**Essential Elements of a Data Security Policy**

1. **Safeguard Data Privacy:** Employees must understand that your privacy policy is a pledge to your customers that you will protect their information. Data should only be used in ways that will keep customer identity and the confidentiality of information secure. Of course, your employees and organizations must conform to all applicable laws and regulations.
2. **Establish Password Management:** A password policy should be established for all employees or temporary workers who will access corporate resources. In general, [password complexity](https://www.travelers.com/resources/cyber-security/password-security-tips.aspx) should be established according to the job functions and data security requirements. Passwords should never be shared.
3. **Govern Internet Usage:** Most people use the internet without a thought to the harm that can ensue. Employee misuse of the internet can place your company in an awkward, or even illegal, position. Establishing limits on employee internet usage in the workplace may help avoid these situations. Every organization should decide how employees can and should access the web. You want employees to be productive, and this may be the main concern for limiting internet usage, but security concerns should also dictate how internet guidelines are formulated.
4. **Manage Email Usage:** Many data breaches are a result of employee misuse of email that can result in the loss or theft of data and the accidental downloading of viruses or other malware. Clear standards should be established regarding use of emails, message content, encryption and file retention.
5. **Govern and Manage Company-Owned Mobile Devices:** When organizations provide mobile devices for their employees to use, a formal process should be implemented to help ensure that mobile devices are secure and used appropriately. Requiring employees to be responsible for protecting their devices from theft and requiring password protection in accordance with your password policy should be minimum requirements.
6. **Establish an Approval Process for Employee-Owned Mobile Devices:** With the increased capabilities of consumer devices, such as smart phones and tablets, it has become easy to interconnect these devices to company applications and infrastructure. Use of these devices to interconnect to company email, calendaring and other services can blur the lines between company controls and consumer controls. Employees who request and are approved to have access to company information via their personal devices should understand and accept the limitations and controls imposed by the company.
7. **Govern Social Media:** All users of social media need to be aware of the risks associated with social media networking. A strong social media policy is crucial for any business that seeks to use social networking to promote its activities and communicate with its customers. Active governance can help ensure employees speak within the parameters set by their company and follow data privacy best practices.
8. **Oversee Software Copyright and Licensing:** There are many good reasons for employees to comply with software copyright and licensing agreements. Organizations are obliged to adhere to the terms of software usage agreements and employees should be made aware of any usage restrictions. Also, employees should not download and use software that has not been reviewed and approved by the company.
9. **Report Security Incidents:** A procedure should be in place for employees or contractors to report malicious malware in the event it is inadvertently imported. All employees should know how to report incidents of malware and what steps to take to help mitigate damage.

**Three Data Security Policies**

This document provides three example data security policies that cover key areas of concern. They should not be considered an exhaustive list but rather each organization should identify any additional areas that require policy in accordance with their users, data, regulatory environment and other relevant factors.

# The three policies cover:

1. Data security policy: Employee requirements
2. Data security policy: Data Leakage Prevention – Data in Motion
3. Data security policy: Workstation Full Disk Encryption.

## Data security policy: Employee requirements

### Using this policy

This example policy outlines behaviors expected of employees when dealing with data and provides a classification of the types of data with which they should be concerned. This should link to your AUP (acceptable use policy), security training and information security policy to provide users with guidance on the required behaviors.

1.0 Purpose

<Company X> must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of data in scope is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. It’s primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

