CITY OF BROADVIEW HEIGHTS
RESOLUTION NO. 2025-172

INTRODUCED BY MAYOR AND ENTIRE COUNCIL

A RESOLUTION ESTABLISHING OF A CYBER SECURITY POLICY IN THE CITY OF BROADVIEW HEIGHTS AND DECLARING AN EMERGENCY

WHEREAS, Ohio Revised Code Section 9.64, enacted through House Bill 96, requires political subdivisions to set and adopt standards safeguarding against cybersecurity threats and ransomware attacks; and

WHEREAS, Cities are required to adopt a Cyber Security Program (Policy) by January 1, 2026.

NOW, THEREFORE, BE IT RESOLVED BY THE COUNCIL OF THE CITY OF BROADVIEW HEIGHTS, COUNTY OF CUYAHOGA AND STATE OF OHIO:

SECTION 1. In accordance with Ohio Revised Code Section 9.64 a Cyber Security Policy shall be established as delineated in Exhibit "A" attached hereto and made a part hereof as if fully rewritten.

SECTION 2. This Resolution is declared to be an emergency measure necessary for the immediate preservation of the public health, safety and welfare and for the further reason stated in the Preamble hereof, and provided it receives the affirmative vote of five (5) or more of the members of Council and the signature of the Mayor; otherwise it shall take effect and be in force from and after the earliest period allowed by law..

Passed and Adopted by the Council on this 15th day of December, 2025

Robert Boldt, President of Council

Samuel J. Alai, Mayor — December 15, 2025 — Date

Attest: Robin Parsons, Clerk of Council — December 15, 2025 — Date

2025
Rev 1.0

Cyber Security Policy

CITY OF BROADVIEW HEIGHTS

Cyber Security Policy

City of Broadview Heights
2025

Version	Modified Date	Reason for Modification	Modified by
1.0	12/10/2025	Document Creation	City of Broadview Heights / Talix

Contents

Cyber Security Policy

City of Broadview Heights
2025

Introduction

What is the primary purpose of this policy?

The primary purpose of this policy is to establish a cybersecurity framework for protecting the City of Broadview Heights' *(hereafter referred to as "the organization")* organizational assets and data, as well as arming the organization's employees against cyber threats and attacks.

How does this policy support organizational goals?

This policy supports organizational goals by ensuring data confidentiality, integrity and availability.

Who is responsible for enforcing this policy?

The Cyber Security Director / CIO / IT Security Team and relevant department heads are responsible for enforcing this policy.

Policy Scope

What systems and networks are included?

The scope of this document includes all servers hosted on-premises or in cloud environments, all endpoints, network devices and IoT devices.

What data types does this policy protect?

The data types protected by this policy include customer data, financial records & intellectual property.

Who are the stakeholders covered under this policy?

Employees, contractors, third-party vendors and partners are covered under this policy. Compliance with this policy is mandatory for all of the above.

Are there any exclusions to this scope?

Personal devices are excluded from the scope of this policy.

Applicable Stakeholders

Name	Type	Roles	Description of CS Duties	Contact Information
Ted Bruzdzinski	IT Employee	CISO / CyberSec Team Lead	Manage the CyberSec Program First contact in IR situations	440-584-8578

Talix	3rd-Party Contractor	IT Contractor	IR Response Team (Hand-off from CyberSec Program Lead/Secondary)	440-717-4112 Talixit.com
Travelers Insurance	Vendor	Insurance Vendor IT Contractor	Initiate Recovery Procedures on behalf of Insurance Company	Emergency Response: 1-800-252-4633
Dave Pfaff	Finance Employee	CyberSec Team (Secondary)	Backup contact in IR situations	440-526-3795
	Other			

Policy Overview

The organization will proactively protect its digital assets and ensure compliance with all applicable regulations (NIST CSF). Adherence to the policy is essential to maintaining confidentiality, integrity, and availability of critical systems and information. Furthermore, in accordance with Sections 149.43 and 149.433 of the Ohio Revised Code, all records, documents, and reports related to the cybersecurity program—including incident reports and procurement details of cybersecurity-related products and services—are classified as non-public and security records. This classification is intended to protect sensitive information from unauthorized disclosure and to enhance the overall security posture of the political subdivision.

This policy will be reviewed annually or as required by emerging threats or compliance changes. This policy will be updated as required.

The high-level objective of this policy is to minimize cybersecurity risks and foster a culture of security awareness within the organization.

Organizational Commitment

The organization's overarching cybersecurity commitment is to safeguard the confidentiality, integrity and availability of all information assets. Adherence to industry standards, proactive risk management and stakeholder training are key principles that guide the organization's cybersecurity efforts. The organization commits fully to implementing cybersecurity controls and practices to achieve the above.

