Municipal IT and Cybersecurity Policy & Procedure Template

A practical policy framework for Maryland municipalities, towns, cities, villages, and related public entities

Prepared for	[Municipality Name]
Prepared by	Advantage Technology
Version	1.0 template
Draft date	June 2, 2026
Effective date	[Insert date after adoption]
Approved by	[Mayor / Council / Town Administrator / City Manager]

This template is designed for adaptation by local leadership, counsel, administration, IT, public safety, public works, finance, HR, and department heads. It is not legal advice and should be reviewed against local charter, ordinances, labor agreements, cyber insurance requirements, grant terms, and applicable Maryland and federal law before adoption.

Executive Use Note

Municipal governments run essential services with limited staff, public accountability, and increasing dependence on cloud platforms, endpoints, public-facing websites, public safety systems, finance systems, and citizen data. This template gives municipal leaders a practical policy baseline that can be adopted as a single policy manual or broken into individual policies.

The template is intentionally written in plain language. It avoids overengineering and focuses on the controls that reduce the most common municipal risks: account compromise, ransomware, unauthorized access, data loss, vendor exposure, weak backups, unmanaged devices, public records mishandling, and unclear incident communication.

How to use this template

- Replace bracketed fields such as [Municipality Name], [IT Lead], and [Information Security Officer].
- Have legal counsel review references to public records, retention, privacy, personnel matters, procurement, police records, public safety, utilities, election interfaces, and collective bargaining obligations.
- Decide whether this will be adopted by council resolution, executive policy, administrative procedure, or a combination of those mechanisms.
- Assign one accountable owner for annual review, exception handling, and evidence collection.
- Train employees on the final version and require signed acknowledgement for acceptable use, data handling, incident reporting, remote work, and device use.

Reference basis

This template aligns to common public-sector cybersecurity frameworks and current Maryland guidance, including:

Reference	Why it matters	Use in this template
NIST Cybersecurity Framework 2.0	Organizes cybersecurity outcomes around Govern, Identify, Protect, Detect, Respond, and Recover.	Used as the organizing model for governance, access, monitoring, response, and recovery.
Maryland DoIT Cybersecurity & Privacy Policy Suite	Maryland published a modernized policy suite in 2026 with governance, risk, asset, acceptable use, access, privacy, training, network security, monitoring, incident response, and continuity policies.	Used to mirror Maryland terminology and policy categories where practical for municipalities.
CISA Cybersecurity Performance Goals and Cyber Essentials	Provides baseline security practices for reducing common, high-impact cyber risk.	Used to keep the control set practical for small and mid-sized public entities.
Maryland Public Information Act and State Archives retention guidance	Municipal records must be managed for transparency, privacy, retention, and lawful disposition.	Used to separate public records handling from cybersecurity operations while ensuring they work together.
CIS / MS-ISAC resources for SLTT governments	Provides threat intelligence, incident response, advisories, peer collaboration, and SLTT-specific cybersecurity services.	Used to encourage information sharing and public-sector coordination.

Adoption options

- **Option A - Policy manual adoption:** Adopt this document as a municipal IT and cybersecurity policy manual, then publish department-level procedures separately.
- **Option B - Administrative policy:** Have the city manager, town administrator, or equivalent executive adopt this as an administrative policy and brief the mayor/council.
- **Option C - Phased adoption:** Adopt the highest-risk sections first: acceptable use, access control, MFA, incident reporting, backups, vendor security, and public records handling. Complete the remaining sections within 90 to 180 days.

Policy Catalog at a Glance

Policy Area	Primary Risk Reduced	Recommended Owner	Minimum Review Cadence
Governance and Accountability	Unclear ownership and inconsistent decisions	Mayor/Council and Municipal Administrator	Annual
Risk Management and Asset Inventory	Unknown systems and unmanaged exposure	IT Lead / Security Officer	Quarterly
Acceptable Use	Unsafe employee behavior and misuse of municipal resources	HR and Administration	Annual
Identity, Access, and MFA	Account takeover and unauthorized access	IT Lead	Quarterly
Data Protection, Privacy, and Records	Data loss, privacy exposure, PIA mistakes, retention failures	Clerk, Legal, IT, Department Heads	Annual

Endpoint, Mobile, and Remote Work	Lost devices, unmanaged devices, insecure remote access	IT Lead and HR	Semiannual
Email, Web, Social Media, and Communications	Phishing, website compromise, public misinformation	Communications Lead and IT	Annual
System, Network, Cloud, and Change Management	Misconfiguration and unpatched systems	IT Lead	Monthly to Quarterly
Backup, Continuity, and Recovery	Ransomware downtime and service disruption	Administration, IT, Finance, Public Safety	Quarterly
Incident Response and Reporting	Delayed response and uncontrolled communications	Municipal Administrator and Security Officer	Semiannual exercise
Vendor and Procurement Security	Third-party risk and unmanaged SaaS	Procurement, Legal, IT	Per purchase and annual
Training, Exceptions, and Enforcement	Policy gaps and inconsistent accountability	HR, Administration, IT	Annual

Core Definitions

Term	Definition
Municipality	The city, town, village, municipal corporation, authority, board, commission, or related public entity adopting this policy.
Municipal Data	Any data created, received, maintained, processed, stored, or transmitted for municipal business, regardless of format or location.
Confidential Data	Data that is not intended for public release and may include personnel records, tax records, police records, public safety information, resident information, credentials, legal records, financial information, security information, and protected vendor information.
Sensitive System	A system that supports finance, payroll, public safety, utilities, water/sewer, permits, public records, elections support, identity, email, website administration, backups, or other essential municipal services.
Privileged Account	Any account that can administer systems, modify security settings, access large amounts of data, approve payments, create users, change permissions, or bypass normal controls.
Cybersecurity Incident	An event that may compromise confidentiality, integrity, availability, privacy, municipal operations, public trust, or the security of data, systems, identities, or services.
Employee	For this policy, employee includes elected officials, staff, volunteers, interns, contractors, vendors, and anyone acting on behalf of the municipality when using municipal systems or data.
IT Lead	The internal or outsourced person responsible for technology operations, system administration, technical support, and coordination with vendors.
Information Security Officer	The internal or outsourced person responsible for cybersecurity governance, risk coordination, incident response coordination, policy maintenance, and security reporting.

