BOARD OF PARK COMMISSIONERS OF THE
CLEVELAND METROPOLITAN PARK DISTRICT
POLICY STATEMENT

SUBJECT: Cybersecurity Policy

EFFECTIVE DATE: June 18, 2026

I. Purpose

This Cybersecurity Policy establishes the framework, guidelines, responsibilities, and behavioral standards required to protect Cleveland Metroparks' information systems, data, and technology assets. This policy applies to all employees, volunteers, interns, vendors, contractors, affiliates, and third parties who access organizational systems or data. This Policy is based on the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF 2.0 standards") and its core functions and is issued in accordance with Ohio Revised Code § 9.64 and other relevant laws and regulations. Supplemental NIST-aligned standard operating procedures and supporting policies are maintained separately by the Information Technology Services (ITS) department and are hereby incorporated by reference into this Cybersecurity Policy.

II. Scope

This policy applies to:

1. All full-time, part-time, temporary, and seasonal employees

2. Contractors, consultants, affiliates, and third-party vendors with access to systems and data

3. Volunteers and interns with access to systems and data

4. All devices (Cleveland-Metroparks-owned and personal) used to access Cleveland Metroparks systems and data

5. All information systems, applications, cloud services, and data repositories maintained or used by Cleveland Metroparks (collectively, "Users")

This Policy also governs the Cleveland Metroparks Police Department. If any of the policies contained herein conflict with State or Federal guidelines for local law enforcement, including but not limited to the FBI Criminal Justice Information Services (CJIS) Security Policy and the Ohio LEADS (Law Enforcement Automated Data System) rules, the State-mandated or Federal-mandated policies take precedence.

III. Compliance with Ohio Revised Code § 9.64

Ohio Revised Code § 9.64 (effective September 30, 2025), requires political subdivisions to adopt and maintain a formal cybersecurity program that safeguards data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.

The law mandates that the program be consistent with generally accepted cybersecurity best practices, the NIST Cybersecurity Framework and the Center for Internet Security (CIS) Cybersecurity Best Practices as recognized standards. In compliance with ORC § 9.64, this Policy:

1. Establishes organizational cybersecurity requirements for all personnel

2. Aligns with the NIST CSF 2.0 best practices

3. Designates accountability for cybersecurity governance and compliance

4. Establishes cybersecurity training requirements for all employees, with frequency and detail corresponding to each employee's duties

5. Mandates incident reporting and response protocols consistent with statutory deadlines

6. Restricts ransom payments in the event of a ransomware incident in accordance with ORC § 9.64(B)

7. Incorporates by reference all NIST-aligned standard operating procedures ("SOPs") and supplemental cybersecurity policies maintained by Cleveland Metroparks

A. Statutory Incident Reporting Requirements

Upon discovering a cybersecurity or ransomware incident, Cleveland Metroparks is required by law to report the incident to Ohio Department of Public Safety, Ohio Cyber Integration Center (OCIC) as soon as possible, but no later than seven (7) days after discovery and to the Ohio Auditor of State (AOS) as soon as possible, but no later than thirty (30) days after discovery.

Notify DPS/OCIC
WITHIN 7 DAYS

- cyber.ohio.gov/priorities/ocic
- 614-387-1089
- OCIC@dps.ohio.gov

Notify AOS
WITHIN 30 DAYS

- Cybersecurity Reporting Form
- Cyber@ohioauditor.gov

B. Ransom Payment Restriction

Pursuant to ORC § 9.64(B), Cleveland Metroparks shall not pay or otherwise comply with a ransom demand in the event of a ransomware incident unless the Board of Park Commissioners passes a formal resolution finding that payment is in the best interest of Cleveland Metroparks.

C. Public Records Exemption

Pursuant to ORC § 9.64(E) and (F), the following are exempt from public records disclosure:

1. All records, documents, and reports related to the cybersecurity program and framework are not public records under ORC § 149.43.

2. Records identifying cybersecurity-related software, hardware, goods, and services, including vendor name, product name, project name, or project description, are security records under ORC § 149.433 and are exempt from public records requests.

D. Compliance & Audit

The Ohio Auditor of State is responsible for auditing political subdivisions for compliance with ORC § 9.64. Non-compliance may result in an audit finding, increased liability, and reputational risk.

