|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Incident Response** | **Updated:** 10/26/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of this policy is to establish a clear and structured approach for identifying, containing, investigating, remedying, reporting, and responding to computer security incidents within the organization. By outlining specific responsibilities and processes for incident response, the policy aims to ensure that all employees, contractors, and third-party vendors can effectively address security threats, thereby minimizing potential damage to the organization’s information assets. This framework not only promotes a proactive stance toward cybersecurity but also fosters a culture of awareness and readiness among all stakeholders.

Implementing this policy provides several key benefits, including enhanced organizational resilience against cyber threats, improved incident response efficiency, and greater protection of sensitive information. By establishing standardized procedures and roles for incident response, the organization can reduce the time taken to detect and mitigate security incidents, thereby limiting operational disruption and potential financial losses. Additionally, regular training, testing, and incorporation of lessons learned foster continuous improvement in the organization’s cybersecurity posture. Ultimately, this policy not only safeguards information assets but also reinforces stakeholder confidence in the organization’s commitment to cybersecurity.

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

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

This policy outlines the framework for effectively managing computer security incidents within the organization. It defines the roles and responsibilities of all stakeholders involved in the incident response process, ensuring clarity and accountability. The policy establishes procedures for identifying, containing, investigating, remedying, reporting, and responding to security incidents, guided by best practices from the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. By adopting this structured approach, the organization aims to enhance its cybersecurity posture, protect sensitive information assets, and promote a culture of security awareness among all employees, contractors, and third-party vendors. Compliance with this policy is essential to ensure a coordinated response to incidents, minimize potential damages, and continuously improve the organization's incident response capabilities.

* 1. Incident Response Policy

[Organization Name] shall:

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

[Organization Name] 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.
   1. Incident Handling

[Organization Name] 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.
   1. Incident Monitoring

[Organization Name] shall employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

* 1. Incident Reporting

[Organization Name] 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].
   1. Incident Response Assistance

[Organization Name] shall:

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

# 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** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

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

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

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

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) SP: 800-61 - Computer Security Incident Handling Guide](https://csrc.nist.gov/pubs/sp/800/61/r2/final)

[National Institute of Standards and Technology (NIST) SP: 800-50 - Building a Cybersecurity and Privacy Learning Program](https://csrc.nist.gov/pubs/sp/800/50/r1/final)

[National Institute of Standards and Technology (NIST) SP: 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](https://csrc.nist.gov/pubs/sp/800/84/final)

[National Institute of Standards and Technology (NIST) SP: 800-53 - Security and Privacy Controls for Information Systems and Organizations](https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final)

[National Institute of Standards and Technology (NIST) SP: 800-92 - Guide to Computer Security Log Management](https://csrc.nist.gov/pubs/sp/800/92/final)