1. Governance and Accountability Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To establish clear leadership accountability for technology, cybersecurity, privacy, public records, and resilience across the municipality.

Policy

- The municipality must treat cybersecurity as a municipal governance and operational risk, not only as an IT issue.
- The mayor, council, municipal administrator, clerk, finance lead, police/fire/public safety leadership, public works leadership, HR, legal counsel, IT, and the Information Security Officer must coordinate on technology risk decisions that affect public services or resident data.

- The municipality must designate an accountable IT Lead and an accountable Information Security Officer. These roles may be internal, outsourced, or combined for smaller municipalities, but accountability must be documented.
- Department heads are responsible for ensuring their teams follow technology and cybersecurity policies, report issues promptly, and support security reviews.
- Cybersecurity status must be briefed to executive leadership at least annually and after any significant incident, audit finding, major technology change, or cyber insurance renewal.
- Exceptions to this policy must be documented, risk reviewed, time limited, and approved by authorized municipal leadership.

Required Procedures

1. Maintain a current list of policy owners, system owners, department contacts, emergency contacts, IT vendors, cyber insurance contacts, law enforcement contacts, and incident response contacts.
2. Review the policy manual at least annually and document changes, approvals, and exceptions.
3. Include cybersecurity risk in budget planning, technology procurement, capital planning, public safety planning, and continuity planning.
4. Track open security findings, overdue remediation items, and accepted risks in a central register.
5. Require that new systems, applications, websites, domains, vendors, and cloud services receive IT and security review before purchase or production use.

Minimum Evidence to Retain

- Approved policy manual
- Named IT Lead and Information Security Officer
- Annual briefing minutes or leadership summary
- Risk register and exception log
- Policy acknowledgement records

2. Cyber Risk Management and Asset Inventory Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To ensure the municipality knows what technology it owns, who owns it, what data it handles, and which risks require action.

Policy

- The municipality must maintain a current inventory of hardware, software, cloud services, websites, domains, network equipment, public safety systems, finance systems, utility systems, and critical vendor platforms.
- Each critical system must have a named business owner and technical owner.
- Systems must be categorized by business impact, data sensitivity, internet exposure, regulatory requirements, and recovery priority.
- Risk decisions must consider resident services, public safety, legal obligations, financial exposure, privacy, cyber insurance requirements, and reputational impact.
- Material risks must be tracked until remediated, transferred, mitigated, or formally accepted by authorized leadership.

Required Procedures

6. Create and maintain an asset inventory covering computers, servers, mobile devices, network equipment, cloud applications, websites, domains, data repositories, and critical vendors.
7. Review the inventory at least quarterly and after procurement, disposal, migration, merger, department change, or incident.
8. Perform a cybersecurity risk review at least annually and when major systems are added or materially changed.

9. Prioritize remediation using impact to public services, known exploitation, internet exposure, privileged access, sensitive data, and backup/recovery dependency.
10. Report high and critical risks to leadership with recommended treatment options and budget impact.

Minimum Evidence to Retain

- Asset inventory
- Risk register
- System owner list
- Remediation plan
- Quarterly review evidence

3. Acceptable Use Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To define acceptable use of municipality-owned or municipality-managed technology resources and reduce misuse, unsafe behavior, and preventable security incidents.

Policy

- Municipal systems must be used for authorized municipal business, approved public service functions, and limited incidental personal use that does not interfere with work, security, legal obligations, or public trust.
- Employees must not use municipal systems to access illegal content, harassing content, discriminatory content, gambling platforms, unauthorized file sharing, personal commercial activity, or content that creates municipal liability.
- Employees must not attempt to bypass security controls, disable endpoint protection, share accounts, use another person's credentials, or connect unauthorized devices to municipal networks.
- Municipal email, chat, file storage, collaboration systems, and devices may be monitored, logged, reviewed, preserved, or disclosed as allowed by law and municipal policy.
- Employees must report suspected phishing, malware, lost devices, unauthorized access, accidental disclosure, and suspicious system behavior immediately.
- Use of personal email, personal cloud storage, personal messaging, or personal devices for municipal records or confidential municipal business is prohibited unless specifically approved and managed under policy.

Required Procedures

11. Provide this acceptable use policy to all employees before granting access to municipal systems.
12. Require signed acknowledgement at hiring, onboarding, appointment, or contract start, and at least annually afterward.
13. Review violations with HR, legal, administration, IT, and department leadership as appropriate.
14. Preserve logs and records related to investigations according to retention and legal hold requirements.
15. Disable access for users who create urgent security risk pending review by authorized leadership.

Minimum Evidence to Retain

- Signed acknowledgements
- Training records
- Violation review records
- Access suspension evidence where applicable

4. Identity, Access Control, and MFA Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors,

	boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To ensure access to municipal systems is authorized, traceable, least privileged, and promptly removed when no longer required.