IV. Cybersecurity Program Framework Alignment

Cybersecurity at Cleveland Metroparks has three components that work together to protect the confidentiality, integrity, and availability of Cleveland Metroparks' systems and data:

1. Administrative Safeguards, including administrative actions, policies, and procedures.
2. Technical Safeguards, including security and access controls for computer, device, and network resources and the use of artificial intelligence (AI) or generative artificial intelligence (GenAI).
3. Physical Safeguards, including electronic information systems and related buildings and infrastructure.

This Policy, Cleveland Metroparks' cybersecurity program, and all associated documents align with NIST CSF 2.0 standards. The NIST CSF 2.0 standards are industry accepted best practices for organizations to address proper enterprise risk management and cybersecurity operations based on six core functions:

Govern	Establish and maintain cybersecurity governance, risk management strategy, roles, responsibilities, and policy oversight across Cleveland Metroparks.
Identify	Understand and document organizational assets, risks, and vulnerabilities to prioritize cybersecurity efforts effectively.
Protect	Implement safeguards to ensure the delivery of critical services and limit the impact of potential cybersecurity events.
Detect	Develop and implement activities to identify the occurrence of a cybersecurity event in a timely manner.
Respond	Take action regarding a detected cybersecurity incident to contain its impact and maintain operations.
Recover	Restore capabilities and services impaired due to a cybersecurity incident and implement improvements.

V. Procedures, Cybersecurity SOPs, and Supplemental Policies

Detailed procedures, standards, and work instructions that support this Policy are maintained in internal Cybersecurity SOPs and Supplemental Policies. Users shall follow the Cybersecurity SOPs/Policies that apply to their roles and activities. Cybersecurity SOPs/Policies may be updated on an as-needed basis to reflect changes in risk, technology, and legal or regulatory requirements. All NIST CSF 2.0 standard SOPs/Policies referenced herein are maintained as separate documents and are incorporated into this Cybersecurity Policy in their entirety. Employees are expected to adhere to both this overarching Cybersecurity Policy and all incorporated supplemental documents.

VI. Definitions

Users	Users include employees, volunteers, interns, vendors, contractors, affiliates, and third parties who are authorized to access or use Cleveland Metroparks information and technology resources.
Information Technology Services (ITS)	The Cleveland Metroparks department responsible for providing and supporting information technology services and implementing cybersecurity controls and operational practices.
Approved	Issued by Cleveland Metroparks or explicitly approved for Cleveland Metroparks business use (including approval by ITS when applicable).
Confidential Information	Information that is not subject to disclosure through the Ohio Public Records Act and is owned or in the short-term or long-term possession of Cleveland Metroparks.
Proprietary Information	Information that is created, generated, or formulated by Cleveland Metroparks, its officers, employees, or agents for Cleveland Metroparks purposes and owned by Cleveland Metroparks.
Sensitive Data	A generalized term that typically represents data classified as Sensitive, according to the data classification scheme defined by Cleveland Metroparks. This term is often used interchangeably with confidential data.
Nonpublic Information	Information that is not intended for public release, including Confidential Information, Sensitive Data, and other internal Cleveland Metroparks information designated as nonpublic.
Authorization	Process of granting or denying access rights and permissions to a user or a system.
Confidentiality	Protection of information from unauthorized access or disclosure.
Integrity	Protection of information from unauthorized modification or destruction.

Availability	Ensuring information and services are available when needed.
Encryption	Converting data from its original form to an unreadable form.
Approved Secure Method	A Cleveland Metroparks-approved method for securely transmitting information, such as encryption or another ITS-approved secure communication method.
Artificial Intelligence (AI) and Generative Artificial Intelligence (GenAI)	Artificial Intelligence is an engineered system where machines learn from experience, adjusting to new inputs, and potentially performing tasks previously done by humans. More specifically, it is a field of computer science dedicated to simulating intelligent behavior in computers. It may include automated decision-making. GenAI is artificial intelligence capable of producing text, images, statistically probable outputs or other data using learning models, often in response to prompts.
Cybersecurity Incident	Means any of the following: A substantial loss of confidentiality, integrity, or availability of Cleveland Metroparks' information system or network; A serious impact on the safety and resiliency of Cleveland Metroparks' operational systems and processes; A disruption of Cleveland Metroparks' ability to engage in business or industrial operations, or deliver goods or services; Unauthorized access to Cleveland Metroparks' information system or network, or nonpublic information contained therein, that is facilitated through or is caused by: A compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or 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 government entity.

