VMEC

VERMONT MANUFACTURING EXTENSION CENTER

A Computer Security and Threat Response Policy defines how an organization will detect, analyze, contain, remove, or recover from a potential security incident. This policy is the roadmap for handling security breaches but distributing roles and responsibilities among team members. This policy is crucial for any organization to minimize damage, restore damaged systems, and prevent future incidents from occurring.

Recommended Actions:

- 🔎 Define incident response roles and responsibilities
- 📣 Implement tools for detecting security incidents
- 📝 Create an incident response plan
- 🔧 Periodically test your incident response plan through exercises

The following template may be used to help with the creation and implementation of your own policies and procedures.

For more information related to Computer Security and Threat Response Plans as well as other fundamental areas please visit the following link:

CMMC Assessment Guide Level 1

Policy #:	Title:	Effective Date:
	Computer Security Threat Response Policy	

PURPOSE

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

REFERENCE

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

POLICY

This policy is applicable to all departments and all information systems.

1. COMPUTER EMERGENCY RESPONSE

a. 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.

b. The CCERT shall consist of representatives from all departments.

c. 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.

d. 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.

2. DEPARTMENTAL COMPUTER EMERGENCY RESPONSE

a. 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.

b. Representatives from each DCERT shall also be active participants in CCERT.

c. 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.

d. Each department shall establish and implement Departmental Computer Emergency Response Procedures that consist of the following, at minimum:

    i. Creating an incident response policy and plan.

    ii. Developing procedures for performing incident handling and reporting.

    iii. Setting guidelines for communicating with outside parties regarding incidents.

    iv. Selecting a team structure and staffing mode.

    v. 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.

    vi. Determining what services the incident response team should provide.

    vii. Staffing and training the incident response team.

e. The DCERT shall inform the CCERT, as early as possible, of security threats to IT resources.

f. Each department shall develop a notification process, to ensure management notification within the department and to the CCERT, in response to IT security incidents.

g. 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.

h. 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.

i. 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.

j. Each department shall provide its primary and secondary CCERT representatives with adequate portable communication devices (e.g., cell phone and pager).

k. In instances where violation of any law may have occurred, proper notifications shall be made in accordance with IT policies. All necessary actions shall be taken to preserve evidence and facilitate the administration of justice.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	
Date Reviewed:	