Policy

- Every user must have a unique account. Shared accounts are prohibited unless formally approved for a documented system limitation and protected with compensating controls.
- Access must be based on job duties, department role, data sensitivity, and least privilege.
- Multi-factor authentication must be required for email, remote access, cloud services, privileged accounts, finance systems, HR systems, public safety administration systems, vendor portals, and other sensitive systems where technically available.
- Privileged accounts must be separate from standard user accounts unless a documented technical exception exists.
- Access must be approved before provisioning and removed immediately when employment, contract, appointment, role, or business need ends.
- Administrative access must be limited to authorized personnel and reviewed at least quarterly.
- Conditional access, location restrictions, device compliance, and sign-in risk controls should be used when available and appropriate.

Required Procedures

16. Require written approval from the department head or system owner before creating or modifying user access.
17. Use standard access groups by role wherever possible rather than assigning one-off permissions.
18. Review active users, privileged accounts, external users, service accounts, shared mailboxes, and high-risk groups at least quarterly.
19. Disable accounts immediately upon termination or loss of business need. Preserve records and mailboxes according to legal and retention requirements.
20. Investigate repeated failed login attempts, impossible travel, suspicious MFA prompts, unusual privilege changes, and access from unmanaged locations or devices.
21. Document any system that cannot support MFA or individual accounts and create a remediation or compensating-control plan.

Minimum Evidence to Retain

- Access request records
- Quarterly access review reports
- Privileged account list
- MFA coverage evidence
- Termination access removal checklist

5. Password and Authentication Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To protect municipal accounts from credential theft, guessing, reuse, phishing, and unauthorized access.

Policy

- Users must create strong passwords or passphrases and must not reuse municipal passwords on personal or third-party accounts.
- Passwords must not be shared, emailed, posted, stored in plain text, or given to supervisors, coworkers, vendors, or IT staff.
- Where technically supported, the municipality must block known compromised passwords and require MFA for higher-risk access.
- Default passwords must be changed before any system, network device, camera, IoT device, application, or cloud service is placed into production.
- Service account credentials, API keys, certificates, and secrets must be inventoried, protected, rotated when personnel or vendor risk changes, and removed when no longer needed.
- Password resets must verify the requestor's identity using a trusted method and must not rely only on email access from the same potentially compromised account.

Required Procedures

22. Set technical controls to enforce password length, lockout/rate limiting, MFA, and compromised password protection where available.
23. Use a managed password vault for administrative credentials, shared secrets, recovery keys, vendor access credentials, and emergency access credentials.
24. Require immediate password change and token/session revocation for suspected compromise.
25. Review service accounts and secrets at least annually and after vendor changes, staff changes, or incidents.
26. Document emergency access accounts and test their availability without using them for routine work.

Minimum Evidence to Retain

- Password standard settings
- MFA settings
- Password vault access list
- Service account inventory
- Emergency access account documentation

6. Data Protection, Privacy, Public Records, and Retention Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To protect municipal data while preserving transparency, lawful access, public records responsibilities, privacy, and retention obligations.

Policy

- Municipal data must be handled according to sensitivity, business purpose, legal obligations, public records requirements, privacy requirements, and retention schedules.
- Confidential data must be stored only in approved systems with appropriate access control, logging, backup, and retention capability.
- Employees must not store municipal records or confidential data in personal email, personal cloud accounts, unapproved USB drives, personal messaging apps, or unmanaged devices.
- The municipality must maintain procedures for responding to Maryland Public Information Act requests while protecting confidential, privileged, exempt, or restricted information.
- Records must be retained and disposed of according to approved retention schedules and legal hold requirements. Employees must not delete or alter records to avoid disclosure or retention obligations.

- Privacy risk must be considered before collecting new resident data, using new systems, adding online forms, changing public portals, or sharing data with vendors.
- Security information such as network diagrams, credentials, vulnerability reports, cyber insurance details, incident reports, and security configurations must be restricted to authorized personnel.

Required Procedures

27. Create a simple data classification model: Public, Internal, Confidential, and Restricted.
28. Map critical systems to the type of municipal data they store or process.
29. Coordinate PIA requests through the designated PIA representative, clerk, legal counsel, and system owners.
30. Apply legal holds promptly when litigation, investigation, incident response, audit, or public records obligations require preservation.
31. Review retention schedules before disposing of records, devices, backup media, email, archived data, or system exports.
32. Use encryption for laptops, mobile devices, backups, and confidential data transfers where technically available.
33. Review access to confidential repositories at least quarterly.

Minimum Evidence to Retain

- Data classification guide
- PIA representative listing
- Retention schedule references
- Legal hold records
- Confidential repository access reviews

7. Email, Collaboration, and Phishing Protection Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To reduce the likelihood and impact of phishing, business email compromise, malware, accidental disclosure, and unauthorized use of municipal communications platforms.

Policy

- Municipal email and collaboration tools must be managed through approved platforms with MFA, anti-phishing controls, spam filtering, malware protection, and retention support.
- Employees must report suspicious emails, attachments, links, payment instructions, credential requests, gift card requests, wire transfer requests, and urgent or unusual communications.
- Employees must verify financial instructions, bank changes, vendor payment changes, payroll changes, and sensitive data requests using an out-of-band trusted method.
- Auto-forwarding municipal email to personal accounts is prohibited unless approved for a documented business need and reviewed by IT and legal counsel.
- Shared mailboxes, distribution lists, group chats, Teams/SharePoint workspaces, and similar collaboration spaces must have assigned owners and reviewed membership.
- Public meeting records, council communications, resident correspondence, and official decisions must be handled in accordance with records and PIA requirements.

