|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Backup and Recovery Policy | | | | | |
| Policy # | CPL-14-01 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457909466)

[Scope 1](#_Toc457909467)

[Policy 1](#_Toc457909468)

[Backup Schedule 1](#_Toc457909469)

[Software and Application Backup 2](#_Toc457909470)

[User Responsibilities 2](#_Toc457909471)

[Backup Locations 2](#_Toc457909472)

[Media 2](#_Toc457909473)

[Testing and Review 3](#_Toc457909474)

[Violations 3](#_Toc457909475)

[Definitions 3](#_Toc457909476)

[References 4](#_Toc457909477)

[Related Documents 4](#_Toc457909478)

[Approval and Ownership 4](#_Toc457909479)

[Revision History 4](#_Toc457909480)

Purpose

This policy defines the requirements for maintaining and recovering backup copies of sensitive Company X information created, processed, or stored on Company X computer and communications systems.

Scope

This policy applies to all Company X computer systems and facilities, with a target audience of Company X Information Technology employees and partners.

Policy

### ****Backup Schedule****

**Regular Data Backups -** All critical business information and critical software resident on Company X computer systems must be periodically backed-up on at least a weekly basis.

**Incremental Backup Process** - Incremental backups for all end-user files must be performed by the on-duty administrator starting at 6:00 PM each business day with exception of Friday when a full backup of all files must be performed.

**Critical Information Backups** - Critical business information and critical software must be backed-up at least quarterly onto archival storage media and kept for at least one year.

### ****Software and Application Backup****

**Master Copies Of Software -** All personal computer software must be copied prior to its initial usage, these master copies must be stored in a safe and secure location, and these master copies must not be used for ordinary business activities.

**Information Preservation After Application Decommission** - Before any Company X product applications are taken out of production, a final backup of all sensitive production data must be made and preserved for at least three (3) years.  Backup media that store this production data must contain a classification label which matches the highest (most sensitive) classification of the data being stored.

### ****User Responsibilities****

**Copies Of Sensitive, Critical, Or Valuable Information** - Unless other backup arrangements are known to be operational, all end users are responsible for making at least two current backup copies of critical files each time that a significant number of changes are saved.

**Automatic Backups** - All users with local area network connections must leave their computers turned on at night for the execution of automatic backup processes.

### ****Backup Locations****

**On-Site Backup Files** - At least one generation of backup files must be maintained on off-line data storage media wherever production computers are located.

**Multiple Backup Copies** - At least two recent and complete backups made on different dates containing critical Company X records must always be stored off-site.

**Backup Media Location** - Essential business information and software backups must be stored in a site that is a sufficient distance away from the originating facility.

### ****Backup Media****

**Backup Media Storage** - Essential business information and software backups must be stored in an environmentally protected and access-controlled site.

**Backup Media Fire Zone** - Computer and network backup storage media must be stored in a separate fire zones from the machine producing the backup.

**Backup Media Storage Units** - Unless they have a closing mechanism that is triggered by a fire alarm, all areas where backup media is stored including, but not limited to, fireproof computer backup storage rooms, vaults, and cabinets must be kept fully closed when not in active use.

**Archival Storage Directory** - All archival backup data stored off-site must be reflected in a current directory that shows the date when the information was most recently modified and the nature of the information.

**Archival Storage Preservation** - Computer media storage procedures must assure that sensitive, critical, or valuable information stored for prolonged periods of time is not lost due to deterioration.

**Backup Media Encryption** - All sensitive, valuable, or critical information recorded on backup computer media and stored outside Company X offices must be encrypted.

### ****Testing and Review****

**Archival Storage Media Testing** - Critical business information and critical software archived on computer storage media for a prolonged period of time must be tested at least annually to provide assurance that they can be fully recovered.

**Archival Storage Media Quality** - The computer data media used for storing sensitive, critical, or valuable information must be high quality and must be periodically tested for reliability.

**Backup Review** - Department managers or their delegates must ensure that proper backups of sensitive, critical and valuable data are being made if such data is resident on personal computers, workstations, or other small systems in their area.

**Backup Information Review** - All files and messages stored on Company X systems are routinely copied to tape, disk, and other storage media and must be recoverable for potential examination at a later date by Systems Administrators and others designated by management.

**Backup Media Storage Review** - Each location that is used to store Company X media backups must be reviewed at least annually to determine that the backup media storage is secure.

**Restoring Critical Backup Files** - Critical data that has been backed up must not be used for data restoration purposes unless another backup copy of the same data exists on different computer storage media. If this additional copy does not presently exist, before the restoration, the copy must first be made on a computer other than the one where the restoration is to take place.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

**Backup** - A copy of files and programs made to facilitate recovery if necessary.

**Business Continuity Plan (BCP)** - The documentation of a predetermined set of instructions or procedures that describe how an organization’s business functions will be sustained during and after a significant disruption.

**Information Asset** - Any Company X data in any form, and the equipment used to manage, process, or store Company X data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

**Partner** - Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

References

CPL: 14.01 Backup and Recovery

ISO/IEC 27002: 12.3 Backup

HIPAA: Contingency Plan 164.308(a)(7) - Data Backup Plan (R)

NIST: CP-9 Information System Backup

PCI-DSS: 9.5.1 Backup Media Storage

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYYY |  |
|  |  |  |  |  |