet servers providing authenticated access to tools and resources. It seeks to enable workforce productivity through internal web apps while preventing external intrusions.

Policy Statements:

- Intranet web servers allowing employee access must be secured to prevent unauthorized use.
- Content must be properly access controlled based on defined user roles and privileges.
- Authentication will integrate with the employee directory and use multifactor methods where possible.
- Intranet resources will only be accessible from the internal corporate network or via VPN tunnels.
- Web traffic must utilize TLS encryption and verified certificates to prevent eavesdropping.
- Servers will have unnecessary services and ports disabled to minimize vulnerabilities.
- Operating systems and web platforms will be kept fully patched and up-to-date.
- Backup routines must ensure content and configuration can be restored after outages.
- Security controls will undergo periodic penetration testing and remediation to identify gaps.

2.8.9 Video Surveillance Infrastructure Policy

Purpose: Establishes capabilities, cyber protections, high availability, open architecture to support integrations, footage retention rules, and access controls mandated for IP-based video surveillance, camera systems and video analytics supporting physical security for municipal government facilities. It aims to enable ongoing situational awareness and forensic investigations.

Policy Statements:

- Surveillance cameras should utilize PoE for connectivity and power where feasible. PoE switching must provide reliable power.
- Cameras must have adequate resolution, storage and bandwidth to enable facial recognition and license plate capture according to system capabilities.
- Video analytics systems require defined use cases, protections and oversight to ensure responsible use.
- Facial recognition capabilities must meet accuracy thresholds prior to deployment in coordination with legal and IT teams.
- License plate recognition requires proper lighting, positioning, resolution and machine learning algorithms.
- Continuous footage streams are needed at sufficient quality levels to support analytics.
- Facial and license plate data constitute sensitive personal information requiring strict access controls and encryption.
- Surveillance servers, workstations and networking equipment will reside on isolated, segmented networks per standards.
- Access controls will govern viewing, search and export of footage based on defined roles. Multifactor authentication is required.
- Encryption must be employed for video at rest and in transit if confidential data could be captured.
- Infrastructure redundancies and backups should allow continuous recording and access to feeds/archives.
- Physical security controls will prevent unauthorized access to surveillance infrastructure and wiring.

3 IT Standards

Purpose: Defines detailed technical specifications, configuration requirements, and design architectures for municipal government software, hardware, networks, facilities, security controls and cloud environments based on industry leading practices to optimize performance, reliability, continuity and security of technology resources.

3.1 Open Source Software Standards

Purpose: Defines security, licensing and procurement controls when adopting open source software platforms across municipal government systems to realize benefits like flexibility and lower costs while managing associated risks.

3.2 IPv6 Adoption Standards

Purpose: Standards and migration approaches for transitioning municipal government networks, systems and devices from IPv4 to IPv6 addressing to align with industry direction and prevent address exhaustion disruptions.

3.3 Firewall Standards

Purpose: Establishes specifications for firewall architecture, encryption capabilities, segmentation, configuration, logging, performance, redundancy and security capabilities to protect municipal government networks.

3.4 Network Infrastructure Standards

Purpose: Provides standards for deploying and managing high availability wired LAN, secure wireless LAN, and reliable WAN connectivity linking all municipal government facilities and users.

3.4.1 Wired LAN Standards

Purpose: Provides detailed technical standards and specifications for designing, deploying and managing secure, high performance, and reliable wired local area network (LAN) infrastructure to sustain connectivity for municipal government users and systems within facilities.

3.4.2 Wireless LAN Standards

Purpose: Defines architecture, segmentation, authentication, encryption, access control and monitoring requirements when implementing and operating municipal government workplace and public wireless local area networks (WLAN). It aims to enable mobility while restricting unauthorized access.

3.4.3 WAN Connectivity Standards

Purpose: Outlines technical specifications, service level requirements, diversity, failover, and security controls when procuring and implementing high speed, low latency, reliable and secure wide area network (WAN) connectivity between municipal government facilities.