Required Procedures

34. Configure email protection, malware scanning, safe links or equivalent protections, attachment controls, and external sender warnings where appropriate.
35. Train users on phishing reporting and payment fraud verification procedures.
36. Review mail flow rules, forwarding rules, delegated mailbox access, shared mailbox permissions, and external guest access at least quarterly.

37. Investigate suspicious inbox rules, unexpected forwarding, mass deletion, credential prompts, impossible travel, and unusual mailbox access.
38. Maintain a documented payment-change verification procedure with finance and procurement.

Minimum Evidence to Retain

- Email protection configuration
- Phishing training records
- Phishing reports
- Mailbox permission reviews
- Payment verification procedure

8. Endpoint, Mobile Device, and Removable Media Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To protect laptops, desktops, tablets, phones, removable media, and field devices used for municipal work.

Policy

- Municipality-owned computers and mobile devices must be inventoried, secured, patched, monitored, encrypted where technically available, and protected by approved endpoint security tools.
- Only approved and properly licensed software may be installed on municipal devices.
- Employees must not disable security tools, remove management agents, alter configurations, or install unauthorized software or browser extensions.
- Lost, stolen, damaged, or suspicious devices must be reported immediately.
- Removable media such as USB drives must be restricted, encrypted when used for confidential data, scanned for malware, and avoided when secure file transfer is available.
- Personal devices may not access confidential municipal data unless explicitly approved and protected under mobile device management, conditional access, or equivalent controls.
- Devices used by public safety, field staff, utilities, and public works must be secured according to operational needs and may require additional protections due to field exposure.

Required Procedures

39. Maintain a device inventory with assigned user, department, device type, serial number, operating system, encryption status, endpoint protection status, and disposal status.
40. Apply operating system and application patches on a defined schedule, with expedited action for actively exploited or critical vulnerabilities.
41. Configure endpoint detection, antivirus/anti-malware, disk encryption, screen lock, remote wipe where available, and standard security baselines.
42. Approve and document any exception for unsupported systems, public kiosks, shared devices, police/utility specialty devices, or legacy equipment.
43. Sanitize or destroy storage media before disposal, reassignment, return to vendor, or recycling.

Minimum Evidence to Retain

- Device inventory
- Patch reports
- Endpoint protection reports
- Encryption reports
- Lost device records
- Disposal certificates

9. Remote Work, Telework, and Remote Access Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To ensure remote work and remote administration do not expose municipal systems or data to unnecessary risk.

Policy

- Remote access to municipal systems must use approved methods, MFA, encryption, logging, and least privilege.
- Employees must not access confidential municipal data from public computers, shared personal devices, or unmanaged networks without approved protections.
- Remote administration tools must be approved, inventoried, restricted, logged, and disabled when no longer required.
- Vendors must not have persistent unattended access to municipal systems unless there is a documented business need, technical control, and owner approval.
- Employees working remotely must protect municipal devices and records from household members, visitors, theft, loss, and unauthorized viewing.
- Remote work does not change public records, retention, confidentiality, incident reporting, or acceptable use obligations.

Required Procedures

44. Approve remote access based on job role, system need, device compliance, MFA status, and data sensitivity.
45. Review remote access users, VPN users, remote support tools, vendor accounts, and privileged remote access at least quarterly.
46. Disable remote access promptly when employment, vendor work, project need, or emergency need ends.
47. Require secure storage and transport of municipal devices and paper records during telework.
48. Investigate remote access from unusual locations, unmanaged devices, impossible travel, or outside expected work patterns.

Minimum Evidence to Retain

- Remote access approval records
- VPN and remote support user reviews
- MFA enforcement evidence
- Vendor access review
- Remote work acknowledgement

10. System, Network, Cloud, and Configuration Security Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To establish baseline controls for municipal infrastructure, cloud services, networks, servers, applications, domains, websites, and specialty systems.

Policy

- Systems must be securely configured before production use and maintained according to approved baselines where available.
- Critical systems must be segmented or otherwise protected to limit the impact of compromise.
- Public-facing systems, websites, portals, remote access points, and cloud services must be inventoried, monitored, patched, and reviewed for exposure.
- Administrative interfaces must not be exposed to the public internet unless required, risk reviewed, protected by MFA, and approved.
- Logging must be enabled for identity, endpoint, email, firewall, VPN, cloud administration, finance systems, and other sensitive systems where technically available.
- DNS, domain names, websites, SSL/TLS certificates, registrar accounts, and website administrative accounts must be owned and controlled by the municipality, not by a single employee or vendor without oversight.
- Specialty environments such as police systems, CJIS-related systems, body camera systems, water/sewer/SCADA, building access, cameras, and public safety systems must follow additional applicable requirements.

Required Procedures

49. Maintain network diagrams, system inventories, cloud tenant inventories, website/domain inventories, and administrative access lists.
50. Review internet-facing services at least quarterly and after firewall, VPN, cloud, DNS, or website changes.
51. Apply configuration baselines to servers, endpoints, cloud services, network devices, and SaaS platforms where practical.
52. Enable logging and alerting for account compromise, administrator changes, malware detection, firewall events, suspicious email activity, backup failures, and high-risk cloud activity.
53. Restrict administrative access by role, source, MFA, device compliance, and just-in-time approval where available.
54. Review DNS records, domain registration, website platform ownership, certificate expiration, and website administrator accounts at least annually.

Minimum Evidence to Retain

- Network diagram
- Cloud tenant inventory
- Website and domain inventory
- Configuration review evidence
- Firewall/VPN review
- Logging and alerting reports

11. Patch, Vulnerability, and Change Management Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To reduce preventable compromise caused by known vulnerabilities, unsupported systems, uncontrolled changes, and configuration drift.