Cybersecurity Goals & Objectives

The key cybersecurity goals are to identify and protect all critical assets, mitigate cybersecurity risks through regular assessments and controls, and continue to evolve the goals as the IT landscape changes.

The measurable objectives of the policy are to conduct quarterly phishing simulations and to ensure compliance with access control protocols.

Key Commitments

The organization will perform regular cybersecurity risk assessments, maintain a continuous monitoring and incident response system. Cybersecurity will be embedded into operational workflows, all decision making relating to IT processes and purchases and vendor management practices. The organization's approach to cybersecurity training and awareness is to provide regular cybersecurity training for all employees and awareness programs for stakeholders.

The organization, if experiencing a ransomware incident, shall not pay or otherwise comply with a ransom demand unless the political subdivision's legislative authority formally approves the payment or compliance with the ransom demand in a resolution or ordinance that specifically states why the payment or compliance with the ransom demand is in the best interest of the political subdivision *(per Ohio HB-96).*

Policy Review & Updates

The policy will be reviewed annually or after significant changes.

The CISO / CyberSecurity Director will be responsible for coordinating the updating of the policy.

Changes in compliance requirements or major security incidents will trigger a policy review.

Compliance & Standards

Regular internal audits, compliance training and third-party assessments will be used to ensure compliance.

Monitoring & Evaluation

The effectiveness of the cybersecurity policy will be evaluated through incident tracking, audit results and stakeholder feedback. The tools or processes used for monitoring compliance will include compliance tools, logging and assessment services provided by third parties.

Risk Assessment

Asset Identification

The organization has identified critical functions and assets and assessed their cybersecurity risk and vulnerabilities. The table below identifies the different types of assets and their criticality.

Asset Type	Examples	Value/Criticality	Owner/Steward	Location
Data	Customer data, financial records	High	*IT & Accounting Team*	Cloud/On-prem Storage/Servers
Devices	Laptops, servers, IoT sensors	Medium	*IT Director*	HQ and branch offices
Applications	CRM, ERP, custom systems	High	*IT Director*	Cloud/On-Prem Servers
Personnel	Employees, contractors	High	*HR Team*	HQ
Networks	VPNs, internal and external networks, network devices	High	*IT Director*	HQ/Data center

Threat Assessment

The organization has identified potential impacts of various types of cybersecurity breaches on operations, safety, and service delivery. The table below outlines the organization's risk level based on various types of attacks and the potential impacts related to them.

Threat Type	Description	Likelihood	Impact	Risk Score
Malware (ransomware)	Encrypts systems and demands ransom	High	High	9
Phishing attacks	Tricking employees to reveal credentials and gain access	Medium	High	6
Insider threat (negligent)	Employee misconfigures system accidentally, causing outage or data loss	Low	Medium	3
Insider threat (purposeful)	Employee misconfigures system w/malicious intent	Low	Medium	3
DDoS attack	Overloads servers causing downtime	Medium	High	6

Vulnerability Evaluation

The organization has defined various potential cybersecurity vulnerabilities and what their impact would be to the organization should one of them occur and be attacked. The current controls implemented by the organization to thwart or prevent these attacks is also listed:

Vulnerability	Description	Impact	Likelihood	Current Controls Implemented
Unpatched software	Outdated OS or apps vulnerable	High	Medium	Patch schedule in place
Unpatched hardware	Outdated firmware	High	Medium	Automated and scheduled patching in place
Weak account passwords	Easy-to-guess credentials	Medium	High	Enforced policy via AD
Insecure or weak e-mail filtering	Phishing susceptibility	High	High	Email filtering enabled
VPN or Systems without MFA enforced	Insecure remote access	High	High	MFA enabled on VPN connections
Cloud tenants insecure	Security settings not enforced in cloud environments	Medium	Medium	Security assessments with remediation active
All of the above	Remediation of all of the above items	N/A	N/A	Periodic security assessments

Impact Analysis

The organization has defined operational, financial and the compliance impact of a cybersecurity incident in the table below.

Risk/Threat	Financial Impact	Reputational Impact	Operational Impact	Compliance Impact
Ransomware attack	$1M (downtime + ransom)	High	Severe (downtime)	High
Phishing credentials	$100k (breach cost)	Medium	Low	Medium
Insider threat (data theft)	$500k (litigation)	High	Moderate	Medium

Risk Management & Mitigation

The organization has determined methods of risk management and mitigation that can help lead to a reduced risk of an incident occurring. These methods are listed below.