3.5 Workstation Configuration Standards

Purpose: Defines standard hardware and software configurations, security controls, managed device settings, and administrative policies for municipal government workstations by operating system and user role to optimize security, performance and support.

3.6 Server Standards

Purpose: Prescribes specifications for hardened server installation, configuration, authentication, encryption, access controls, virtualization, administration and lifecycle replacement of municipal government servers.

3.7 Server Room and Data Center Standards

Purpose: Provides detailed requirements for physical security, power delivery, battery backup, generator backup, HVAC temperature/humidity controls, water detection, fire suppression systems and cabling within rooms and data centers housing critical municipal government IT server and network infrastructure. It aims to create resilient reliable spaces protecting critical systems from environmental threats, disruptions and unauthorized physical access.

3.8 Equipment Racks and Cabinets

Purpose: Requirements for standardizing IT infrastructure rack design, power distribution, cooling, cable management and equipment mounting to provide consistent and safe installation.

3.9 Access Control and Authentication Standards

Purpose: Specifies standards for electronic physical access control systems, user authentication methods, and secure remote access to provide identity validation and restrict unauthorized access to municipal government resources.

3.9.1 Access Control Standards

Purpose: Defines requirements for electronic physical access control systems including supported strong authentication methods, audit logging, door controller and electrified lock specifications, request/approval processes, and integration with other security systems. It aims to allow appropriate access while preventing unauthorized entry to restricted areas.

3.9.2 Authentication Standards

Purpose: Establishes approved methods, protocols and technologies to authenticate identity when granting access to specific municipal government IT resources based on data sensitivity levels. It aims to properly verify users are who they claim to be through standards covering passwords, multi-factor authentication, biometrics, digital certificates, single sign-on, and identity federation.

3.9.3 Network Access Standards

Purpose: Specifies secure protocols, encryption algorithms, configuration controls, timeout thresholds, logging, and layered defenses required when accessing internal municipal government enterprise networks or resources remotely over untrusted external networks. It seeks to enable secure remote connectivity to government systems for authorized users.

3.10 VoIP Infrastructure Standards

Purpose: Defines detailed availability, call routing, quality of service, security, power backup, redundancy, surge protection, and wiring requirements for municipal government Voice over Internet Protocol (VoIP) communications systems including IP phones, PBXs, voice gateways, session border controllers and underlying network infrastructure. It aims to deliver reliable enterprise telephony capabilities.

3.11 Video Surveillance Standards

Purpose: Outlines minimum camera resolution, retention duration, availability, cyber protection, secure integrations, access control and data handling mandates for video surveillance, IP cameras, digital video recorders, video analytics, and monitoring workstations used to enhance physical security of municipal government facilities based on industry best practices.

3.12 Cellular Device Standards

Purpose: Establishes standard secure configurations, device management standards, data encryption, remote wipe abilities, system integrations, and acceptable use policies for municipally-owned cellular phones, smartphones, wireless hotspots and cellular-enabled devices issued to government employees based on data sensitivity levels. It aims to maintain appropriate mobile security.

3.13 Cloud Computing Standards

Purpose: Defines security, redundancy, procurement, and governance requirements when adopting infrastructure (IaaS), platform (PaaS), software (SaaS) or other cloud computing delivery models to provide services involving municipal government data. It seeks to enable cloud benefits while ensuring provider oversight, managing risks, retaining control over sensitive data, and supporting continuity.

3.14 Database Server Standards

Purpose: Outlines specifications for secure installation, configuration, encryption, access controls, permissions, auditing, redundancy, and disaster recovery when deploying and managing database servers containing restricted municipal government information. It aims to protect the confidentiality, integrity and availability of database systems and data.