Policy

- Municipal systems must be patched on a defined schedule based on risk, business impact, vendor support, and exploit activity.
- Critical and actively exploited vulnerabilities must be prioritized for expedited remediation or documented compensating controls.
- Unsupported operating systems, applications, network devices, cameras, phone systems, websites, or specialty systems must be upgraded, isolated, replaced, or formally risk accepted.

- Material technology changes must be planned, reviewed, approved, tested where practical, documented, and reversible where possible.
- Emergency changes may be made to protect public services or security, but must be documented and reviewed after the fact.
- Vulnerability scanning or equivalent assessment must be performed on a recurring schedule appropriate to municipal size and exposure.

Required Procedures

55. Maintain a patch calendar for workstations, servers, network equipment, firewalls, cloud services, websites, and critical applications.
56. Track patch compliance and vulnerability remediation with priority, owner, due date, and closure evidence.
57. Review critical vulnerabilities weekly when alerts are issued and at least monthly during routine operations.
58. Use a change request process for firewall changes, remote access changes, identity changes, email security changes, website changes, new applications, and critical system changes.
59. Maintain a list of unsupported or exception systems and review it at least quarterly.
60. Test restoration or rollback plans for high-risk changes where practical.

Minimum Evidence to Retain

- Patch reports
- Vulnerability scan reports
- Change records
- Unsupported system register
- Emergency change review records

12. Backup, Continuity, and Disaster Recovery Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To ensure the municipality can recover essential services after ransomware, accidental deletion, equipment failure, vendor outage, natural disaster, or other disruption.

Policy

- Critical municipal systems and data must be backed up according to documented recovery requirements.
- Backups must be protected from deletion, encryption, tampering, and unauthorized access, including protection from compromised administrator accounts where possible.
- Backup coverage must include servers, critical cloud data, finance data, public records, public safety administration data, utility data, website content, and other systems required for municipal operations.
- Recovery priorities must be documented for essential services, including emergency communications, public safety, finance/payroll, email, public notices, permits, utilities, and council operations.
- Restoration testing must be performed at least quarterly for critical data or systems and after major changes.
- Continuity plans must identify manual workarounds when systems are unavailable.

Required Procedures

61. Define recovery time objectives and recovery point objectives for critical systems.
62. Maintain a backup inventory showing what is backed up, frequency, retention, storage location, encryption, immutability or deletion protection, and responsible owner.
63. Review backup success and failure reports at least weekly for critical systems.
64. Perform documented restoration tests at least quarterly for high-value systems and at least annually for all critical systems.

65. Store incident response, vendor contacts, recovery procedures, insurance contacts, and emergency access information in a secure location accessible during an outage.
66. Review continuity and disaster recovery plans with department heads at least annually.

Minimum Evidence to Retain

- Backup inventory
- Backup success reports
- Restoration test records
- Recovery priority list
- Continuity plan
- Emergency contact list

13. Cybersecurity Incident Response and Reporting Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To ensure cybersecurity incidents are reported quickly, contained effectively, communicated appropriately, and handled with legal, operational, public safety, privacy, and public trust considerations.

Policy

- Employees must immediately report suspected cybersecurity incidents, lost devices, accidental disclosure, suspicious login activity, phishing, malware, ransomware, unauthorized access, vendor compromise, website defacement, payment fraud, and unusual system behavior.
- The municipality must maintain an incident response team with defined roles for executive decision making, IT/security response, legal, communications, HR, finance, department operations, and public safety where applicable.
- Incident communications must be coordinated through authorized leadership. Employees must not independently contact the media, post incident details, or disclose sensitive security information unless authorized.
- Incident response must preserve evidence, logs, impacted systems, emails, and relevant records when possible and lawful.
- The municipality must coordinate with cyber insurance, legal counsel, law enforcement, Maryland cyber reporting channels, affected vendors, and other required parties as appropriate.
- After material incidents, the municipality must complete an after-action review and remediation plan.

Required Procedures

67. Maintain a current incident response contact list and escalation procedure.
68. Train employees on what to report and how to report it.
69. Use an incident severity model to determine response urgency, leadership notification, insurance notification, legal involvement, and public communication requirements.
70. During suspected compromise, preserve relevant logs and isolate affected systems where directed by IT/security.
71. Use pre-approved communication templates for internal notifications, vendor requests, resident updates, elected official briefings, and media statements.
72. Perform at least one tabletop exercise annually and after major technology changes.

Minimum Evidence to Retain

- Incident response plan
- Contact list
- Incident tickets or reports
- After-action reports
- Tabletop exercise records

- Communication approvals

14. Vendor, Contractor, and Procurement Security Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To reduce technology and data risk introduced by vendors, contractors, hosted services, cloud applications, consultants, managed service providers, website providers, payment processors, public safety vendors, and other third parties.

Policy

- Technology purchases, renewals, websites, cloud services, applications, managed services, public safety platforms, and vendors with access to municipal systems or data must receive IT/security review before approval.
- Contracts must define security responsibilities, data ownership, confidentiality, breach notification, access control, backup, retention, subcontractor use, support obligations, termination assistance, and return or destruction of data where applicable.
- Vendors must use unique accounts and MFA for access to municipal systems where technically available.
- Vendor remote access must be limited to approved purposes, systems, and timeframes, and must be logged where possible.
- The municipality must know where municipal data is stored, who can access it, how it is protected, how it is backed up, how it can be exported, and how it is deleted or returned at contract end.
- High-risk vendors must be reviewed at least annually or before renewal.