* 1. Scope
     1. Any employee, contractor or individual with access to <Company X> systems or data.
     2. Definition of data to be protected (you should identify the types of data and give examples so that your users can identify it when they encounter it)
* PII
* Financial
* Restricted/Sensitive
* Confidential
* IP
  1. Policy – Employee requirements
     1. You need to complete <Company X>’s security awareness training and agree to uphold the acceptable use policy.
     2. If you identify an unknown, un-escorted or otherwise unauthorized individual in <Company X> you need to immediately notify <complete as appropriate>.
     3. Visitors to <Company X> must be escorted by an authorized employee at all times. If you are responsible for escorting visitors you must restrict them to appropriate areas.
     4. You are required not to reference the subject or content of sensitive or confidential data publicly, or via systems or communication channels not controlled by <Company X>. For example, the use of external e-mail systems not hosted by <Company X> to distribute data is not allowed.
     5. Please keep a clean desk. To maintain information security you need to ensure that data is not left unattended at your workstation.
     6. You need to use a secure password on all <Company X> systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
     7. Terminated employees will be required to return all records, in any format, containing personal information. This requirement should be part of the employee onboarding process with employees signing documentation to confirm they will do this.
     8. You must immediately notify <complete as appropriate> in the event that a device containing data is lost (e.g. mobiles, laptops etc).
     9. In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform <complete as appropriate> so that they can take appropriate action.
     10. If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Seek guidance from <complete as appropriate> if you are unsure as to your responsibilities.
     11. Please ensure that assets holding data are not left unduly exposed, for example visible in the back seat of your car.
     12. Data that must be moved within <company X> is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). <Company X> will provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle in scope data. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with <complete as appropriate>.
     13. Any information being transferred on a portable device (e.g. USB stick, laptop) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding the requirements, seek guidance from

<complete as appropriate>)

## Data security policy: Data Leakage Prevention – Data in Motion

### Using this policy

This example policy is intended to act as a guideline for organizations looking to implement or update their DLP controls. Adapt this policy, particularly in line with requirements for usability or in accordance with the regulations or data you need to protect. This policy provides a framework for classes of data that may wish to be monitored. You should expand them to cover the sensitive assets in your business and subject to the types of you hold.

### Background to this policy

Data leakage prevention is designed to make users aware of data they are transferring which may be sensitive or restricted in nature.

1.0 Purpose

<Company X> must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of data is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. It’s primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

* 1. Scope
     1. Any <Company X> device which handles customer data, sensitive data, personally identifiable information or company data. Any device which is regularly used for e-mail, web or other work related tasks and is not specifically exempt for legitimate business or technology reasons.
     2. The <Company X> information security policy will define requirements for handling of information and user behavior requirements. This policy is to augment the information security policy with technology controls.
     3. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted being authorized by security management. See **Risk Assessment** process (reference your own risk assessment process).
  2. Policy
     1. <Company X’s> data leakage prevention (DLP) technology will scan for data in motion.
     2. The DLP technology will identify large volumes (thus, of high risk of being sensitive and likely to have significant impact if handled inappropriately) of data. A large number of records is defined as <complete as appropriate> (tailor to your enterprise’s stance e.g. 1000 records).

Data is defined as: (you should adjust this to reflect the data that you are regulated on, or that which could be most damaging to your organization. The below is an appropriate template for many organizations)

* + - 1. Credit card details, bank account numbers and other financial identifiers
      2. E-mail addresses, names, addresses and other combinations of personally identifiable information
      3. Documents that have been explicitly marked with the ‘<Company X> Confidential’ string.
    1. DLP will identify specific content, i.e.:
       1. Sales data – particularly forecasts, renewals lists and other customer listings
       2. Exports of personally identifiable information outside controlled systems (this is data that you are particularly concerned about losing and wish to ensure is detected by the DLP policy).
    2. DLP will be configured to alert the user in the event of a suspected transmission of sensitive data, and the user will be presented with a choice to authorize or reject the transfer. This allows the user to make a sensible decision to protect the data, without interrupting business functions. Changes to the DLP product configuration will be handled through the

<Company X> IT change process and with security management approval, to identify requirements to adjust the information security policy or employee communications.

* + 1. DLP will log incidents centrally for review. The IT team will conduct first level triage on events, identifying data that may be sensitive and situations where its transfer was authorized and there is a concern of inappropriate use. These events will be escalated to HR to be handled through the normal process and to protect the individual. (you will need to tailor this for your organisation. It is common to defer enforcement to business owners of data rather than having IT conduct the triage).
    2. Where there is an active concern of data breach, the IT incident management process is to be used with specific notification provided to <complete as appropriate> (for example HR, Legal and Security Management).
    3. Access to DLP events will be restricted to a named group of individuals to protect the privacy of employees. A DLP event does not constitute evidence that an employee has intentionally, or accidentally lost data but provides sufficient basis for investigation to ensure data has been appropriately protected.
  1. Technical guidelines

Technical guidelines identify requirements for technical implementation and are typically technology specific.

