|  |  |
| --- | --- |
| **[Organization Name]**  **Information Technology Standard** | **No:** [Policy Number: e.g. POL-GOV-01] |
| **IT Standard**:  **Media Protection** | **Updated:** [Updated Date] |
| **Issued By:** [Authority: e.g. CEO or CIO]  **Owner:** [Owner: e.g. IT Department] |

# 1.0 Purpose and Benefits

To ensure that Information Technology (IT) controls access to and disposes of media resources in compliance with IT security policies, standards, and procedures.

# 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 [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.

# Information Statement

Needed

### 4.1 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.

### 4.2 Media Storage

The [Owner]

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.

### 4.3 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.

### 4.4 Media Sanitization

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.

### 4.5 Media Use

The [Owner] shall:

1. 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 |
|  |  |

# 8.0 Contact Information

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

[Organization Address & Policy Owner’s Contact Info]

# 9.0 Review and Revisions

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 (SP): NIST SP 800-53 – Media Protection (MP), NIST SP 800-12, NIST SP 800-56, NIST SP 800-57, NIST SP 800-60, NIST SP 800-88, NIST SP 800-100, NIST SP 800-111;  
NIST Federal Information Processing Standards (FIPS) 199