Required Procedures

73. Use a vendor security intake checklist before procurement or renewal.
74. Identify vendors that store confidential data, process payments, administer systems, host public websites, provide public safety functions, manage backups, or connect to municipal networks.
75. Request appropriate security documentation such as SOC reports, cyber insurance evidence, incident notification commitments, vulnerability management statements, data location, backup capability, MFA support, and subcontractor information.
76. Disable vendor access immediately when work ends, contracts expire, personnel change, or risk is identified.
77. Ensure procurement and legal counsel involve IT/security before signing technology contracts or renewals.

Minimum Evidence to Retain

- Vendor inventory
- Vendor intake checklist
- Security review records
- Contract security terms
- Vendor access review
- Renewal risk review

15. Technology Procurement, Software, SaaS, and AI Use Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To ensure the municipality does not unintentionally create risk through unapproved applications, cloud services, browser extensions, artificial intelligence tools, online forms, or citizen-facing platforms.

Policy

- Employees must not purchase, subscribe to, install, connect, or use software, SaaS, AI tools, browser extensions, websites, online forms, or cloud services for municipal work without approval through the municipality's technology review process.
- Municipal data must not be entered into public AI tools or unapproved platforms when the data is confidential, restricted, privileged, personnel-related, law enforcement-related, financial, security-sensitive, export-controlled, resident-specific, or otherwise not intended for public release.
- AI-generated content used for official municipal business must be reviewed by a qualified human before use, publication, decision making, resident communication, legal action, financial action, or public record creation.
- The municipality must maintain ownership and administrative control over its websites, domains, social media accounts, online forms, data repositories, SaaS platforms, and public communication channels.
- Online services that collect resident information must be reviewed for privacy, retention, accessibility, security, data export, and public records implications.

Required Procedures

78. Create a technology request form for new software, SaaS, AI, online forms, websites, payment tools, integrations, and data-sharing platforms.
79. Review each request for business need, data sensitivity, access control, MFA, logging, data ownership, retention, backup, vendor risk, cost, support, and exit strategy.
80. Maintain an approved software and SaaS inventory.
81. Block or remove unapproved tools that create security, privacy, legal, or operational risk.
82. Train employees on approved AI use and prohibited data entry into unapproved tools.

Minimum Evidence to Retain

- Technology request forms
- Approved software list
- SaaS inventory
- AI use guidance
- Online form review records

16. Physical Security and Environmental Protection Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To protect municipal technology, records, network equipment, public safety systems, and facilities from unauthorized physical access, theft, damage, and environmental hazards.

Policy

- Network closets, server rooms, dispatch technology areas, camera systems, backup media, finance records, public safety records, and other sensitive areas must be physically secured.
- Only authorized personnel may access areas containing critical technology, confidential records, or public safety systems.
- Visitors, contractors, and vendors must be escorted or authorized before accessing sensitive areas.
- Environmental risks such as heat, water, power failure, fire, poor cabling, blocked ventilation, and unsecured equipment must be corrected or tracked as risks.

- Paper records and removable media containing confidential information must be secured when not in use.
- Physical keys, access cards, door codes, alarm codes, and camera administration must be managed and revoked when no longer needed.

Required Procedures

83. Maintain an access list for server rooms, network closets, records storage, public safety technology rooms, and other sensitive areas.
84. Review physical access at least annually and after staffing, contractor, or facility changes.
85. Ensure critical network and server equipment has appropriate power protection, ventilation, cable management, and environmental monitoring where needed.
86. Lock unattended municipal devices and secure portable devices during travel, field work, and public meetings.
87. Document physical security incidents, lost keys/cards, unauthorized access, and environmental issues.

Minimum Evidence to Retain

- Physical access list
- Facility review checklist
- Key/card inventory
- Environmental issue log
- Visitor/vendor access records

17. Security Awareness and Workforce Training Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To ensure employees understand their responsibilities and can recognize common threats to municipal systems, data, and public services.

Policy

- All employees with access to municipal systems must receive cybersecurity and privacy awareness training at onboarding and at least annually.
- Training must cover phishing, MFA, password safety, acceptable use, incident reporting, data handling, public records, payment fraud, remote work, mobile devices, and vendor/social engineering risks.
- Users with elevated risk roles must receive role-based training. This includes finance, HR, clerks, police/public safety administration, public works/utilities, department heads, elected officials, IT administrators, website administrators, and users with privileged access.
- Phishing simulations or practical exercises should be used where appropriate to reinforce reporting behavior, not to shame employees.
- Employees who repeatedly miss training or create elevated risk may have access restricted until corrective action is complete.

Required Procedures

88. Maintain a training plan with required courses, target audiences, frequency, and completion tracking.
89. Assign training during onboarding before or shortly after access is granted.
90. Track completion and report overdue training to department heads and administration.
91. Provide targeted reminders after incidents, phishing campaigns, audit findings, or major policy updates.
92. Train elected officials and department heads on governance responsibilities and incident communication expectations.

Minimum Evidence to Retain

- Training plan

- Completion reports
- Role-based training records
- Phishing exercise reports
- Corrective action records

18. Website, Domain, Social Media, and Public Communications Security Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes
Policy Status	Template language for municipal review and adoption

Purpose

To protect the municipality's public digital presence, official communications, domain names, online forms, and citizen-facing services.