3.15 Email Server Standards

Purpose: Provides minimum requirements for storage quota assignment, retention duration, attachment restrictions, encryption, IMAP/POP3 access controls and authentication mechanisms for municipal government enterprise email platforms along with availability, redundancy, security hardening and backup specifications. It seeks to balance communication utility with security for email infrastructure.

3.16 Directory Services Standards

Purpose: Defines specifications for centralized directory services and identity stores supporting single sign-on, role-based access controls, password synchronization, identity lifecycle management, and redundancy for municipal government user authentication systems. It aims to streamline identity management and access control administration.

4 IT Procedures

Purpose: Provides instructions and standardized processes for executing routine IT management tasks related to assets, changes, incidents, availability, backups, projects and other technology operational areas to maintain consistent, efficient service delivery.

4.1 Asset Management Procedures

Purpose: Provides instructions for maintaining a frequently updated centralized inventory of all municipal government information technology hardware and software assets including data sources, scanning processes, inventory maintenance workflow, and integration with other IT systems for tracking licenses, contracts, acquisitions and depreciation.

4.2 Change Management Procedures

Purpose: Outlines required procedures and responsibilities for requesting, reviewing, approving, scheduling, testing, implementing, documenting and verifying changes to municipal government technology systems, infrastructure, hardware, software, applications and services per defined change management processes.

4.3 Incident Response Procedures

Purpose: Formally defines roles, responsibilities, internal/external communications channels, triage processes, reporting requirements and steps to detect, analyze, prioritize and respond to information security incidents, cyber attacks and data breaches against municipal government digital assets according to established protocols.

4.4 Disaster Recovery Procedures

Purpose: Provides detailed checklists of sequential recovery steps, testing methods, and responsibilities for enacting municipal government disaster recovery plans to restore essential IT operations, critical infrastructure and key systems to re-establish productivity following different type of outage or disruption scenarios.

4.5 Backup and Restore Procedures

Purpose: Delineates standardized processes, scheduling, reporting, verification testing, and data protection handling requirements for conducting backups of critical municipal government systems and data along with executing restores of files, folders, applications, databases, servers and operating systems when needed.

5 IT Security

Purpose: Prescribes information security protocols, controls, and safeguards required to maintain confidentiality, integrity, and availability of municipal systems and data based on risk assessments and recognized standards to guard against cyber threats.

5.1 Acceptable Encryption Standards

Purpose: Specifies approved advanced encryption algorithms, protocols, minimum key lengths, industry standards and implementation methods required when implementing cryptographic protection controls to secure highly sensitive or confidential municipal government data at rest, in transit, or for communications based on data classification risk assessments.

5.2 Password Security Standards

Purpose: Establishes baseline complexity requirements, rotation frequency, reuse prohibitions, failed login policies, multifactor authentication specifications, storage hashing parameters, and transmission encryption methods according to current industry recognized best practices for authentication credentials protecting access to municipal government systems.

5.3 Access Control Standards

Purpose: Provides detailed technical specifications and configurations for implementing least privilege role-based access control (RBAC), identity federation, authorization limitations, and separation of duties when granting access across diverse municipal government computing systems and resources based on assigned roles and data sensitivity.

5.4 Network Security Standards

Purpose: Defines baseline requirements, controls, protocols, perimeter defense capabilities, encryption mechanisms, redundancies, compensating controls and recommended technologies to implement layered network security defenses protecting all municipal government networks against both internal and external-based cybersecurity threats and attacks.

6 Compliance and Audits

Purpose: Validates alignment with legal, regulatory and policy mandates related to technology management and data protections through risk assessments, compliance audits, and evidence collection. Seeks to identify gaps, reduce deficiencies, and strengthen governance.

6.1 Compliance Requirements

Purpose: Identifies key regulatory compliance obligations, data types, infrastructure categories, agency reporting, technology usage standards and general security controls that invoke applicable federal, state and municipal statutes, regulations and ordinances which municipal government IT systems, networks, and data activities must adhere to.

