DEPARTMENT OF MANAGEMENT

IT CyberSecurity Policy

Version Version 3 · Published January 30, 2026 · Budget and Appropriations

Department of Management IT Cybersecurity Policy

Policy Number: DOM-IT-SEC-001

Version: 1.0

Effective Date: [Date]

Approved By: [Approving Authority, e.g., Department Head]

1. Purpose

The purpose of this IT Cybersecurity Policy is to establish a framework for protecting the information assets of the Department of Management from security threats, whether internal or external, deliberate or accidental. This policy is designed to safeguard the confidentiality, integrity, and availability of our data and IT systems, ensure compliance with legal and regulatory requirements, and promote a culture of security awareness among all personnel.

2. Scope

This policy applies to:

- All employees of the Department of Management, including full-time, part-time, temporary staff, and interns.
- All contractors, vendors, and third parties who are granted access to the Department's information systems and data.
- All information technology resources owned or managed by the Department, including but not limited to hardware (servers, desktops, laptops, mobile devices), software, networks, cloud services, and the data stored, processed, or transmitted on these systems.

3. Policy Statement

All individuals and systems within the scope of this policy must adhere to the following core principles to ensure a secure operating environment.

3.1 Data Classification and Handling

All departmental data must be classified according to its sensitivity. Data handling procedures must align with its classification level. The four levels are:

- **Public:** Information intended for public consumption.
- **Internal:** Information for use within the Department that does not require strict confidentiality.
- **Confidential:** Sensitive business or personal information that, if disclosed, could cause harm to the Department or individuals. Access is restricted.
- **Restricted:** Highly sensitive data that requires the highest level of protection and is subject to strict legal or regulatory controls. Access is severely limited.

3.2 Access Control

Access to Department of Management information systems and data will be granted based on the principle of *least privilege*. Users will only be given the minimum level of access necessary to perform their job functions. All user accounts must be unique to an individual, and multi-factor authentication (MFA) is required for accessing critical systems and remote services.

3.3 Acceptable Use

Department IT resources are provided for business purposes. Users are expected to act responsibly and ethically. Prohibited activities include, but are not limited to:

- Sharing passwords or authentication credentials.
- Installing unauthorized software or hardware.
- Engaging in illegal activities or accessing inappropriate content.
- Circumventing security controls.

3.4 Password Management

Strong passwords are a critical first line of defense. All passwords must meet the following minimum requirements:

- A minimum length of 12 characters.
- A combination of uppercase letters, lowercase letters, numbers, and symbols.
- Must not be based on personal information or common dictionary words.
- Must be changed every 90 days.

3.5 Device and Network Security

All devices connecting to the Department's network must be secured. This includes approved and up-to-date antivirus software, enabled firewalls, and timely

installation of security patches. Department-issued laptops must use full-disk encryption. Use of the corporate Virtual Private Network (VPN) is mandatory for accessing internal resources from untrusted networks.

3.6 Incident Response

All suspected cybersecurity incidents, including but not limited to malware infections, data breaches, or lost/stolen devices, must be reported immediately to the IT Help Desk. Timely reporting is crucial to mitigating potential damage.

3.7 Security Awareness Training

All personnel are required to complete mandatory cybersecurity awareness training upon hiring and on an annual basis thereafter. This training covers current threats, best practices, and responsibilities under this policy.

4. Procedures

4.1 Incident Reporting Procedure

1. **Identify:** Recognize a potential security incident (e.g., suspicious email, unusual system behavior, lost device).
2. **Report Immediately:** Contact the IT Help Desk via phone or email. Do not attempt to investigate, delete, or modify files yourself, as this may hinder the investigation.
3. **Provide Information:** Supply the IT Help Desk with all relevant details, such as the time of the event, systems affected, a description of the issue, and your contact information.
4. **Follow Instructions:** Await and follow instructions from the IT security team. This may include disconnecting your device from the network or ceasing use of the affected system.

4.2 Access Management Procedure

- **Requesting Access:** New access or changes to existing access must be requested by a manager through the official IT service portal. The request must specify the systems and data required and provide a business justification.
- **Provisioning Access:** The IT department will grant access based on the approved request, adhering to the principle of least privilege.
- **Access Review:** Managers are responsible for reviewing their team members' access rights on a quarterly basis to ensure they remain appropriate.
- **Terminating Access:** All access rights will be revoked immediately upon an individual's termination of employment or contract.

4.3 Secure Remote Work Procedure

- **Secure Connection:** Always connect to the Department's network using the approved VPN client when working remotely.
- **Physical Security:** Secure your company-issued devices at all times. Do not leave them unattended in public places. Ensure your screen is locked when you step away from your computer.
- **Wi-Fi Usage:** Avoid using public, unsecured Wi-Fi networks for work purposes. If you must, ensure the VPN is active at all times.

5. Compliance

5.1 Monitoring and Auditing

The Department of Management reserves the right to monitor all use of its IT resources to ensure compliance with this policy. This includes monitoring network traffic, system logs, and application access. Periodic internal and external audits will be conducted to assess the effectiveness of security controls and verify adherence to this policy.

5.2 Non-Compliance

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract, in accordance with Human Resources guidelines. Depending on the severity of the violation, legal action may also be pursued.

Any exception to this policy must be formally requested in writing and approved by the Chief Information Security Officer (CISO) or designated authority. Approved exceptions will be documented and reviewed periodically.

5.3 Policy Review

This IT Cybersecurity Policy will be reviewed and updated annually, or more frequently if significant changes occur in the threat landscape, business operations, or regulatory environment. The CISO is responsible for maintaining and updating this policy.