Policy

- Municipal websites, domains, DNS, SSL/TLS certificates, social media accounts, online forms, and resident portals must have documented ownership, administrative access, MFA where available, and backup or recovery procedures.
- Official municipal social media accounts must be controlled by the municipality, not a personal account, and must have at least two authorized administrators where the platform allows.
- Public website content, emergency notices, council information, public meeting materials, and resident communications must follow approval, accessibility, retention, and public records procedures.
- Website vendors and marketing vendors must not be the sole holders of domain registrations, hosting credentials, DNS control, or website administrative credentials.
- Online forms must not collect confidential or sensitive information unless reviewed and approved for privacy, security, retention, and data routing.
- Security incidents affecting public communications, websites, domains, or social media must be escalated as cybersecurity incidents.

Required Procedures

93. Maintain an inventory of domains, DNS providers, website hosts, content management systems, registrars, certificates, social media accounts, online forms, and administrators.
94. Review public-facing accounts and administrators at least quarterly.
95. Use MFA for website, registrar, DNS, social media, and resident portal administration where available.
96. Back up website content or maintain recovery capability for critical public information.
97. Review online forms before use and confirm where submitted data is stored, who receives it, and how long it is retained.

Minimum Evidence to Retain

- Domain and website inventory
- Social media admin list
- Certificate expiration tracker
- MFA evidence
- Online form review records

19. Enforcement, Exceptions, and Policy Maintenance Policy

Policy Owner	Municipal Administrator / City Manager, IT Lead, and Information Security Officer
Applies To	Elected officials, employees, volunteers, interns, contractors, vendors, boards, commissions, and any person or entity with access to municipality systems or data
Review Frequency	Annual, and after material technology, legal, or risk changes

Policy Status	Template language for municipal review and adoption

Purpose

To ensure cybersecurity requirements are applied consistently, exceptions are managed transparently, and policies remain current.

Policy

- Failure to follow this policy may result in corrective action, access restriction, disciplinary action, contract remedies, or other action consistent with law, personnel policies, and contractual obligations.
- Security exceptions must be documented with business justification, risk, compensating controls, expiration date, and approval authority.
- Exceptions must not be permanent by default and must be reviewed at least annually.
- Policy conflicts, unclear requirements, or operational limitations must be escalated to administration, IT, security, HR, and legal counsel as appropriate.
- This policy manual must be reviewed annually, after significant incidents, after major technology changes, after major legal or regulatory changes, and before cyber insurance renewal where practical.

Required Procedures

98. Maintain a policy exception register with owner, risk, compensating controls, expiration, and approval status.
99. Review exceptions at least quarterly for high-risk exceptions and annually for all exceptions.
100. Document enforcement actions according to HR, legal, and procurement procedures.
101. Update the policy manual when standards, systems, vendors, laws, grant requirements, cyber insurance requirements, or risk conditions materially change.
102. Provide updated training or acknowledgement when policy changes materially affect employees.

Minimum Evidence to Retain

- Exception register
- Policy revision history
- Enforcement records where applicable
- Annual review record
- Updated acknowledgements

Procedure Templates

The following procedure templates are designed to be copied into municipal operating procedures, department manuals, onboarding/offboarding checklists, incident response runbooks, and vendor intake processes.

A. New User Access Procedure

103. Department head submits access request with employee name, role, start date, department, supervisor, systems needed, groups needed, device needed, and whether remote access is required.
104. HR or administration confirms employment, appointment, volunteer role, or contract status.
105. IT provisions unique account, MFA, device assignment, email, required applications, and role-based permissions.
106. User completes acceptable use acknowledgement, basic security training, and any role-specific training before full access is granted where practical.
107. IT records provisioning details in the access system, ticketing system, or onboarding checklist.

B. Role Change Access Procedure

108. Supervisor notifies IT, HR, and administration before role changes take effect where practical.
109. System owners review current access against the new role.
110. IT removes access that is no longer needed before adding new access whenever possible.
111. Privileged access requires separate approval and must be reviewed within 30 days after role change.
112. Access review evidence is stored with the personnel or access record according to retention requirements.

C. Termination and Offboarding Procedure

113. HR, administration, or department head notifies IT immediately of termination, resignation, appointment end, contractor end, vendor end, or leave requiring access removal.
114. IT disables accounts, revokes sessions/tokens, removes remote access, disables MFA methods, and blocks privileged access at the required time.
115. Municipal devices, keys, access cards, badges, removable media, records, and credentials are recovered or documented as missing.
116. Mailboxes, files, records, and department data are preserved or transferred according to legal, retention, and business requirements.
117. Vendor and SaaS access associated with the user is removed or transferred.

D. Lost or Stolen Device Procedure

118. Employee immediately reports the loss to supervisor and IT/security, including last known location, device type, whether confidential data may be present, and whether police report is needed.
119. IT attempts remote lock, wipe, tracking, session revocation, password reset, and account review where available.
120. Information Security Officer determines whether confidential data, public safety data, resident data, or credentials may have been exposed.
121. Legal, HR, cyber insurance, and leadership are notified when privacy, security, or reporting obligations may apply.
122. Incident record is closed only after containment, recovery, replacement, and lessons learned are documented.

E. Cyber Incident Initial Response Procedure

123. Receive report and record who reported it, when, what happened, affected systems, observed indicators, screenshots, messages, and immediate business impact.
124. Classify severity as Low, Moderate, High, or Critical based on data exposure, public service impact, public safety impact, ransomware indicators, privilege compromise, or public visibility.
125. Contain using approved steps such as isolating device, disabling account, revoking sessions, blocking malicious sender, blocking network traffic, preserving logs, and notifying vendor support.
126. Escalate to municipal leadership, legal counsel, cyber insurance, incident response provider, Maryland cyber reporting channel, law enforcement, or other parties based on severity and obligation.
127. Coordinate internal and external communications through authorized leadership. Do not speculate publicly.
128. Document root cause, scope, remediation, recovery, notifications, costs, downtime, and after-action improvements.

