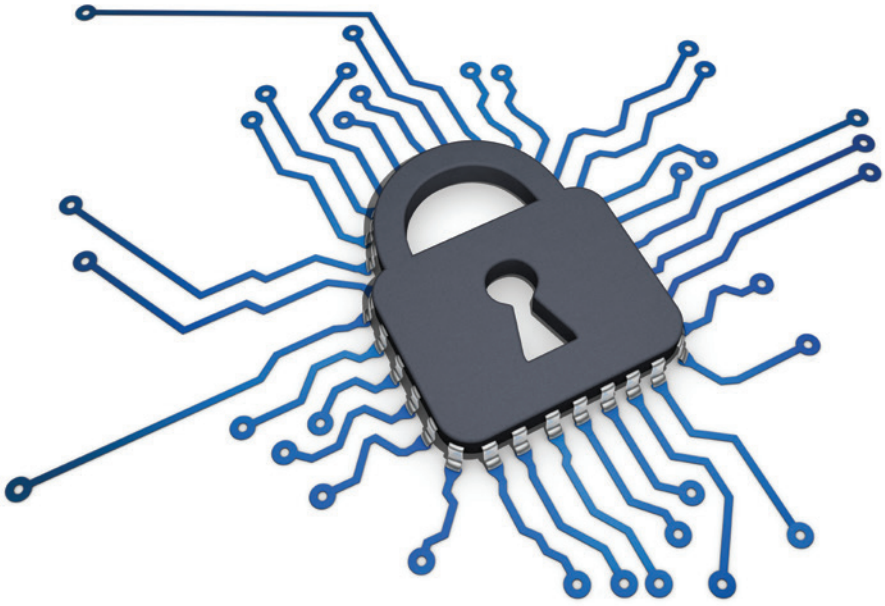
SOPHOS

Security made simple.



Sample 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

Comments to assist in the use of these policies have been added *in red*.

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.

2.0 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

3.0 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 appropriate areas.
4. You are required not to reference the subject or content of sensitive or confidential data publically, 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 all printed in scope 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 in scope 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 in scope are not left unduly exposed, for example visible in the back seat of your car.
12. 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. 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 in scope 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.

2.0 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 behaviour 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)*.

3.0 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 in scope data. A large number of records is defined as <complete as appropriate> *(tailor to your enterprise's stance e.g. 1000 records)*.

   In scope 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)*

   a. Credit card details, bank account numbers and other financial identifiers

   b. E-mail addresses, names, addresses and other combinations of personally identifiable information

   c. Documents that have been explicitly marked with the '<Company X> Confidential' string.

3. DLP will identify specific content, i.e.:
    a. Sales data – particularly forecasts, renewals lists and other customer listings
    b. 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)*.
4. 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.
5. 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)*.
6. 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)*.
7. 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.

4.0 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.

5.0 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.

2.0 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)*.

3.0 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.
11. Configuration changes are to be conducted through the <complete as appropriate> change control process, identifying risks and noteworthy implementation changes to security management.

4.0 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.
4. 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.
5. 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)*.

5.0 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.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

2058-11.14DD.na.simple