6.2 Information Security Audits

Purpose: Outlines methodology, frequency, auditors, review categories, vulnerability probing restrictions, reporting formats and notification procedures for both internal self-assessments and third party audits evaluating the effectiveness of implemented security controls and adherence to policies for the municipal government's information security program. It seeks to identify gaps, policy violations and improvement opportunities.

7 Appendix

Purpose: Supplemental reference materials, links, supporting documents, guidelines and forms used in administering municipal government IT policies, standards and procedures. Enables lookup of additional details for carrying out technical, administrative and managerial tasks covered in Sections 2 through 6.

7.1 Glossary of Terms

Purpose: Provides definitions and explanations of key information technology and information security terminology, acronyms, and abbreviations used within municipal government IT policies, standards and procedures to ensure consistent understanding across documents.

Access Control - Managing access to resources and systems based on identity and authorized permissions.

Active Directory - Microsoft directory service managing permissions and access to resources.

Antivirus Software - Program designed to detect, stop and remove viruses and other malicious code.

Asset Management - The process of tracking, maintaining and protecting IT hardware and software assets.

Authentication - Verifying the identity of a user or system attempting access.

Backdoor - Undocumented way of gaining remote access to a system bypassing normal security controls.

Backup - Copying data to a second location to enable recovery in case of data loss.

Bandwidth - Maximum volume of data that can be transmitted over a network connection in a given time period.

Botnet - Network of compromised devices infected with malware allowing centralized remote control by an attacker.

BYOD - Bring Your Own Device; the practice of allowing employees to use personal mobile devices to access company data and systems.

Cloud Computing - Utilizing shared computing resources, software and information provided over the internet rather than local servers.

Cybersecurity - Protecting systems and data from digital attacks to ensure confidentiality, integrity and availability.

Data Breach - Unauthorized access, theft or release of sensitive information.

Data Classification - Categorizing data by sensitivity and business impact to determine protection requirements.

DDoS - Distributed Denial of Service; Malicious attempt to disrupt network traffic by overwhelming a target with fake requests.

DLP - Data Loss Prevention; controls to prevent unauthorized data exfiltration.

DMZ - Demilitarized Zone; a subnet segmenting an organization's internal network from the public internet.

DNS - Domain Name System; system that resolves human readable hostnames to machine IP addresses.

DoS - Denial of Service; cyber attack aiming to disrupt system and network availability.

Encryption - Encoding data in a form that can only be accessed by authorized parties.

Endpoint - Laptops, desktops, mobile devices and other systems used to access networks and applications.

Firewall - A network security system that monitors inbound and outbound traffic based on security rules.

Hacker - An unauthorized user that attempts to gain access to computer systems for malicious purposes.

Hash - Transforming a string into a fixed alphanumeric string using a cryptographic algorithm.

IDS - Intrusion Detection System; monitors networks and systems for malicious activity.

Information Security - Protecting the confidentiality, integrity and availability of data and systems through controls.

IP Address - Numerical internet protocol address uniquely identifying a computer system connected to a network.

IT - Information Technology; the infrastructure, systems, software, networking for managing and processing data.

LAN - Local Area Network linking computers within a facility or campus.

Log - Record of events, access or changes in a computer system stored sequentially.

Logic Bomb - Code intentionally inserted into a system to execute a malicious action when specified conditions are met.

Malware - Malicious software intended to compromise systems such as viruses, trojans, spyware.

MFA - Multifactor Authentication; Authentication using two or more proofs of identity.

NGFW - Next-Generation Firewall; Advanced network firewalls incorporating application data and intelligence.

Password - A secret string of text entered to authenticate and gain access to a computer system.

PCI DSS - Payment Card Industry Data Security Standard for handling credit cards.

Penetration Testing - Authorized simulated attacks against an environment to test security posture.

PHI - Protected Health Information regulated under HIPAA.

PII - Personally Identifiable Information that can identify an individual.

