Incident Response Policy

Municipality of Hastings Highlands- Corporate Policies and Procedures			
DEPARTMENT: Administration Department			**POLICY #:**
POLICY: Incident Response Policy			
DATE: November 19, 2025	**REV. DATE:**	**COVERAGE:** Municipal Staff, Members of Council, and Volunteers	**PAGE #:** 1-4

1.0 Policy Statement:

The Municipality of Hastings Highlands is committed to protecting the confidentiality, integrity, and availability of its information systems and data. This Incident Response Policy establishes the framework for detecting, reporting, assessing, and responding to cyber information security incidents in a timely and coordinated manner.

The purpose of this policy is to minimize the impact of security incidents on municipal operations, limit potential damage, reduce recovery time and associated costs, and prevent recurrence through continuous improvement of security practices.

This policy applies to all employees, contractors, and third-party vendors who access, manage, or store municipal information assets across all platforms and systems. Compliance with this policy supports the Municipality's obligations under applicable legislation, including the *Municipal Act, Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), and the *Emergency Management and Civil Protection Act.*

2.0 Purpose:

The purpose of this policy is to define the process for detecting, reporting, assessing, and responding to information security incidents. The goal is to limit damage, reduce recovery time and costs, and prevent future incidents.

3.0 Scope:

This policy applies to:

- All employees, contractors, and third-party vendors.
- All organizational information systems (on-premises, cloud, mobile).
- All data types, including personally identifiable information (PII) and personal health information (PHI), financial data, and intellectual property.

4.0 Definitions:

- **Security Incident**: Any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.
- **Incident Response Team (IRT)**: The team responsible for managing the incident lifecycle. This would include the Municipal Emergency Control Group (MECG) and Hastings County IT representatives.
- **Containment**: Short-term and long-term actions taken to limit the scope and impact.
- **Eradication**: The process of removing the root cause and related artifacts of the incident.
- **IT Security Team**: Comprised of Hastings County IT support team and external 3rd party IT security teams

5.0 Roles and Responsibilities:

Role	**Responsibilities**
Incident Response Team (IRT) –	Lead and coordinate incident response efforts.
IT Security Team –	Investigate, contain, eradicate, and recovery systems.
Employees, Council, & Volunteers –	Report any suspected incidents immediately.
Municipal Emergency Control Group –	Provide support for legal, regulatory, and communication needs.

6.0 Incident Response Lifecycle:

Incident handling follows the NIST (the widely adopted “National Institute of Standards and Technology”) framework:

a. Preparation

- Maintain updated contact lists.
- Train staff on incident reporting procedures.
- Deploy security systems and monitoring tools.

b. Detection and Analysis

- Detect incidents via monitoring tools or user reports.
- Classify and prioritize based on severity and impact.

c. Containment, Eradication and Recovery

- Implement short-term actions (e.g., isolate affected systems).
- Plan long-term containment strategies to avoid reinfection.
- Remove malware or unauthorized access.
- Patch vulnerabilities and harden affected systems.
- Restore systems from clean backups.
- Monitor for signs of residual or new threats.

d. Post-incident Activity

- Conduct post-incident reviews within 10 business days.
- Document findings and update controls and procedures.

7.0 Reporting an Incident:

- All incidents must be reported **immediately** to the IT Support Team at: ithelpdesk@hastingscounty.com or 613-966-0234. After hours at (613) 966-0334
- Users must not delete or alter data related to the incident.

8.0 Classification of Incidents:

Incidents are classified as follows:

Level	Description	Response Time
Low	Minor disruption; no sensitive data involved	24 hours
Medium	Moderate impact; may involve sensitive data	4 hours
High	Major disruption; confirmed data breach or malware	Immediate

9.0 Communication Protocol:

- Communication must be coordinated through designated channels.
- External communication (media, public) must be approved by Incident Response Team.

10.0 Documentation and Retention:

- All incident records must be retained for two (2) years.
- Documentation includes logs, timelines, communications, and postmortem reports.

11.0 Compliance and Enforcement:

- Violations of this policy may result in disciplinary action up to and including termination.
- This policy supports compliance with applicable regulations (e.g. *Municipal Act,* MFIPPA, *Emergency Management and Civil Protection Act*)

12.0 Review and Maintenance:

- This policy must be reviewed annually or after any major incident.
- Updates must be approved by Council.