F. Payment Change and Fraud Verification Procedure

129. Any request to change banking, payment instructions, vendor contact, payroll destination, or wire/ACH details must be verified through a trusted phone number already on file, not through the request email.
130. Finance staff must obtain secondary approval for payment changes above a defined threshold.
131. Suspicious payment requests must be reported to finance leadership, IT/security, and administration immediately.
132. Email thread history, attachments, phone verification notes, and approval records must be retained according to finance and records requirements.

G. Backup Restoration Test Procedure

133. Select system, dataset, or mailbox for test based on criticality and rotation schedule.
134. Confirm backup exists, date/time of backup, retention point, storage location, and responsible owner.
135. Restore to a test location or approved alternate location without overwriting production data unless part of an approved recovery exercise.
136. Validate that restored files, permissions, application data, and dependencies are usable.
137. Document result, time required, issues found, corrective actions, and next test date.

H. Vendor Security Intake Procedure

138. Identify what municipal data the vendor will access, where it will be stored, and whether the vendor will connect to municipal systems.
139. Confirm whether MFA, logging, encryption, backups, data export, breach notification, subcontractor controls, and administrative control are available.
140. Review contract terms for data ownership, confidentiality, security responsibilities, breach notification, termination assistance, insurance, and data return or destruction.
141. Assign a municipal business owner and technical owner before the service is approved.

142. Add the vendor to the vendor inventory and schedule renewal review.

Employee Acknowledgement Template

I acknowledge that I have received, read, and understand the [Municipality Name] Municipal IT and Cybersecurity Policy & Procedure Template, including acceptable use, data protection, incident reporting, remote work, device use, and public records responsibilities. I understand that municipal systems and data must be used only as authorized and that violations may result in corrective action, access restriction, disciplinary action, contract remedies, or other action consistent with law and municipal policy.

Name	
Role / Department	
Signature	
Date	
Supervisor / Witness if required	

Municipal Cybersecurity Annual Review Checklist

Governance

Item	Complete	Owner	Notes / Evidence
Policy owner confirmed	[ ]		
Information Security Officer confirmed	[ ]		
Annual leadership briefing completed	[ ]		
Exception register reviewed	[ ]		
Cyber insurance requirements reviewed	[ ]		

Identity and Access

Item	Complete	Owner	Notes / Evidence
MFA coverage reviewed	[ ]		
Privileged accounts reviewed	[ ]		
Terminated users removed	[ ]		
Vendor accounts reviewed	[ ]		
Shared accounts documented or eliminated	[ ]		

Systems and Data

Item	Complete	Owner	Notes / Evidence
Asset inventory updated	[ ]		
Critical systems identified	[ ]		
Confidential data repositories reviewed	[ ]		
Retention schedules confirmed	[ ]		
Public records process reviewed	[ ]		

Operations

Item	Complete	Owner	Notes / Evidence
Patch reports reviewed	[ ]		
Backup reports reviewed	[ ]		
Restore test completed	[ ]		
Vulnerability remediation tracked	[ ]		
Change process followed	[ ]		

Incident Readiness

Item	Complete	Owner	Notes / Evidence
Incident contact list updated	[ ]		

Cyber insurance contact verified	[ ]		
Tabletop exercise completed	[ ]		
Public communication template reviewed	[ ]		
After-action items closed	[ ]		

Vendors and Procurement

Item	Complete	Owner	Notes / Evidence
Vendor inventory updated	[ ]		
High-risk vendors reviewed	[ ]		
Contract security terms checked	[ ]		
Vendor remote access reviewed	[ ]		
SaaS inventory reconciled	[ ]		

Optional Council Resolution Language

The following language is a starting point only and must be reviewed by municipal legal counsel before use.

> WHEREAS, [Municipality Name] relies on information technology systems, digital records, communications platforms, public websites, and third-party service providers to deliver municipal services;
>
> WHEREAS, cybersecurity incidents may affect public services, resident data, public trust, financial operations, public safety, legal obligations, and the continuity of municipal operations;
>
> WHEREAS, the municipality desires to establish clear expectations for acceptable use, access control, data protection, incident reporting, vendor oversight, backup and recovery, and cybersecurity governance;
>
> NOW, THEREFORE, BE IT RESOLVED that [Municipality Name] adopts the Municipal IT and Cybersecurity Policy & Procedure Template, as amended for local use, and directs the [Municipal Administrator / City Manager / Town Administrator / Clerk] to implement, maintain, and review the policy in coordination with department heads, IT, legal counsel, and other appropriate officials.

Reference Links

- NIST Cybersecurity Framework 2.0 overview: https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework
- Maryland DoIT Cybersecurity & Privacy Policy Suite: https://doit.maryland.gov/policies/ci/Pages/default.aspx
- Maryland DoIT Office of Security Management: https://doit.maryland.gov/About-DoIT/Offices/Office-of-Security-Management/Pages/default.aspx
- CISA Cybersecurity Performance Goals: https://www.cisa.gov/cybersecurity-performance-goals-cpgs
- CISA Cyber Essentials: https://www.cisa.gov/resources-tools/resources/cyber-essentials
- CISA StopRansomware Guide: https://www.cisa.gov/stopransomware/ransomware-guide
- Maryland Public Information Act information: https://www.marylandcomptroller.gov/about/comptroller/pia.html
- Maryland State Archives retention schedules: https://msa.maryland.gov/msa/intromsa/html/record_mgmt1/toc.html
- CIS MS-ISAC: https://www.cisecurity.org/ms-isac