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

# 1.0 Purpose and Benefits

The purpose of the cybersecurity contingency planning policy is to establish a structured framework for ensuring the availability of critical Information Technology (IT) resources and information systems during unexpected disruptions. This policy aims to minimize the impact of service interruptions on essential business functions by outlining clear procedures for recovery, restoration, and maintenance of operations. By proactively planning for various types of disruptions—whether due to cyber incidents, natural disasters, or technical failures—the organization can safeguard its information assets and ensure continuity of operations, ultimately supporting its mission and strategic objectives.

Implementing this contingency planning policy provides numerous benefits, including enhanced resilience against service disruptions and a systematic approach to recovery. With clearly defined roles, responsibilities, and procedures, the organization can respond swiftly and effectively to incidents, thereby reducing downtime and associated losses. Regular testing and updates to the contingency plan foster a culture of preparedness among employees, ensuring they are equipped to act in emergencies. Additionally, this policy aids in compliance with industry standards and regulatory requirements, which often mandate the existence of contingency plans. By ensuring that essential functions remain operational, the organization can maintain stakeholder trust and protect its reputation in the face of challenges.

# 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 Cybersecurity Contingency Planning Policy is designed to ensure the continued availability of critical Information Technology (IT) resources and information systems during disruptions. It establishes procedures for recovery, restoration, and the maintenance of essential business functions in the event of incidents such as cyberattacks, natural disasters, or technical failures. All employees, contractors, and third-party vendors are required to familiarize themselves with this policy and adhere to its guidelines to protect organizational assets and ensure operational continuity. Compliance with this policy is essential for safeguarding the integrity and availability of the organization’s information systems.

* 1. Contingency Plan

The [Policy Owner] shall:

1. Develop a contingency plan for the information system, in direct guidance and association with the information system owner, that:
   1. Identifies essential missions and business functions and associated contingency requirements.
   2. Provides recovery objectives, restoration priorities, and metrics.
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information.
   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.
   6. Is reviewed and approved by the [owner], and information system’s owner management on at least an annual basis.
2. Distribute copies of contingency plans to key contingency personnel, identified by name and/or by business role.
3. Coordinate contingency planning activities with incident handling activities.
4. Update the contingency plan to address changes to the business owner’s mission, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
5. Communicate contingency plan changes to key contingency personnel identified by name and/or by business role.
6. Protect the contingency plan from unauthorized disclosure and modification.
   1. Contingency Training

The [Policy Owner] shall:

1. Provide contingency training to information system users consistent with assigned roles and responsibilities
2. Ensure designated personnel receive contingency training at least biannually of assuming a contingency role or responsibility, and when required by information system changes.
   1. Contingency Plan Testing

The [Policy Owner], along with information systems owners, shall:

1. Test the contingency plan for the information system, as determined by the mission critical nature of the business system(s) no less than annually.
2. Use strategic and tactical planning during testing to simulate a production information system to determine the effectiveness of the plan and the organizational readiness to execute the plan.
3. Review the contingency plan test results.
4. Initiate corrective actions, as needed.
5. Coordinate contingency plan testing with organizational elements responsible for related plans; plans related to contingency plans for information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans.
   1. Alternate Storage Site

The [Policy Owner] shall:

1. Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.
2. Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.
3. Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.
4. Identify and document potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.
   1. Alternate Processing Site

The [Policy Owner] shall:

1. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of the information system operations for essential missions/business functions within the time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.
2. Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the agreed upon time period for transfer/resumption.
3. Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site.
4. Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.
5. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.
6. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with business objectives and availability requirements.
   1. Telecommunications Services

The [Policy Owner] shall:

1. Establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within agreed upon recovery timeframes when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
2. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with agreed upon recovery objectives and availability requirements.
3. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.
   1. Information System Backup

The [Policy Owner] shall:

1. Conduct backups of user-level information contained in the information system defined by frequency consistent with recovery time and recovery point objectives.
2. Conduct backups of system-level information contained in the information system defined by frequency consistent with recovery time and recovery point objectives.
3. Conduct backups of information system documentation including security-related documentation defined by frequency consistent with recovery time and recovery point objectives.
4. Protect the confidentiality, integrity, and availability of backup information at storage locations.
5. Test backup information to verify media reliability and information integrity.
   1. Information System Recovery and Reconstitution

The [Policy Owner] shall:

1. Provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
2. Provide that the information system implements transaction recovery for systems that are transaction-based.

# 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 800-34, Contingency Planning Guide for Federal Information Systems](https://csrc.nist.gov/csrc/media/events/hipaa-2010-safeguarding-health-information-buil/documents/2-2b-contingency-planning-swanson-nist.pdf)

[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)