Risk/Threat	Mitigation Strategy	Controls Implemented	Responsible Party	Timeline
Ransomware attack	Enhance backup systems	3-2-1 Backup Implemented	IT & Security Team	Continuous
Phishing credentials	Employee training and MFA	Phishing simulations, MFA	Cybersecurity Team	Continuous
Insider threat (negligent)	Review access control policies	Regular audits	HR & IT Team	Annual

Employee Training

All employees of the organization must undergo cybersecurity training annually. Training shall be role-specific and will be provided by *The State of Ohio* or the *Ohio Persistent Cyber Initiative (OPCI) via the Ohio Cyber Range Institute*. This training is also supplemented by continuous phishing training via external third party programs like those offered by KnowBe4 (periodic simulated phishing campaigns), which the organization subscribes to.

Access Management & Controls

Authentication Systems & Controls

The organization uses the following authentication controls where possible to control access to data and systems across the organization:

Control Type	Description	Examples/Tools
Password Authentication	Identity confirmation through a secure username-password pair.	Password policies, SSO
Biometric Authentication	Identity verification using physical traits.	Fingerprint scanners, Face ID where applicable
Multifactor Authentication (MFA)	Adds an extra layer of security beyond passwords (e.g., OTP, push notifications).	Authenticator apps, SMS OTP
Risk-Based Authentication	Dynamically adjusts security based on user behavior and location.	Conditional access policies

Authorization Processes

The organization uses the following authorization processes where possible to control access and permissions for data and systems across the organization:

Policy	Description	Implementation
Least Privilege Principle	Grants only the minimum access rights required for a role or task.	Role-Based Access Control (RBAC)
Role-Based Access Control	Assigns permissions to roles instead of individual users	Defined job profiles
Data Segmentation	Segregates sensitive data from general access.	Defined permissions, based on group/role

Documentation, Logging & Auditing

The organization has put in place the following monitoring and logging processes to assist in detection and prevention of incidents:

Activity	Description	Tools/Procedures
Access Logging	Record access to sensitive data, successful/failed login attempts.	Firewall logging, Domain Controller auditing
Monitoring for Anomalies	Track irregular access patterns (e.g., at odd hours or from unusual locations).	User Behavior Analytics (UBA) via Office 365 Alerts
Compliance Audits	Periodically review access logs and policy adherence.	Internal audits, third-party auditors
Forensic Investigations	Analyze logs during a suspected breach.	Incident response tools (Scripts, Log Analysis, EDR/XDR Tools)

Password Security

The organization adheres to the following security policies relating to passwords across all systems with the goal of preventing unauthorized access to any of the organization's systems or data:

Policy	Description	Implementation
Complexity Requirements	Passwords must include a mix of uppercase, lowercase, numbers, and symbols.	Enforced by IT systems
Password Expiration	Passwords must be changed regularly (every 90 days).	Automated notifications
Reuse Limitations	Users cannot reuse recent passwords.	Enforced by system group policies
Password Management Tools	Encourage the use of secure password vaults for storage.	KeePass, etc.
Passwordless Solutions	Transition to secure alternatives (e.g., biometrics, FIDO2 tokens).	Hardware keys, SSO

Session Security

The organization has implemented session security where possible to terminate idle sessions that might be an attack vector to the environment:

Policy	Description	Implementation
Session Timeout	Automatically logs out inactive sessions after a specified period.	Timeout policies (GPO & VPN)
Risk-Based Termination	Terminates sessions flagged for unusual activity or risks.	AI-based monitoring (EDR)
VPN Timeout	Automatically disconnects idle VPN sessions	Firewall-based idle timeout

Incident Response

Incident Response Plan

The organization's Incident Response Plan aligns with the National Institute of Standards and Technology (NIST) cybersecurity framework (2.0), and the center for internet security cybersecurity (CIS) best practices:

- **Identify**
  - The steps involved in being ready to handle incidents effectively. Identifying physical and software assets within the organization. Discovering vulnerabilities in said assets and identifying risk response and tolerance.
  - Actions – defining the Incident Response Team, identifying and establishing cybersecurity policies, assigning roles and responsibilities, providing training to users, establishing asset management.
- **Protect**
  - Implementing protection processes for information systems and assets. Protecting identity management and access control within the organization, including physical and remote access. Empowering staff through security training. Establishing data protection consistent with risk management. Protecting assets via maintenance activities.
- **Detect**
  - Timely identification and evaluation of potential and active incidents. Ensuring anomalies are detected within the environment. Implementing continuous monitoring and detection.
  - Actions – monitoring using tools, analyzing alerts, classifying incidents based on severity, vulnerability scanning (internal/external), collecting logs for analysis, penetration testing.
- **Respond**
  - Limiting the damage and spread of the attack by isolating compromised systems.
    - Actions – disconnecting affected devices, applying patches, removing malware, activating DR plans, securing backups, identifying root causes and mitigating vulnerabilities.
  - Ensuring response planning processes are executed during and after an incident.
  - Communicating internally via secure messaging tools about the incident
  - Designating a spokesperson for internal / external communications.
  - E-mail updates to stakeholders periodically.