Ransomware - Malware that encrypts data until ransom is paid.

Router - Network device that forwards packets between networks using routing tables.

Server - A computer that provides data or services to other devices on a network.

Software - Programs and applications that run on computer systems and devices.

Spyware - Software that covertly monitors activity and sends data to interested parties.

SQL Injection - Code injection attack against databases.

SYSLOG - Standard for sending log messages across a network.

Trojan - Malware that misleads users about its true intent.

Virus - Malicious software that replicates itself to infect computer systems.

VLAN - Virtual Local Area Network used to isolate traffic on the same physical network.

VPN - Virtual Private Network; provides secure remote internet access to a local network.

Vulnerability - Security flaws or misconfigurations in systems that attackers can exploit.

WAF - Web Application Firewall; Protects web apps from attacks and applies security policies.

WAN - Wide Area Network that links networks across a large geographical area.

WLAN - Wireless Local Area Network - Network segment connected over WiFi rather than cabling.

Worm - Self-replicating malware that spreads itself automatically over networks.

XSS - Cross-Site Scripting; code injection attack against websites.

7.2 References

Purpose: Lists and provides links to specific laws, statutes, regulations, standards and guidance documents referenced in policies established within the municipal government IT policy manual to enable lookup of background information and validate compliance.

Information Security Standards and Frameworks

- ISO/IEC 27001 - Information security management systems requirements
<https://www.iso.org/standard/27001>
- NIST Cybersecurity Framework - Industry standards for critical infrastructure
<https://www.nist.gov/cyberframework>
- ISACA COBIT 2019 - IT governance and management framework
<https://www.isaca.org/resources/cobit>
- CIS Critical Security Controls - Top cyber defenses developed by experts
<https://www.cisecurity.org/controls>

Compliance Regulations

- PCI DSS - Payment Card Industry Data Security Standard
<https://www.pcisecuritystandards.org/>
- HIPAA - Health data privacy and security standards
<https://www.hhs.gov/hipaa/index.html>
- SOX - Financial data controls in Sarbanes-Oxley Act
<https://www.soxlaw.com/>
- GDPR - Data privacy regulations in EU
<https://gdpr.eu/>

Government Legislation

- FISMA - Federal Information Security Modernization Act
<https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act>
- FERPA - Student privacy protection regulations
<https://studentprivacy.ed.gov/ferpa>
- CCPA - California consumer data privacy protections
<https://oag.ca.gov/privacy/ccpa>

Municipal Government Guidelines

- National Institute of Standards in Technology IT Guidelines for Local Governments
<https://csrc.nist.gov/publications/detail/sp/800-100/final>
- Maine Notice of Risk to Personal Data Act
<https://www.mainelegislature.org/legis/statutes/10/title10ch210-Bsec0.html>

- Maine Criminal History Record Information Act
<https://legislature.maine.gov/statutes/16/title16ch7sec0.html>
- Maine Insurance Information and Privacy Protection Act
<https://www.mainelegislature.org/legis/statutes/24-A/title24-Ach24sec0.html>
- Maine Title 1, Chapter 13: PUBLIC RECORDS AND PROCEEDINGS
<https://legislature.maine.gov/statutes/1/title1ch13sec0.html>
- Maine Title 1, Chapter 14: ELECTRONIC ACCESS TO PUBLIC INFORMATION
<https://legislature.maine.gov/statutes/1/title1ch14sec0.html>
- Maine Title 1, Chapter 14-A: NOTICE OF INFORMATION PRACTICES
<https://legislature.maine.gov/statutes/1/title1ch14-Asec0.html>
- Maine Title 1, Chapter 14-B: DATA GOVERNANCE PROGRAM
<https://legislature.maine.gov/statutes/1/title1ch14-Bsec0.html>
- Maine Title 5: ADMINISTRATIVE PROCEDURES AND SERVICES Part 1: STATE DEPARTMENTS
Chapter 6: STATE ARCHIVIST §95-A. Protection and recovery of public records
<https://legislature.maine.gov/statutes/5/title5sec95-A.html>
- Maine Title 5: ADMINISTRATIVE PROCEDURES AND SERVICES Part 1: STATE DEPARTMENTS
Chapter 6: STATE ARCHIVIST §95-B. Local government records
<https://legislature.maine.gov/statutes/5/title5sec95-B.html>

