|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Media Protection** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of the Media Protection Policy is to establish a comprehensive framework for the management and protection of both digital and non-digital media containing sensitive information. This policy aims to ensure that access to media is restricted to authorized personnel, thereby safeguarding against unauthorized disclosure, alteration, or destruction of data. By defining clear protocols for media storage, transport, and sanitization, the policy helps mitigate risks associated with data breaches and ensures compliance with applicable federal regulations and organizational standards. Ultimately, the policy seeks to create a structured environment that prioritizes the integrity and confidentiality of the organization's information assets.

The benefits of the Media Protection Policy are multi-faceted, contributing to enhanced information security and operational efficiency. By restricting media access and defining robust storage and transport protocols, the policy minimizes the risk of data breaches, thereby protecting the organization from potential financial and reputational damage. Furthermore, the requirement for sanitization before disposal or reuse ensures that sensitive information is effectively destroyed, reducing the likelihood of data recovery by unauthorized individuals. Additionally, clear accountability and documentation requirements facilitate compliance with regulatory standards, ultimately fostering a culture of security awareness among staff. This comprehensive approach not only safeguards critical information but also instills confidence among stakeholders regarding the organization's commitment to data protection.

# 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

The Media Protection Policy establishes guidelines for managing access to, storage, transport, sanitization, and use of both digital and non-digital media within the organization. Its primary objective is to safeguard sensitive information by restricting access to authorized personnel, ensuring proper marking of media to indicate security protocols, and defining physical controls for secure storage. The policy mandates that all media be protected during transport and maintains accountability for their handling outside controlled areas. Additionally, it outlines stringent procedures for sanitizing media before disposal or reuse, ensuring compliance with federal and organizational standards. By prohibiting the use of unapproved security safeguards on entity-owned equipment, this policy reinforces a culture of security and integrity, aiming to mitigate risks associated with unauthorized access and data breaches.

* 1. Media Access

The [Owner] through direction from departments shall:

1. Restrict access to [entity defined types of digital and/or non-digital media] to [entity identified staff].
2. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.
   1. Media Storage

The [Owner] shall:

1. Specify staff to physically control and securely store media within defined controlled areas.
2. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
   1. Media Transport

The [Owner] shall:

1. Protect and control media during transport outside of controlled areas.
2. Maintain accountability for information system media during transport outside of controlled areas.
3. Document activities associated with the transport of information system media.
4. Restrict the activities associated with the transport of information system media to authorized personnel.
   1. Media Santization

The [Owner] shall:

1. Sanitize prior to disposal, release out of organizational control, or release for reuse using [entity specified standard] in accordance with applicable federal and organizational standards and policies.
2. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
   1. Media Use

The [Owner] shall prohibit the use of [entity defined types of information system media] on entity owned equipment using unapproved security safeguards.

# 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) Special Publications 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) Special Publications 800-88 – Guidelines for Media Sanitization](https://csrc.nist.gov/pubs/sp/800/88/r1/final)

[National Institute of Standards and Technology (NIST) Special Publications 800-111 – Guide to Storage Encryption Technologies for End User Devices](https://csrc.nist.gov/pubs/sp/800/111/final)