        - Actions – calling/messaging spokespeople, the state (per above), releasing pre-approved statements, conference calls, repeated updates to keep everyone involved in the know.
    - Notification of a Ransomware incident to the Ohio Dept of Public Safety and the Ohio Auditor of State are required per the following regulations:
        - The Executive Director of Ohio Homeland Security within the Ohio Department of Public Safety will be notified as soon as possible but not later than 7 days after discovering the incident. Incidents can be reported to Homeland Security's Ohio Cyber Integration Center (OCIC) at: Ohio Cyber Integration Center | Ohio Homeland Security, OCIC@dps.ohio.gov or 614-387-1089.
        - The Ohio Auditor of State will be notified as soon as possible but not later than thirty (30) days after discovering the incident. Incidents can be reported to the Ohio Auditor of State via email to Cyber@ohioauditor.gov using the form located at: https://ohioauditor.gov/fraud/cybersecurity.html
- **Recover**
    - Rebuilding affected systems, restoring data from backups that have had integrity verifications, confirming patching of vulnerabilities and that no threats remain.
    - Actions – Run vulnerability scans, verify backup integrity, continue heightened monitoring.
    - Analyzing logs, identifying root causes, tracing attacker behavior, implementing improvements learned from the incident.
    - Actions – creating an incident report, including post-incident meeting notes. Modify the incident response and prevention measures based on findings, improving the policy. Reviews will be done annually at a minimum.

Incident Response Process

Based on the NIST alignment above, these are the steps for incident response within the organization:

Identify

1. Monitor IT systems using cyber security detection tools and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.
2. Talix will assist the IR Team in reviewing logs from the appropriate systems (eg. Active Directory, Azure AD, AV/EDR, Office 365, Firewall, etc.) and will document and save all evidence related to the incident.

Detect

1. Talix, through log and environmental investigations, and in lock step with any Cyber Security IR/Forensic team, will assist to establish the source attack vector as quickly as possible and take immediate action to remove or restrict access to said attack vector.
2. Continued detection of issues in the environment throughout the engagement will take place. Documentation of any further discoveries will be taken.

Protect

1. Perform short-term containment, by isolating the network segment that is under attack. Then focus on long-term containment, which involved temporary fixes to allow systems to be used in production, while rebuilding clean systems.
2. Talix will assist the IR Team with long term containment through immediate recommendations of fixes and mitigations that will thwart further attacks through this and any adjacent attack vectors that may still be available.
3. In the case of a breach or Ransomware attack, Talix will assist the IR Team to ensure any affected systems will be taken offline until they can be secured either via software or manual disconnection. The goal is to ensure that no other devices remain vulnerable.

Respond

1. Remove malware/vulnerabilities from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
2. Using enterprise-grade security tools including EDR/MDR and remediation scripts, Talix will assist the IR Team to clean and restore any devices that can be restored to health adequately, or in most cases recommend a full wipe of affected systems and restore from backup.
3. Notification of a Ransomware incident to the Ohio Dept of Public Safety will be performed.
4. If necessary, notification will be sent to LEADS Control (1-800-589-2077) within 24 hours and the completed and returned LEADS Security Incident Response Form to the LEADS security team within seven days' time.

Recover

1. Bring affected production systems back online carefully, to prevent additional attacks. Test, verify, and monitor affected systems to ensure they are back to normal activity.
2. Talix will assist the IR Team to determine whether backups are viable and unaffected by the incident, and in such a case will work with the IR Team to begin the restoration process of unaffected servers and data.
3. Talix will assist the IR Team by performing a thorough analysis of the incident and recovery process undertaken. Recommendations and concerns for potential future attacks and how to remediate any outstanding vulnerabilities will be delivered to the organization.

Backup & Disaster Recovery

Backup Procedures

Critical systems and data are defined via an inventory of assets (databases, files, applications, configurations). Schedules for backup frequency are determined based on the criticality of the above data and applied to the systems (real-time, daily, weekly, monthly). Secure and redundant storage locations are used to store the backups of said data, including on-premises and cloud locations. Periodic checks are carried out on said backups to ensure their viability and restorability. The duration for retaining backups is defined based on compliance/legal requirements.