Ransomware Incident	"Ransomware incident" means 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

VII. Roles and Responsibilities

Executive Leadership/Legal	Approve and resource the cybersecurity program; ensure organizational commitment to security culture and compliance. Develop and maintain NIST-aligned policies and procedures.
ITS Security Team	Implement technical controls, manage incidents, in coordination with Legal/Risk Management, maintain infrastructure security, and administer this policy.
Department Managers/Directors	Ensure staff and vendor compliance with this policy; escalate incidents; integrate security into departmental operations.
All Users	Adhere to this policy and all incorporated SOPs/Policies; complete required training; report incidents promptly.
Third-Party Vendors/Contractors	Comply with applicable organizational cybersecurity requirements as defined in vendor agreements, this policy, and SOPs.

VIII. User Guidelines

A. Workforce Cybersecurity Responsibilities

Cleveland Metroparks Users shall protect Cleveland Metroparks' information and technology resources by:

1. Using Cleveland Metroparks-approved accounts and access methods for Cleveland Metroparks business, safeguarding account credentials, and not using personal accounts (including personal email) to conduct Cleveland Metroparks work.
2. Handling Confidential, Sensitive, and Proprietary Information in accordance with this Policy and applicable Cybersecurity SOPs.
3. Users acknowledge that Cleveland Metroparks information systems, accounts, devices, and network traffic may be monitored at any time and audited periodically for security, compliance, and business purposes.
4. Users shall comply with Cleveland Metroparks software installation, configuration, and change control requirements, and shall not install or connect unauthorized hardware or software to Cleveland Metroparks systems.
5. Users must follow cybersecurity standards and procedures maintained in Cybersecurity SOPs and policies.

B. Security and Incident Response

1. Cleveland Metroparks Users shall protect Cleveland Metroparks-owned or Cleveland Metroparks-authorized devices and systems against unauthorized physical access, including when devices are unattended.
2. Cleveland Metroparks shall maintain and follow incident response policies and procedures.
3. Users shall immediately report suspected cybersecurity incidents, suspicious activity, lost or stolen devices, or potential unauthorized access in accordance with Cleveland Metroparks incident reporting procedures and applicable Cybersecurity SOPs and policies.
4. Report incidents to: ITS Security Team at cyberalert@clevelandmetroparks.com or via the ITS Help Desk helpdesk@clevelandmetroparks.com or call 216-635-3375.
5. No User will face retaliation for reporting a suspected cybersecurity incident in good faith.

C. System and Network Activities

1. Users shall not use Cleveland Metroparks' information and technology resources for illegal, criminal, or unauthorized purposes.
2. Users shall not access, attempt to access, or use Cleveland Metroparks' data, systems, servers, applications, or accounts except as authorized by Cleveland Metroparks for business purposes.
3. Users shall not disclose, upload, or otherwise share Cleveland Metroparks nonpublic information (including Confidential, Sensitive, Proprietary, personnel, or cybersecurity-related information) to unauthorized individuals or systems, including public-facing AI or generative AI tools that are not approved for Cleveland Metroparks business use.
4. Users shall not introduce malicious code or activities that could disrupt, damage, degrade, or interfere with Cleveland Metroparks systems or network operations.
5. Users shall not bypass security controls, disable protections, or attempt to circumvent authentication or access controls.
6. Users shall not share credentials or allow others to use their accounts or access methods, except as authorized by Cleveland Metroparks procedures.
7. Users shall not copy, distribute, or use software or content in violation of licensing, copyright, trade secret, or other intellectual property protections.
8. Users shall not use Cleveland Metroparks' resources to create, transmit, or store content that violates Cleveland Metroparks policies (including harassment, discrimination, threats, or other prohibited conduct).

