|  |  |
| --- | --- |
| **[Entity]**  **Information Technology Standard** | **No:** |
| **IT Standard**:  **Incident Response Policy** | **Updated:** |
| **Issued By:**  **Owner:** |

# 1.0 Purpose and Benefits

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

# 2.0 Authority

*[Authority Needed]*

# 3.0 Scope

[Scope Needed]

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

# 4.0 Information Statement

*Information statement needed*

### Incident Response Policy

The [entity] shall:

1. Provide incident response training to information system users consistent with assigned roles and responsibilities:
2. Within [entity defined time period] of assuming an incident response role or responsibility.
3. When required by information system changes, and [entity defined frequency] thereafter.
4. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.
5. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

### Incident Response Testing

The [entity] shall:

1. Test the incident response capability for the information system [entity defined frequency] using [Assignment: entity defined tests] to determine the incident response effectiveness and documents the results.
2. 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.

### Incident Handling

The [entity] shall:

1. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
2. Coordinate incident handling activities with contingency planning activities.
3. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

### Incident Monitoring

The [entity] shall:

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

### Incident Reporting

The [entity] shall:

1. Require personnel to report suspected security incidents to the incident response capability within [entity defined time period].
2. Report security incident information to [entity defined authorities].

### Incident Response Assistance

The [entity] shall:

1. 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.

### Incident Response Plan

The [entity] shall:

1. Develop an incident response plan that:
2. Provides the entity with a roadmap for implementing its incident response capability.
3. Describes the structure of the incident response capability.
4. Provides a high-level approach for how the incident response capability fits into the overall entity.
5. Meets the unique requirements of the entity, which relate to mission, size, structure, and functions.
6. Defines reportable incidents.
7. Provides metrics for measuring the incident response capability within the entity.
8. Defines the resources and management support needed to effectively maintain and mature an incident response capability.
9. Is reviewed and approved by [entity defined personnel or roles].
10. Distribute copies of the incident response plan to [entity defined incident response personnel (identified by name and/or by role)].
11. Review the incident response plan [entity defined frequency].
12. Update the incident response plan to address system changes or problems encountered during plan implementation, execution, or testing.
13. Communicate incident response plan changes to [entity defined incident response personnel (identified by name and/or by role)].
14. Protect the incident response plan from unauthorized disclosure and modification.

# 5.0 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.

# 6.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | Definition |
|  |  |

# 7.0 Contact Information

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

**[Entity Address]**

# 8.0 Revision History

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

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

# 9.0 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 800-53a – Incident Response (IR), NIST SP 800-16, NIST SP 800-50, NIST SP 800-61, NIST SP 800-84, NIST SP 800-115

# 10.0 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.