Data Criticality	Backup Storage	Tools/Storage Used	Backup Frequency
Production Critical	On-Premise + Second Location, Cloud Replication	Enterprise backup software Secured cloud storage SAN/NAS devices	At least daily
Non-Production Data	On-Premise + Second Location	Enterprise backup software SAN/NAS devices	Company discretion

Disaster Recovery Plan

The Disaster Recovery Plan assesses the nature and extent of the disaster (eg. Hardware failure, ransomware, etc) and is carried out by the Incident Response Team, often at the direction of the Cyber Insurance-appointed recovery team. *It is imperative that where Cyber Insurance has been secured, that the Cyber Insurance company and their hand-picked response team is brought in at the start of the engagement to direct the recovery process in line with the Cyber Insurance coverage.* Systems will be prioritized by criticality to resuming operations. The restoration and recovery process will begin with that priority in mind. Clear communication will be established and maintained with stakeholders during the recovery process, based on an incident communication plan. Validation of the restored systems by the IT and Security teams is required to ensure integrity and functionality.

Business Continuity Plan

The organization's Business Continuity Plan consists of tools for internal/external communications during downtime, using encrypted messaging apps or dedicated lines. The availability of essential tools (e-mail, ERP system, other required tools) during the disruption is vital. If necessary, temporary workspaces will be designated and set up for users to work from alternatively during the downtime, if not from home. Key personnel contact information will be distributed to stakeholders and users during the recovery effort. Documentation will be provided to end users outlining how to continue with operations during the incident and recovery. Cloud availability and storage for said documents, tools and messaging apps is a priority.

Regulatory Compliance

Governance & Compliance

The organization is committed to safeguarding its digital infrastructure and ensuring accountability in the implementation of cybersecurity measures. Compliance with this policy is mandatory for all employees, contractors, and any other individuals or entities who interact with or manage the organization's information technology systems and data. Adherence to the policy is essential to maintaining confidentiality, integrity, and availability of critical systems and information. Furthermore, in accordance with Sections 149.43 and 149.433 of the Ohio Revised Code, all records, documents, and reports related to the cybersecurity program—including incident reports and procurement details of cybersecurity-related products and services—are classified as non-public and security records. This classification is intended to protect sensitive information from unauthorized disclosure and to enhance the overall security posture of the political subdivision.

Applicable Regulatory & Industry Standards

The following are compliance standards that the organization recognizes and adheres to for applicable data and systems:

Standard/Regulation	Applicability	Description
CJIS Security Policy	Criminal Justice system protected data	The CJIS Security Policy is a standard for how organizations must handle and protect CJI throughout its entire lifecycle (creation, storage, transmission, and destruction).
Other		

Control Implementation

The control of the implementation of regulatory compliance is split into 5 categories:

- Access Control
  - The organization limits data access based on user roles and responsibilities using role based access control (RBAC), granular permissions, MFA to secure the access.
- Data Protection
  - The organization secures data in transit and at rest using AES-256 encryption, TLS 1.2+, FIPS 140-3 compliance VPNs, etc.
- Data Processing
  - The organization ensures legal basis for data collection and storage.

- Incident Response
  - The organization is prepared to send breach notifications within regulatory timeframes depending on the applicable regulatory and industry standards.
- Data Minimization
  - The organization stores only the necessary data for business processes using data retention policies.

Documentation Guidelines

The organization defines controls and compliance frameworks on an annual or as-needed basis. Auditing reports will adhere to standards and be reviewed as per an auditing schedule. Data storage, processing and transfers will be tracked as needed. Compliance reports to prove adherence to regulations will be completed on an as-needed basis, based on external auditing requirements.

Auditing and Reporting

Internal audits will be performed on an as-needed basis, in compliance with internal policies and regulations. External, independent audits and assessments for certifications or regulatory requirements will be performed on a per-regulation basis. Gap analysis of non-conforming areas will be prioritized and reviewed on an annual basis. Compliance reports for regulatory authorities or customers will be provided on an as-required basis based on regulation.

Definitions

- Cybersecurity Incident:

  (a) A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;

  (b) A serious impact on the safety and resiliency of a covered entity's operational systems and processes;

  (c) A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;

  (d) Unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by:

  (i) A compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or (ii) A supply chain compromise. "Cybersecurity incident" does not include mere threats of disruption as extortion; events perpetrated in good faith in response to a request by the system owner or operator; or lawfully authorized activity of a United States, state, local, tribal, or territorial Entity.

- Ransomware Incident: a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a political subdivision's information technology systems or data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.