| Policy #: | Title: | Effective Date: |
|---|---|---|
| x.xxx | Incident Response Policy | MM/DD/YY |

## PURPOSE

To ensure that Information Technology (IT) properly identifies, contains, investigates, remedies, reports, and responds to computer security incidents.

## REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Incident Response (IR), NIST SP 800-16, NIST SP 800-50, NIST SP 800-61, NIST SP 800-84, NIST SP 800-115

## POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. INCIDENT RESPONSE TRAINING
   The cisecurity shall:

   a. Provide incident response training to information system users consistent with assigned roles and responsibilities:

      i. Within 30 days of assuming an incident response role or responsibility.

      ii. When required by information system changes, and at least annually thereafter.

   b. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

   c. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

2. INCIDENT RESPONSE TESTING
   The cisecurity shall:

   a. Test the incident response capability for the information system at least annually using simulated cyber incidents, tabletop exercises, and technical breach simulations to determine the incident response effectiveness and documents the results.

   b. Coordinate incident response testing with entity contacts responsible for related plans such as Business Continuity Plans, Contingency Plans, Disaster

Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

3. INCIDENT HANDLING
   The cisecurity shall:

   a. Implement an incident handling capability for security incidents that 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/exercises, and implements the resulting changes accordingly.

4. INCIDENT MONITORING
   The cisecurity shall:

   a. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

5. INCIDENT REPORTING
   The cisecurity shall:

   a. Require personnel to report suspected security incidents to the incident response capability within 15 minutes of discovery or suspicion, using designated reporting channels such as the Security Incident Reporting Portal or emergency hotline.

   b. Report security incident information to ASSI, ANPDP or supervisory authority, in accordance with applicable laws and organizational policies.

6. INCIDENT RESPONSE ASSISTANCE
   The cisecurity shall:

   a. Provide an incident response support resource, integral to the incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

7. INCIDENT RESPONSE PLAN
   The cisecurity shall:

   a. Develop an incident response plan that:

    i. Provides the cisecurity with a roadmap for implementing its incident response capability.

    ii. Describes the structure of the incident response capability.

    iii. Provides a high-level approach for how the incident response capability fits into the overall cisecurity.

    iv. Meets the unique requirements of the cisecurity, which relate to mission, size, structure, and functions.

    v. Defines reportable incidents.

    vi. Provides metrics for measuring the incident response capability within the cisecurity.

    vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

    viii. Is reviewed and approved by Chief Information Security Officer (CISO) on an annual basis or upon significant changes.

b. Distribute copies of the incident response plan to designated incident response personnel, including SOC analysts, IT security staff, and relevant department heads, identified by name or by role.

c. Review the incident response plan at least annually, and following major incidents or significant organizational/system changes.

d. Update the incident response plan to address system changes or problems encountered during plan implementation, execution, or testing.

e. Communicate incident response plan changes to all authorized incident response personnel, and document acknowledgment of updates.

f. Protect the incident response plan from unauthorized disclosure and modification.

## 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 and confer with the requesting department.

## RESPONSIBLE DEPARTMENT

Chief Information Office

## DATE ISSUED/DATE REVIEWED

| | |
|---|---|
| Date Issued: | MM/DD/YYYY |
| Date Reviewed: | MM/DD/YYYY |