* + 1. The technology of choice is <complete as appropriate>
    2. The product will be configured to identify data in motion to Browsers, IM Clients, E-mail clients, Mass storage devices and writable CD media.
  1. Reporting requirements
     1. Weekly reports of incidents to <complete as appropriate>
     2. High priority incidents discovered by IT should be immediately flagged with <complete as appropriate>
     3. Monthly report showing % devices compliant with DLP policy.

## Data security policy: Workstation Full Disk Encryption

### Using this policy

This example policy is intended to act as a guideline for organizations looking to implement or update their full disk encryption control policy. Adapt this policy, particularly in line with requirements for usability or in accordance with the regulations or data you need to protect.

### Background to this policy

Full disk encryption is now a key privacy enhancing technology which is mandated my many regulatory guidelines.

1.0 Purpose

<Company X> must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. A collection of global regulations (such as <complete as appropriate>) also require the protection of a broad scope of data, which this policy supports by restricting access to data hosted on <complete as appropriate> devices.

As defined by numerous compliance standards and industry best practice, full disk encryption is required to protect against exposure in the event of loss of an asset. This policy defines requirements for full disk encryption protection as a control and associated processes.

* 1. Scope
     1. All <Company X> workstations – desktops and laptops (depending on the type of data you hold and physical security some organizations adjust this just to cover laptops).
     2. All <Company X> virtual machines.
     3. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted being authorized by security management. See **Risk Assessment** process (reference your own risk assessment process).
  2. Policy
     1. All devices in scope will have full disk encryption enabled.
     2. <Company X’s> Acceptable Use Policy (AUP) and security awareness training must require users to notify <complete as appropriate> if they suspect they are not in compliance with this policy as per the AUP.
     3. The AUP and security awareness training must require users to notify <complete as appropriate> of any device which is lost or stolen.
     4. Encryption policy must be managed and compliance validated by <complete as appropriate>. Machines need to report to the central management infrastructure to enable audit records to demonstrate compliance as required.
     5. Where management is not possible and a standalone encryption is configured (only once approved by a risk assessment), the device user must provide a copy of the active encryption key to IT.
     6. <Complete as appropriate> has the right to access any encrypted device for the purposes of investigation, maintenance or the absence of an employee with primary file system access. <complete as appropriate, AUP and security awareness training will advise users of this requirement. (Depending on your AUP, or agreement with employees you will want to alter the stance of this policy requirement).
     7. The encryption technology must be configured in accordance with industry best practice to be hardened against attacks.
     8. All security related events will be logged and audited by <complete as appropriate> to identify inappropriate access to systems or other malicious use.
     9. The <complete as appropriate> help desk will be permitted to issue an out-of-band challenge/response to allow access to a system in the event of failure, lost credentials or other business blocking requirements. This challenge/response will be provided only in the event that the identity of the user can be established using challenge and response attributes documented in the password policy.
     10. (Some enterprises may have a requirement to practice a tiered approach to data security. This may involve a set of users that have particularly sensitive data and require greater security. You can remove this if this is not a requirement of your business).

A group of sensitive data/VIP users will be identified by the restricted data policy. Users in this group will require a member of <complete as appropriate> (e.g. Senior Management or IT) authorization for key changes or challenge response. The help desk will not be permitted to access said systems without authorization. These systems are identified as having access to highly sensitive, restricted use data and have a requirement for separation of duty. Where identified by the authentication and restricted data policy, a system/user will be required to use two factor authentications in accordance with the <complete as appropriate> defined standard. The authentication will occur in the pre boot environment.