Industry Best Practices

- ISACA Policy Templates for IT Governance
<https://www.isaca.org/resources/frameworks-standards-and-models>
- SANS Institute Information Security Policy Templates
<https://www.sans.org/information-security-policy/>

7.3 IT Forms and Templates

Purpose: Provides originals and instructions for consistent utilization of fillable forms, questionnaires, procedural checklists, configuration worksheets, and standard template documents referenced in defined municipal government IT procedures that enable operationalization of specific administrative, technical, and management processes.

- IT Equipment Request Form
- IT Software Request Form
- IT Remote Access Request Form
- IT Account Access Revocation Form
- New Employee IT Setup Request
- Employee Separation IT Checklist
- Vendor Access Request Form
- Guest WiFi Access Request Form
- BYOD Enrollment Request Form
- Change Management Request Form
- Change Approval/Rejection Notification
- Incident Response Form
- Major Incident Escalation Form
- IT Purchase Requisition Form
- IT Budget Request Form
- IT Policy Waiver Request Form
- Cloud Services Provisioning Request
- IT Project Request Form
- IT Asset Disposal/Surplus Request Form
- Vulnerability Scanning Waiver Form
- Loaner Equipment Sign-Out Form

Quit Claim Deeds

Board of Selectmen – Agenda Item Request Form

401 Webbs Mills Rd
Raymond ME 04071
204-655-4742 fax 207-655-3024
sue.look@raymondmaine.org

Requested Meeting Date:

Requested By & Date:

CONTACT INFORMATION

Address:

Email Address:

Phone #:

AGENDA ITEM REQUESTED

Agenda Item Subject:

Agenda Item Summary:

Action Requested/Recommendation: ☐ Approval ☐ Public Hearing ☐ Information Only

List of Attachments Included:

Maine Short Form Quit Claim Deed Without Covenant

THE INHABITANTS OF THE TOWN OF RAYMOND, a body politic located at Raymond, County of Cumberland and State of Maine, for consideration paid, releases to STANLEY SUSAN in said County and State, a certain parcel of land situated in the Town of Raymond, County of Cumberland, and State of Maine, being all and the same premises described at Map 015, Lot 078

The purpose of this conveyance is to release any interest which this grantor may have in and to the above premises by a lien filed for nonpayment of taxes on said parcel of land with reference being made to a lien filed against Map 015, Lot 078, in the name of STANLEY SUSAN and recorded in said Registry of Deeds

BK 33358	PG 303	BK 34141	PG 81	BK 35065	PG 47
BK 35913	PG 171	BK 37080	PG 74	BK 38553	PG 48
BK 39673	PG 111	BK 40312	PG 293		

IN WITNESS WHEREOF, the said INHABITANTS OF THE TOWN OF RAYMOND have caused this instrument to be sealed with its corporate seal and signed in its corporate name by JOSEPH BRUNO, ROLF OLSEN, SAMUEL GIFFORD, TERESA SADAK, AND DEREK RAY thereto duly authorized, this 10th day of October 2023.

THE INHABITANTS OF THE TOWN OF RAYMOND

_____	By: _____
Witness to All	JOSEPH BRUNO, Selectman

	ROLF OLSEN, Selectman

	SAMUEL GIFFORD, Selectman

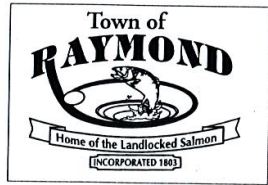
	TERESA SADAK, Selectman

	DEREK RAY, Selectman

STATE OF MAINE
CUMBERLAND, SS.

