# Data Security Plan Template

**Purpose**

Data moves through a number of states throughout its lifecycle. Accounting for the security of the data during each of these states is necessary to ensure the confidentiality and integrity of the data and is required in order to meet compliance standards. By addressing and documenting the controls below you can establish a comprehensive data security plan.

**Scope**

This security plan covers all computing and data resources used throughout the firm.

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Date** | **Items revised** | **Author** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Identification**

The first step in establishing an effective security plan is identifying all the assets and data that are covered by the plan. It is important to document responsible parties, locations, and unique identifiers for these assets, as this provides an auditable record that may be referenced as needed for implementing security measures and investigating incidents. Below are two sets of inventories that should be completed and expanded as appropriate. *The first several lines contain examples* *of inventory entries and should be removed from your plan.*

**Asset Inventory**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Asset Name** | **Make** | **Model** | **Serial #** | **Owner** | **Use** |
| *Desktop* | *PC\_1* | *Dell* | *Latitude E6530* | *12ABC34* | *Company name* | *Internal* |
| *Laptop* | *John\_PC* | *Lenovp* | *Thinkpad* | *XYZ1234* | *Employee Ed* | *Out of office* |
| *Thumbdrive* | *None* | *None* | *None* | *None* | *Company name* | *Out of office* |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

#### Data Inventory

|  |  |  |
| --- | --- | --- |
| **Data Type** | **Storage Location** | **Responsible person** |
| *E-files* | *Server* | *Nathan* |
| *Tax software files* | *Server* | *Nathan* |
| *Paper client files* | *Throughout office* | *All preparers* |
| *Outgoing mail* | *Front desk* | *Amanda* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Secure Storage**

Data, and the assets containing that data, should be stored in a manner commensurate with their sensitivity.

**Physical Security Controls**

Physical security controls address all aspects of in-person access to data or computing resources. They can be used to deter or prevent unauthorized physical access to assets. In the charts below, indicate physical security controls protecting computing assets/data storage locations and, where appropriate, describe their implementation.

**Monitoring / Alert Systems**

Monitoring and alert systems allow monitoring of physical access and, at times, immediate notification that access has occurred. Examples of monitoring/alert systems include alarmed doors and security cameras.

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Item** | **Location** | **Purpose & Details** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Security Personnel**

Security personnel may monitor facilities or verify identities of other personnel. Example of security personnel include guards and receptionists.

|  |  |  |  |
| --- | --- | --- | --- |
| **Job Title** | **Location** | **Hours** | **Purpose** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Access Restrictions**

Access restrictions are checkpoints at which proof of authorization is required in order to gain physical access. Examples of access restrictions include badge requirements and locked doors requiring keys, codes, or biometrics.

|  |  |  |  |
| --- | --- | --- | --- |
| **Location** | **Restriction** | **Details** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Environmental Controls**

Environmental controls ensure that assets containing sensitive data are not destroyed by accidental or malicious events in their immediate surroundings, such as fire or power outage. Examples of environmental controls include temperature monitoring/alerts and backup power.

|  |  |  |  |
| --- | --- | --- | --- |
| **Environmental Control** | **Location** | **Details** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Visitation Policies**

Visitation policies establish the number and authorization requirements for any individual wishing to gain physical access to data or assets. Examples of visitation policies include sign-in sheets and requirements for temporary badges or photo IDs.

|  |  |  |  |
| --- | --- | --- | --- |
| **Restriction** | **Location** | **Details** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Anti-Theft/Anti-Tampering Controls**

Anti-theft/anti-tampering controls prevent or track unauthorized removal of or changes to physical assets. Examples of anti-theft/anti-tampering controls include tracking devices and computer case or peripheral equipment locks.

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Item** | **Location** | **Details** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Other**

Describe other physical security controls, as appropriate.

|  |
| --- |
|  |
|  |
|  |
|  |

**Security Features/Configurations**

In addition to physical protections, technological protections should be installed or configured on assets containing sensitive data.