D. Cybersecurity Controls

1. ITS shall define and implement a cybersecurity awareness and training program for Cleveland Metroparks Users which shall correspond to the duties of each User.
2. ITS shall implement and maintain security controls and operational practices to protect Cleveland Metroparks systems and data, including access controls and authentication mechanisms appropriate to the risk and sensitivity of the information.
3. ITS shall establish and maintain data backup, disaster recovery, data retention, and data lifecycle management practices in accordance with applicable legal, regulatory, and contractual requirements.
4. Users shall protect Confidential and Sensitive Information by using Cleveland Metroparks-approved safeguards for storage and transmission, using encryption when required or applicable, and limiting access and disclosure to what is authorized and necessary to perform assigned job duties.

5. Users shall use only Cleveland Metroparks-approved services and methods for transferring Cleveland Metroparks information to third parties, including approved file-sharing solutions.

E. Internal and External Communication (Phone System, Email, Fax, E-Fax)

1. Users shall use Cleveland Metroparks-approved communication systems for Cleveland Metroparks business communications and shall protect communications from unauthorized access, interception, or disclosure.
2. Users shall ensure voicemail greetings are current and do not disclose organizational details that could compromise internal information or organizational processes. When an employee is taking extended leave, voicemail messages shall be routed to the appropriate designated contact or team.
3. Users shall not transmit sensitive or confidential data through email unless an approved secure method is used.

F. Mobile Devices Used for Cleveland Metroparks Business

1. Users who are assigned Cleveland Metroparks-owned mobile devices shall secure the device using a strong passcode or other ITS-approved device authentication method.
2. Cleveland Metroparks-owned mobile devices shall be managed using ITS-approved mobile device management (MDM) controls.
3. ITS reserves the right to remotely reset a mobile device to protect Cleveland Metroparks' information and technology resources when a device is lost, stolen, compromised, or otherwise requires protective action.
4. Users shall refer to the Cleveland Metroparks Employee Handbook for additional guidelines and requirements related to mobile devices and personal device usage.

G. Training and Awareness

1. All employees must complete mandatory cybersecurity awareness training upon hire and annually thereafter. The duration and details of employee training shall correspond to the duties of each employee.
2. Participation in phishing simulation exercises is mandatory for all staff.
3. Training completion is tracked and reported to department leadership. Non-compliance may result in disciplinary action.
4. Cleveland Metroparks will provide ongoing awareness communications including security alerts, newsletters, workgroups, and policy updates.

H. Exemptions

1. Requests for exemptions to this Cybersecurity Policy shall be submitted in advance of the activity and approved by the Chief Information Officer (CIO).
2. Approved exemptions shall be documented and shall include the requester, approver, reason for exemption, and date approved.
3. Exemption documentation shall be completed using an ITS-approved exemption form and maintained for audit purposes.
4. Exemptions shall be reviewed annually.

I. Violation of Policy

1. Violations of this Policy will be handled under Cleveland Metroparks' established procedures. Violations of this policy or any incorporated SOPs may result in disciplinary action up to and including termination of employment, contract termination, and/or referral to law enforcement where applicable. The severity of the response will be commensurate with the nature and impact of the violation.

2. A User's failure to comply with this Policy may result in disciplinary action, up to and including termination of employment.
3. Any third party's failure to comply with this Policy and SOPs may result in Cleveland Metroparks terminating contracts or restricting access and terminating or restricting access to volunteer opportunities.
4. Intentional or malicious violations, including unauthorized disclosure of data, may be referred for criminal prosecution under applicable state and federal law.
5. Compliance monitoring is conducted on an ongoing basis by the ITS Security Team.

J. Policy Review and Updates
1. This policy will be reviewed and updated at least biannually by the ITS Security Team and Legal.
2. Policy updates may also be triggered by significant changes in technology, law, regulation, threat environment, or organizational structure.
3. All updates will be communicated to employees promptly, and training will be provided as needed.
4. The effective date and version history are maintained on record by the ITS Security Team.

By approving this policy, the Board confirms its commitment to maintaining a cybersecurity program aligned with NIST standards and Ohio Revised Code § 9.64.

Replaces and Supersedes: Chief Executive Officer's Cybersecurity Policy, February 12, 2024

Citations:
Ohio Revised Code § 9.64
Ohio Revised Code §§ 1349.19, 1349.191, 1349.192, 1347.12
Ohio Revised Code §§ 149.43, 149.433
Certain organization approved NIST 800-Series Publications

Approved:

Chief Executive Officer

Board of Park Commissioners President

6/18/26
Approval Date

June 2031
Review Date