Personally, JOSEPH BRUNO, ROLF OLSEN, SAMUEL GIFFORD, TERESA SADAK, AND DEREK RAY appeared the aforesaid Selectmen known to me, this 10th day of October 2023 and acknowledged before me the foregoing instrument to be their free act and deed in their said capacity.

NOTARY



*401 Webb's Mills Road
Raymond, Maine 04071
207.655.4742
655-3024 (Fax)*

Tax Acquired Property

Name: STANLEY SUSAN

Map: 15

Lot: 78

Location: 184 MOUNTAIN RD

Foreclosure Date: FEBRUARY 15, 2018

Amount paid: \$ 9070.76

GRANTED DISABILITY

Maine Short Form Quit Claim Deed Without Covenant

THE INHABITANTS OF THE TOWN OF RAYMOND, a body politic located at Raymond, County of Cumberland and State of Maine, for consideration paid, releases to LIPTON MCKENNA CATHERINE in said County and State, a certain parcel of land situated in the Town of Raymond, County of Cumberland, and State of Maine, being all and the same premises described at Map 019, Lot 020B

The purpose of this conveyance is to release any interest which this grantor may have in and to the above premises by a lien filed for nonpayment of taxes on said parcel of land with reference being made to a lien filed against Map 019, Lot 020B, in the name of LIPTON MCKENNA CATHERINE and recorded in said Registry of Deeds

BK 34141	PG 34	BK 35065	PG 40	BK 35913	PG 94
BK 37079	PG 271	BK 38553	PG 24	BK 39673	PG 161
BK 40312	PG 254				

IN WITNESS WHEREOF, the said INHABITANTS OF THE TOWN OF RAYMOND have caused this instrument to be sealed with its corporate seal and signed in its corporate name by JOSEPH BRUNO, ROLF OLSEN, SAMUEL GIFFORD, TERESA SADAK, AND DEREK RAY thereto duly authorized, this 10th day of October 2023.

THE INHABITANTS OF THE TOWN OF RAYMOND

_____	By: _____
Witness to All	JOSEPH BRUNO, Selectman

	ROLF OLSEN, Selectman

	SAMUEL GIFFORD, Selectman

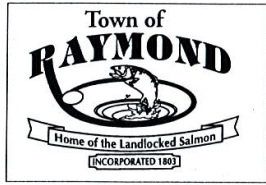
	TERESA SADAK, Selectman

	DEREK RAY, Selectman

STATE OF MAINE
CUMBERLAND, SS.

Personally, JOSEPH BRUNO, ROLF OLSEN, SAMUEL GIFFORD, TERESA SADAK, AND DEREK RAY appeared the aforesaid Selectmen known to me, this 10th day of October 2023 and acknowledged before me the foregoing instrument to be their free act and deed in their said capacity.

NOTARY



401 Webb's Mills Road
Raymond, Maine 04071
207.655.4742
655-3024 (Fax)

Tax Acquired Property

Name: LIPTON MCKENNA CATHERINE

Map: 19

Lot: 20B

Location: 382 NORTH RAYMOND RD

Foreclosure Date: JANUARY 7, 2019

Amount paid: \$ 4890.85

Sold property.

RSU #14 Referendum Question Warrant

**WARRANT AND NOTICE OF ELECTION
CALLING REGIONAL SCHOOL UNIT NO. 14 REFERENDUM
(20-A M.R.S. §§ 1501-04)**

TO: Mike Duffy, a resident of Regional School Unit No. 14, composed of the Towns of Raymond and Windham, State of Maine.