**Antiviral Software**

Antiviral software prevents the installation of malicious software on assets containing sensitive data. Examples of antiviral software include Symantec Antivirus, Malwarebytes, and Windows Defender.

|  |  |  |  |
| --- | --- | --- | --- |
| **Software Name** | **Location** | **Date Last Updated** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Monitoring/Alerting Software**

Monitoring/alerting software periodically examines activity on systems, looking for indicators of compromise and sometimes triggering notification when certain thresholds are reached. Examples of monitoring/alerting software include Nagios and Solar Winds.

|  |  |  |  |
| --- | --- | --- | --- |
| **Software Name** | **Location** | **Date Last Verified** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Logging Utilities**

Logging utilities provide evidence of activity on the system that can be used to audit access and identify incidents. Examples of logging utilities include Windows Event Monitor and Logger.

|  |  |  |  |
| --- | --- | --- | --- |
| **Software Name** | **Location** | **Date Last Verified** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**File-Level or Full Disk Encryption**

File-level or full disk encryption prevents unauthorized access to data by encoding files, folders, or entire operating systems such that only authorized individuals with the decoding key may gain access. Examples of file-level or full disk encryption utilities include FileVault, Bitlocker, and Symantec PGP.

|  |  |  |  |
| --- | --- | --- | --- |
| **Encrypted Item** | **Details** | **Date Last Updated** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Host and/or Network Firewalls**

Firewalls prevent unauthorized access to data over the network by inspecting and allowing or disallowing network traffic at the asset or network level. Examples of host firewall tools available for assets include Windows Firewall and iptables. Examples of network firewalls include Juniper and Cisco network devices.

|  |  |  |  |
| --- | --- | --- | --- |
| **Software Name** | **Location & Details** | **Date Last Updated** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

####

**Backup and Retention**

To protect against the loss of integrity or availability of data, backup and retention policies and controls must be in place.

**Secure Backups**

The existence and location of backups should be determined by the sensitivity of data and the legal, contractual, or other restrictions regarding storage locations. This may involve prohibitions against backups or, conversely, requirements that backups be made and stored at a separate physical location than in-use data. Examples of backup locations include cloud services such as CrashPlan and internal or external RAID arrays.

Backup frequency and schedule should be determined by workflow requirements and legal, contractual, or other restrictions. Examples of considerations for backup frequency and scheduling include how often changes are made to data and what extent of data loss can be tolerated.

|  |  |  |  |
| --- | --- | --- | --- |
| **Backup Method** | **Frequency** | **Responsible person** | **Date Last Verified** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Disaster Recovery/Business Continuity Planning**

Disaster recovery/business continuity planning outlines the company’s response to potential risks such as security breaches or natural disasters. Examples include data restoration plans, off-site redundancy, and procedures for identification and escalation of security incidents.

|  |  |  |  |
| --- | --- | --- | --- |
| **Anticipated Disaster/Problem** | **Planned Response** | **Responsible Person** | **Required Reporting** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Data Retention**

Data retention policies establish the requirements and procedures for long-term data storage and data removal. Retention of sensitive data beyond its useful life may expose the company to unnecessary risk in the event of a security incident. Examples of data retention policies include maximum and minimum periods of time for data retention and long-term storage locations.

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Type** | **Maximum Retention Period** | **Disposal Method** | **Responsible Person** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### Secure Shredding Services

Secure shredding services remove data from an asset in a manner that makes it highly difficult or impossible to retrieve. Examples of secure shredding services include hard drive destruction, paper shredders, and the security software Eraser.

|  |  |  |
| --- | --- | --- |
| **Data Type** | **Disposal Method** | **Responsible Person** |
|  |  |  |
|  |  |  |
|  |  |  |

**Other**

Describe other backup and retention controls, as appropriate.

|  |
| --- |
|  |
|  |
|  |
|  |

**Secure Transmission**

In addition to protecting data in its storage locations, data must be protected in transit between systems.

**Data Flow**

The first step in understanding how to protect data during transmission is to identify the assets or systems between which data is transferred and the path that data takes. Once the flow of data between systems is understood, security controls that protect the data in transit can be employed. Attach a diagram or description of the flow of data, both internal and external to the company.

*See Attachment 1.*

**Network Encryption**

Network encryption prevents unauthorized access to data by encoding data as it travels across a network such that only authorized individuals with the decoding key may gain access. Examples of network encryption include HTTPS, SSL/TLS, and VPN tunnels.