* + 1. Configuration changes are to be conducted through the <complete as appropriate> change control process, identifying risks and noteworthy implementation changes to security management.
  1. Technical guidelines

Technical guidelines identify requirements for technical implementation and are typically technology specific.

* + 1. <Complete as appropriate> is the standard product.
    2. Strong, industry best practice defined cryptographic standards must be employed. AES-256 is an approved implementation.
    3. The BIOS will be configured with a secure password (as defined by password policy) that is stored by IT. The boot order will be fixed to the encrypted HDD. If an override is required by a user for maintenance or emergency use, the helpdesk can

authenticate the user and then provide the password for the BIOS. The objective being to avoid an attacker cold booting and attacking the system.

* + 1. Synchronization with Windows credentials will be configured so that the pre boot environment is matched to the user’s credentials and only one logon is required.
    2. A pre boot environment will be used for authentication. Credentials will be used to authenticate the user in compliance with

<complete as appropriate>password security policy. (Some enterprises have a requirement to use two factor, and this should be reflected here as required).

* 1. Reporting requirements
     1. A monthly report that identifies the % of encrypted systems versus assets in scope
     2. A monthly report that identifies the compliance status of managed, encrypted systems
     3. A monthly report that identifies the number of lost assets and validation that lost devices have been handled appropriately.

**Company data protection policy**

This **Company Data Protection Policy** template is ready to be tailored to your company’s needs and should be considered a starting point for setting up your employment policies.

# Policy brief & purpose

Our **Company Data Protection Policy** refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

# Scope

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

**Who is covered under the Data Protection Policy?**

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

# Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

Accurate and kept up-to-date

Collected fairly and for lawful purposes only

Processed by the company within its legal and moral boundaries

* Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

* Communicated informally
* Stored for more than a specified amount of time
* Transferred to organizations, states or countries that do not have adequate data protection policies
* Distributed to any party other than the ones agreed upon by the data’s owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

Let people know which of their data is collected Inform people about how we’ll process their data

Inform people about who has access to their information

Have provisions in cases of lost, corrupted or compromised data

Allow people to request that we modify, erase, reduce or correct data contained in our databases

# Actions

To exercise data protection we’re committed to:

Restrict and monitor access to sensitive data Develop transparent data collection procedures

Train employees in online privacy and security measures Build secure networks to protect online data from [cyberattacks](https://resources.workable.com/cyber-security-policy)

Establish clear procedures for reporting privacy breaches or data misuse Include contract clauses or communicate statements on how we handle data

Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Our data protection provisions will appear on our website.

# Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

Disclaimer: This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. The author nor Workable will assume any legal liability that may arise from the use of this policy.

#### **Sample Clean Desk Policy**

#### 1. Overview

a. The purpose for this policy is to establish a culture of security and trust for all employees at (company). An effective clean desk effort involving the participation and support of all (Company Name) employees can greatly protect paper documents that contain sensitive information about our clients, customers and vendors. All employees should familiarize themselves with the guidelines of this policy.

#### 2. Purpose

a. The main reasons for a clean desk policy are:

i. A clean desk can produce a positive image when our customers visit the company.

ii. It reduces the threat of a security incident as confidential information will be locked away when unattended.

iii. Sensitive documents left in the open can be stolen by a malicious entity.

#### 3. Responsibility

a. All staff, employees and entities working on behalf of [COMPANY] are subject to this policy

#### 4. Scope

a. At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.

b. At the end of the working day the employee is expected to tidy their desk and to put away all office papers. (Company) provides locking desks and filing cabinets for this purpose.

#### 5. Action

a. Allocate time in your calendar to clear away your paperwork.

b. Always clear your workspace before leaving for longer periods of time.

c. If in doubt - throw it out. If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to place it in the shred bin.

d. Consider scanning paper items and filing them electronically in your workstation.

e. Use the recycling bins for sensitive documents when they are no longer needed.

f. Lock your desk and filing cabinets at the end of the day

g. Lock away portable computing devices such as laptops or PDA devices

h. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

#### 6. Enforcement

a. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

#### 7. Revision History

a. Policy is in effect on (date)

b. Document revised on (date)

Computer and Email Usage Policy

To help you do your job, COMPANY may give you access to computers, computer files, the email system, and software. You should not use a password, access a file, or retrieve any stored communication without authorization. To make sure that all employees follow this policy, we may monitor computer and email usage.

