Removable Media Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

This policy governs the use of Removable Media used in ABC Company’s Information Systems.

# II. Purpose

This policy is established to minimize risks related to removable media and Sensitive Information.

# III. Scope

This policy applies to all Staff that access ABC Company’s Information Resources.

# IV. Policy

The Chief Security Officer shall ensure:

* Policies and procedures govern device and media (including USB storage devices) controls. Procedures specify how devices are to be identified when there are multiple devices of the same type. Procedures ensure inventory logs of all media are implemented and maintained. Media inventories shall be conducted at least annually.
* Procedures classify media so the sensitivity of the data can be determined. Procedures specify the types of hardware and electronic media (e.g. hard drives, backup media, optical discs, digital memory cards) that must be tracked.
* Procedures store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Procedures ensure a review the media storage location’s security at least annually.
* Procedures specify the record of the movements of hardware and electronic media and the person responsible for its movement. Procedures ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals). Procedures specify the receipt and removal of hardware and electronic media that contain sensitive information into and out of a facility, and the movement of those items within the facility. Media to be sent by secured courier or other delivery method that can be accurately tracked.
* Procedures for removal of sensitive information from electronic media before the media are available for reuse. Procedures specify situations where all sensitive information must be permanently deleted or when the electronic media should only be reformatted so that no files are accessible.
* Devices are configured to not auto-run content from removable media.

ABC Company Staff may only use ABC Company Removable Media. Removable Media may not be connected to or used in computers that are not owned or leased by ABC Company without explicit permission of the IT Department.

Sensitive information shall be stored on Removable Media only when required in the performance of assigned duties or when providing information on Removable Media as required by state or federal agencies. When sensitive information is stored on Removable Media, it must be encrypted in accordance with ABC Company’s Encryption Policy.

Data shall be copied or stored on Removable Media only by authorized access in the performance of official duties. Removable Media containing sensitive information shall have an external label that is marked and dated. Such external labeling shall include any special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates). Refer to the Data Classification Policy and Data Marking Policy for more information.

Except for backups, access controls shall prohibit copying, moving or storing sensitive data on local hard drives and removable media.

Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation. When in transit, sensitive data stored on Removable Media must not be left unattended, even temporarily, and must remain in an authorized employee’s physical control at all times.

Physical and environmental protection controls shall be provided for Removable Media containing sensitive data. Removable Media containing sensitive data must be kept in a secure safe or a locked cabinet and returned to safe storage during breaks and at the end of each work day.

Staff shall adhere to the requirements outlined in the Disposal Policy when disposing of Removable Media.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO12.02, APO12.07, APO14.01-02, APO14.10, MEA03.01

GDPR Article 25, 32

HIPAA 164.310(d)(1), 164.310(d)(2)(i), 164.310(d)(2)(ii), 164.310(d)(2)(iii)

ISO 27001:2013 7.5.2, A.8.3, A.11.2.7, A.11.2.9

NIST SP 800-37 3.2, 3.4

NIST SP 800-53 3.11 (MP-1-8), MA-2, PE-6, PE-16, SC-28

NIST Cybersecurity Framework PR.AC-2, PR.PT-2, ID.RA-6, DE.CM-2, RS.MI-2

PCI 3.4, 9.1, 9.5-10