In the name of the State of Maine, you are hereby ordered to serve upon the municipal clerks of each of the municipalities within Regional School Unit No. 14, namely, the Towns of Raymond and Windham, an attested copy of this warrant and notice of election. Service shall be in hand within three (3) days of the date of this warrant and notice of election. The municipal clerks of the above municipalities shall immediately notify the respective municipal officers. The municipal officers shall meet forthwith and countersign this warrant and notice of election. The municipal officers shall provide below for the respective municipal clerks to post or have posted this warrant and notice of election.

**TOWN OF RAYMOND
REGIONAL SCHOOL UNIT NO. 14 REFERENDUM
WARRANT AND NOTICE OF ELECTION**

Cumberland County, ss.

State of Maine

TO: Mike Duffy, Resident of Regional School Unit No. 14: You are hereby required in the name of the State of Maine to notify the voters of this municipality of the election described in this warrant and notice of election.

TO THE VOTERS OF THE TOWN OF RAYMOND: You are hereby notified that a Regional School Unit No. 14 referendum election will be held at Jordan Small Middle School, 423 Webbs Mills Road in the Town of Raymond on Tuesday, November 7, 2023 for the purpose of determining the following question:

Question 1: Do you favor authorizing the School Board of Regional School Unit No. 14 (the "RSU") to issue bonds or notes in the name of RSU for school construction purposes in an amount not to exceed \$171,563,889 (the "Bonds") to construct and equip a new consolidated Grade 5 through Grade 8 middle school to be located at the site in Windham described below (the "Project"); and to acquire and convey such real estate interests for the Project as the School Board deems necessary?

- A. Project Location. The proposed site ("Proposed Site") is approximately 53 acres of land located on the southerly side of Windham Center Road and the easterly side of River Road. The Proposed Site will include the acquisition of the following land: (i) approximately 43.5 acres pursuant to an Option Agreement between the RSU and JDT Realty LLC; (ii) approximately 9 acres pursuant to a Property Exchange Agreement between the RSU and the Town of Windham; and (iii) approximately 1 acre pursuant to an Option Agreement between the RSU and the Presumpscot Regional Land Trust.

- B. Project to Consolidate and Replace Existing Middle Schools. The Project will create a single consolidated middle school for Grades 5 through 8. Space created by grade reconfiguration will provide the opportunity for universal Pre-K. The RSU will offer the two current middle schools, Jordan-Small Middle School and Windham Middle School, back to the towns in which they are located for community use or other disposition.
- C. Operating Cost Estimated Net Savings. The RSU estimates \$200,000 in annual net savings in operating costs attributable to the Project during each of the first two years.
- D. Responsibility for Bond Payments. The Project budget is \$171,563,889. The state-funded portion is \$131,725,445 (76.8%). The non-state-funded portion is \$39,838,444 (23.2%). The RSU is responsible for the local share of annual principal and interest payments for the Project included in the total cost of education appropriated pursuant to Title 20-A, section 15690, subsection 1, if any, and for the annual principal and interest payments for the non-state-funded portion of the Project.

The polls must be opened at 7:00 A.M. and closed at 8:00 P.M.

The Registrar of Voters will hold office hours while the polls are open to correct any error in or change a name or address on the voting list, to accept the registration of any person eligible to vote, and to accept new enrollments.

A person who is not registered as a voter may not vote in any election.

[SIGNATURE PAGE FOLLOWS]

This Warrant and Notice of Election given under our hand this day, October 4, 2023 at Windham, Maine.

Kate Bix
Christina Small
William Howard
Colewell
Mike Bridges

[Signature]
Adams
Jenna Burt
Jodi Canell

A majority of the School Board of Regional School Unit No. 14

A true copy of the Warrant and Notice of Election, attest:

[Signature]
Mike Duffy
Resident of
Regional School Unit No. 14

Countersigned this 10th day of October, 2023 at the Town of Raymond, Maine.

A majority of the municipal officers of the Town of Raymond

A true copy of the Warrant and Notice of Election, attest:

Sue Look, Municipal Clerk
Town of Raymond