We try hard to have a workplace that is free of harassment and sensitive to the diversity of our employees. Therefore, we do not allow employees to use computers and email in ways that are disruptive, offensive to others, or harmful to morale.

At COMPANY you may not display, download, or email sexually explicit images, messages, and cartoons. You also may not use computers and email for ethnic slurs, racial comments, off-color jokes, or anything that another person might take as harassment or disrespect.

You may not use email to ask other people to contribute to or to tell them about businesses outside of COMPANY religious or political causes, outside organizations, or any other non-business matters.

COMPANY buys and licenses computer software for business purposes. We do not own the copyright to this software or its documentation. Unless the software developer authorizes us, we do not have the right to use the software on more than one computer.

You may only use software on local area networks or on multiple machines according to the software license agreement. COMPANY prohibits the illegal duplication of software and its documentation.

If you know about any violations to this policy, notify your supervisor, the Human Resources Department or any member of management. Employees who violate this policy are subject to disciplinary action, up to and including termination of employment.

Sample Policy:

XXX is dedicated to providing the best possible service and security for our clients. We apply this client-focused approach to every aspect of our services; that includes investing as much time and attention protecting the security of our clients' data and materials as with any other aspect of our operations.

To that end, XXX has made data and physical plant security a core attribute of our business. This high level of security has been achieved through standard business practices of major data centers and financial institutions, as well as the development of extensive operating procedures and investments in security measures.

The following are specific and detailed aspects of how XXX has addressed security issues in numerous areas.

The keys to maintaining our high level of security and ensuring our continued focus are:

**People**

* XXX utilizes strict written security protocols that each staff member must adhere to as a condition of his/her employment
* Visitors' and vendors' access to our premises is highly controlled. Throughout their visits, all guests must be accompanied by employee escorts. Access to any area must include proper authorization for employees and visitors.
* Security background checks are conducted on all new employees.
* All employees are bonded.

**Facilities**

* Exterior doors are opened only with valid security code. For those few doors not designed to be entered from the outside (such as fire escape accessibility), an alarm sounds whenever they are opened.
* Key production facilities are video and sight monitored 24 hours a day.
* Security partitions at key entrances in production areas allow for deliveries and pick-ups without the need for visitors to access the shop floor.
* All warehousing is done within one central, on-site secured area, featuring the same security levels as our production areas.
* Warehouse employees visually inspect all incoming shipments for signs of damage or tampering. Suspect shipments are refused at the door.
* The mailing process is highly automated from production through insertion, with on-site postal facilities minimizing the opportunity for interruption of the delivery process.

**Hardware/Software**

* All Internet connections are protected by Cisco firewall.
* We employ extensive use of encryption for documents shared on the FTP site.
* All incoming data is secured, processed and held for thirty days before deletion.
* We adhere to strict operational procedures for system authentication, administration and data protection.
* XXX regularly performs audits of systems and infrastructure for compliance with clients' procedures.

**Client Audits**

Many ofX:XX's clients operate in highly regulated industries such as health care, financial services and telecommunications. Because security mandates vary among these industries,

### HIPM Summary

XXX's operating procedures and processes must address each client's unique needs. XXX regularly performs detailed audits to ensure compliance with governmental requirements and association recommendations in regulating production, storage, communications and other factors.

The vigorous auditing we perform for our clients typically covers the following areas:

* Human Resources Screening and Statistics
* Training Procedures and Documentation
* Insurance, Legal and Liability Coverage
* Operational Workflow Controls
* Materials Management
* Policies, Standards and Procedures
* Management Reporting and Planning
* Access - Physical, Logical and Electronic
* Disaster Recovery Processes and Controls
* Authorization processes
* Environmental Controls
* Data Management procedures
* Contingency Planning