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Type Being Transferred** | **From** | **To** | **Encryption Method** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Network Isolation/Segmentation**

Network isolation/segmentation provides a private network to which users must authenticate and over which data may travel more securely.

|  |
| --- |
| **Private Network Details** |
|  |
|  |
|  |

**Data Transmission Policies**

Data transmission policies establish acceptable methods of transmission for data. Examples of data transmission policies include prohibition of data transmission via e-mail or fax.

|  |  |
| --- | --- |
| **Data Type**  | **Restrictions** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Data Loss Prevention Software**

Data loss prevention software inspects data that a user intends to transmit via a variety of technical methods and allows or disallows the action as configured by administrators. For example, Symantec DLP, Websense, McAfee Total Protection, etc.

|  |  |  |
| --- | --- | --- |
| **Software Name** | **Location** | **Date Last Updated** |
|  |  |  |
|  |  |  |
|  |  |  |

**Other**

Describe other data transmission controls, as appropriate.

|  |
| --- |
|  |
|  |
|  |
|  |

**Authentication and Authorization**

Access to sensitive data should be restricted to a specific set of individuals with a specific set of permissions. Indicate authentication and authorization access controls in place to protect data and, where appropriate, describe their implementation.

**Least Privilege**

The principle of least privilege requires that each user be assigned the minimum permissions level required in order to perform job functions. This includes both the breadth of access (what data is accessible) and the depth of access (what actions the user is able to perform on that data).

|  |  |  |
| --- | --- | --- |
| **Data Type** | **Location** | **Restriction** |
|  |  |  |
|  |  |  |
|  |  |  |

**Individual Login Credentials**

Separate login credentials (vs. shared accounts) allow data access and activities on a system to be traced to individuals and permissions to be assigned on a need-to-know basis. It may be appropriate to give some individuals two sets of login credentials; one for administration duties and one for general data access and use. It is important that Company know all log-in and password information for all users for all systems!

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item Accessing** | **Person** | **Log-In** | **Password** | **Date Update Required** |
| *Lisa desktop* | *Lisa* | *Lisa* | *L4ifmI9* | *1-1-20* |
| *Lacerte* | *Lisa* | *LisaIhm* | *I284729mm* | *1-1-20* |
| *Quickbooks* | *Lisa* | *LisaIhm* | *I284729mm* | *1-1-20* |
| *Calendar* | *All staff* | *Company* | *929292mmm* | *1-1-20* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Strong Password Requirements**

Strong password requirements ensure that authentication credentials used to access sensitive data cannot be easily guessed or brute-forced. Examples of strong password requirements include complexity specifications (length, character type) and expiration/renewal deadlines.

|  |  |  |
| --- | --- | --- |
| **Item Accessing** | **Password Requirement** | **Time Before Change Required** |
|  |  |  |
|  |  |  |
|  |  |  |

**Authentication Checkpoints**

Authentication checkpoints are used to affirm or reaffirm access permissions at various stages of data access. Examples of authentication checkpoints include pre- boot BIOS or encryption login, operating system login, and application login

|  |  |
| --- | --- |
| **Item Accessing** | **Authentication Method** |
|  |  |
|  |  |
|  |  |

**Audit Logs**

A record of both failed and successful login attempts can help identify attempts to breach a system and gain unauthorized access to data.

|  |  |  |
| --- | --- | --- |
| **Item Logged** | **Review Frequency** | **Responsible Person** |
|  |  |  |
|  |  |  |
|  |  |  |

**Secure Hiring, Termination, and Role Change Practices**

Secure hiring, termination, and role change practices ensure that access to data is appropriately granted, altered, and revoked as appropriate. Examples of secure hiring, termination, and role change practices include background checks, confidentiality agreements, procedures for deactivating credentials, changing access permissions and passwords, and security awareness and policy training.

|  |
| --- |
| **Hiring** |
|  **Action Required** | **Time Period** | **Responsible Person** |
| *Background check* |  |  |
| *Confidentiality agreement* |  |  |
| *Security training* |  |  |

|  |
| --- |
| **Termination** |
|  **Access Deactivation** | **Time Period** | **Responsible Person** |
| *Desktop* |  |  |
| *Tax software* |  |  |
| *E-file cabinet* |  |  |
| *Keys* |  |  |
| *Alarm system* |  |  |
| *Internal lockbox* |  |  |

**Other**

Describe other authentication, authorization, or access controls, as appropriate.

|  |
| --- |
|  |
|  |
|  |
|  |