[Insert Company Name Or Logo]	
Title: Cybersecurity Incident Communication Policy	**P&P #:**
Approval Date: [Date]	**Review:**
Effective Date: [Date]	**Information Technology**

Purpose
This policy defines the communication methods when incidents arise in the organization. The incidents should be handled in a manner that is appropriate and in line with the organization's values and goals. It is important to communicate any recovery plan to external and internal stakeholders and other management team.

Scope
This policy applies to all employees and other members of the workforce (whether paid, volunteer or contractor) working in all facilities under the organization's ownership.

Definitions

Incident Response Plan - The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattack against an organization's information systems network.

Policy
Our Incident Response (IR) Team will implement policies and procedures for identifying and responding to suspected or known information security incidents; mitigating, to the extent practicable, harmful effects of information security incidents that are known to our organization; and documenting information security incidents and their outcomes.

All workforce members are responsible for complying with our information security incident response and reporting policies and procedures.

Procedures
The Security Officer or Incident Response Team shall update and maintain the policy(ies) to reflect its current incident response communications methods and procedures.

The incident should be recovered in a timely manner to ensure integrity of the data and system(s) and reduce the loss of assets and reputation of the organization.

Public relations are managed

1. Organization will follow these steps to appropriately handle incidents.
    a. Implement an incident handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.
    b. Coordinate incident handling activities with contingency planning activities.
    c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Reputation is repaired after an incident

1. To restore and repair reputation of the organization after an incident, the organization should:
    a. Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.
    b. Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization within 24 hours of the incident.
    c. Analyze malicious code and/or other residual artifacts remaining in the system after the incident.
    d. Establish and maintain a security operations center.
    e. Manage public relations associated with an incident; and employ measures to repair the reputation of the organization.

Recovery activities are communicated to internal and external stakeholders as well as executive and management

1. Develop a contingency plan for the system that:
    a. Identifies essential mission and business functions and associated contingency requirements.
    b. Provides recovery objectives, restoration priorities, and metrics.
    c. Addresses contingency roles, responsibilities, assigned individuals with contact information.
    d. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure.
    e. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented.
    f. Addresses the sharing of contingency information.
    g. Is reviewed and approved by the Incident Response (IR) team.
2. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
3. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training.
4. Protect the contingency plan from unauthorized disclosure and modification.

Violations: Our workforce members are responsible for complying with our information security incident response and reporting policies and procedures. Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or assignment.

Attachments: None

Related Policies:

Reference: *NIST Special Publication 800-53 Revision 5*

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.