|  |  |
| --- | --- |
| **[Organization Name]**  **Information Technology Standard** | **No:** [Policy Number: e.g. POL-GOV-01] |
| **IT Standard**:  **Computer Security Threat Response Policy** | **Updated:** [Updated Date] |
| **Issued By:** [Authority: e.g. CEO or CIO]  **Owner:** [Owner: e.g. IT Department] |

# 1.0 Purpose and Benefits

# The purpose of this policy is to define the [entity’s] responsibility in responding to security threats affecting the confidentiality, integrity, and/or availability of information technology (IT) resources.

# 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 [Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to users of any system’s information or physical infrastructure regardless of its form or format, created or used to support the organization. It is the user’s responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the organization’s Information Security Policy and its associated standards.

# 4.0 Information Statement

Needed

### 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.

### Departmental Computer Emergency Response

1. 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.
2. Representatives from each DCERT shall also be active participants in CCERT.
3. 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.
4. Each department shall establish and implement Departmental Computer Emergency Response Procedures that consist of the following, at minimum:
5. Creating an incident response policy and plan.
6. Developing procedures for performing incident handling and reporting.
7. Setting guidelines for communicating with outside parties regarding incidents.
8. Selecting a team structure and staffing mode.
9. 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).
10. Determining what services the incident response team should provide.
11. Staffing and training the incident response team.
12. The DCERT shall inform the CCERT, as early as possible, of security threats to IT resources.
13. Each department shall develop a notification process, to ensure management notification within the department and to the CCERT, in response to IT security incidents.
14. 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.
15. 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.
16. 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.
17. Each department shall provide its primary and secondary CCERT representatives with adequate portable communication devices (e.g., cell phone and pager).
18. 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 |
|  |  |

# 8.0 Contact Information

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

[Organization Address & Policy Owner’s Contact Info]

# 9.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

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

# 10.0 Related Documents

NIST Special Publication 800-92, Guide to Computer Security Log Management

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-61 - Computer Security Incident Handling Guide

National Institute of Standards and Technology (NIST) Special Publications (SP):   
NIST SP 800-53a – Contingency Planning (CP), NIST SP 800-16, NIST SP 800-34, NIST SP 800-50, NIST SP 800-84; NIST Federal Information Processing Standards (FIPS) 199