|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Computer Security**  **Threat Response** | **Updated:** 10/26/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of this policy is to define the organization’s responsibilities in responding to security threats that may compromise the confidentiality, integrity, or availability of its information technology (IT) resources. By establishing clear protocols and roles, the policy aims to ensure a structured and efficient response to incidents that could affect IT systems. This proactive approach enables the organization to quickly identify and mitigate potential risks, safeguard sensitive information, and maintain operational continuity during security incidents.

Implementing this policy provides several critical benefits. Firstly, it fosters a culture of security awareness across all levels of the organization, empowering employees to understand their roles in protecting IT resources. Additionally, the establishment of a Computer Emergency Response Team (CCERT) and departmental teams (DCERTs) enhances coordination and communication during security incidents, allowing for quicker and more effective responses. The policy also aids in compliance with industry standards and best practices, thereby strengthening the organization’s overall cybersecurity posture. Ultimately, by minimizing the impact of security threats, the policy helps protect the organization’s reputation, operational efficiency, and trust among stakeholders.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

This policy outlines the responsibilities and procedures for responding to security threats that may impact the confidentiality, integrity, or availability of the organization’s information technology resources. It establishes the framework for the formation of a Computer Emergency Response Team (CCERT) and departmental response teams (DCERTs) to ensure a coordinated approach to incident management. All employees, contractors, and third-party vendors are required to adhere to this policy, promoting a culture of security awareness and preparedness. By defining clear roles, communication channels, and response protocols, this policy aims to effectively mitigate security incidents and protect the organization’s information assets.

* 1. Computer Emergency Response

1. A Computer Emergency Response Team (CCERT) shall be established. The CCERT shall be led by the Chief Information Security Officer (CISO) or the Chief Information Officer or their equivalent when the CISO is not available.
2. The CCERT shall consist of representatives from all departments.
3. The CCERT shall communicate security information, guidelines for notification processes, identify potential security risks, and coordinate responses to thwart, mitigate, or eliminate security threats to IT resources.
4. Upon the activation of CCERT by the CISO, all Departmental Information Security Officers (DISO), and other CCERT representatives shall report directly to the CISO for the duration of the CCERT activation.
   1. Departmental Computer Emergency Response
5. Each department shall establish a Departmental Computer Emergency Response Team (DCERT) that is led by the DISO and has the responsibility for responding to and/or coordinating the response to security threats to IT resources within the department.
6. Representatives from each DCERT shall also be active participants in CCERT.
7. Upon the activation of a department’s DCERT by the DISO, all DCERT representatives shall report directly to the DISO for the duration of the DCERT activation.
8. Each department shall establish and implement Departmental Computer Emergency Response Procedures that consist of the following, at minimum:
   1. Creating an incident response policy and plan.
   2. Developing procedures for performing incident handling and reporting.
   3. Setting guidelines for communicating with outside parties regarding incidents.
   4. Selecting a team structure and staffing mode.
   5. Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies).
   6. Determining what services the incident response team should provide.
   7. Staffing and training the incident response team.
9. The DCERT shall inform the CCERT, as early as possible, of security threats to IT resources.
10. Each department shall develop a notification process, to ensure management notification within the department and to the CCERT, in response to IT security incidents.
11. The CCERT and DCERTs have the responsibility to take necessary corrective action to remediate IT security incidents. Such action shall include all necessary steps to preserve evidence in order to facilitate the discovery, investigation, and prosecution of crimes against IT resources.
12. Each department shall provide CCERT with contact information, including, without limitation, after-hours, for its primary and secondary CCERT representatives (e.g., DISO and Assistant DISO), and immediately notify CCERT of any changes to that information.
13. Each department shall maintain current contact information for all personnel who are important for the response to security threats to IT resources and/or the remediation of IT security incidents.
14. Each department shall provide its primary and secondary CCERT representatives with adequate portable communication devices (e.g., cell phone and pager).
15. In instances where violation of any law may have occurred, proper notifications shall be made in accordance with IT policies. All necessary action shall be taken to preserve evidence and facilitate the administration of justice.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) SP: 800-61 - Computer Security Incident Handling Guide](https://csrc.nist.gov/pubs/sp/800/61/r2/final)

[National Institute of Standards and Technology (NIST) SP: 800-50 - Building a Cybersecurity and Privacy Learning Program](https://csrc.nist.gov/pubs/sp/800/50/r1/final)

[National Institute of Standards and Technology (NIST) SP: 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](https://csrc.nist.gov/pubs/sp/800/84/final)