





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.

本文档提供了三个示例数据安全策略，涵盖了关键的关注领域。它们不应被视为一份详尽的清单，而是每个组织应根据其用户、数据、监管环境和其他相关因素确定任何其他需要制定政策的领域。

The three policies cover:

1. Data security policy: Employee requirements 员工要求
2. Data security policy: Data Leakage Prevention – Data in Motion 防止数据泄漏-动态数据
3. Data security policy: Workstation Full Disk Encryption 工作站全盘加密

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

用于帮助使用这些政策的注释已添加为红色。

# 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.

这个示例策略概述了员工在处理数据时所期望的行为，并提供了他们应该关注的数据类型的分类。这应该链接到您的AUP(可接受使用政策)、安全培训和信息安全政策，为用户提供所需行为的指导。

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.

<公司X>必须保护受限制的、机密的或敏感的数据免受损失，以避免声誉受损，避免对我们的客户造成不利影响。保护作用域中的数据是一项关键的业务需求，但是访问数据和有效工作的灵活性也是关键的。

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.

预计该技术控制不能有效地处理恶意盗窃场景，也不能可靠地检测到所有数据。它的主要目标是用户意识和避免意外损失场景。该策略概述了数据泄漏预防的要求、策略的重点和基本原理。

* 1. Scope
     1. Any employee, contractor or individual with access to <Company X> systems or data. 任何可以访问<公司X>系统或数据的员工、承包商或个人。
     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)* 要保护的数据的定义(你应该识别数据的类型，并给出例子，以便你的用户在遇到数据时可以识别)

🢝 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. 您需要完成<公司X>的安全意识培训，并同意遵守可接受的使用政策。
     2. If you identify an unknown, un-escorted or otherwise unauthorized individual in <Company X> you need to immediately notify

<complete as appropriate>. 如果您在< X公司>中发现一个未知的、无护送的或未经授权的个人，您需要立即通知 <complete as appropriate>。

* + 1. 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. 参观公司X>时，必须有授权员工陪同。如果你负责护送游客，你必须限制他们在适当的区域。
    2. 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. 您不得公开引用敏感或机密数据的主题或内容，或通过不受< X>公司控制的系统或通信渠道。例如，不允许使用不由<Company X>托管的外部电子邮件系统来分发数据。
    3. 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.

请保持桌面整洁。为确保资讯安全，你必须确保所有印制在范围内的资料不会无人看管地留在你的工作站上

* + 1. 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. 根据密码策略，您需要在所有<Company X>系统上使用安全密码。这些凭据必须是唯一的，并且不能在其他外部系统或服务上使用。
    2. 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*. 被解雇的员工将被要求以任何格式返回所有包含个人信息的记录。这一要求应该成为员工入职过程的一部分，并由员工签署文件以确认他们将这么做。
    3. You must immediately notify <complete as appropriate> in the event that a device containing in scope data is lost (e.g. mobiles, laptops etc). 如果包含范围数据的设备丢失(例如手机、笔记本电脑等)，您必须立即通知<complete酌情>。
    4. 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. 如果您发现您怀疑的系统或流程不符合本政策或信息安全目标，您有责任通知<complete as possible >，以便他们采取适当的行动。
    5. 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. 如果您被分配了远程工作的能力，您必须采取额外的预防措施，以确保数据得到适当的处理。如果你对自己的职责不确定，请向<complete as appropriate>寻求指导。
    6. Please ensure that assets holding data in scope are not left unduly exposed, for example visible in the back seat of your car. 请确保在范围内的资产持有数据没有被过度暴露，例如在您的汽车后座上可见。
    7. 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>.必须在<company X>内移动的数据只能通过企业提供的安全传输机制(例如加密USB密钥、文件共享、电子邮件等)传输。<公司X>将为您提供符合此目的的系统或设备。不能使用其他机制来处理范围内的数据。如果您有一个关于传输机制使用的查询，或者它不符合您的业务目的，您必须在适当的>中使用<complete来提出这个查询。
    8. 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>.

任何在便携式设备上传输的信息(例如USB，笔记本电脑)必须按照行业最佳实践和适用的法律法规进行加密。如果对要求有疑问，请向 <complete as appropriate>寻求指导。

# 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.

本示例策略旨在为那些希望实现或更新DLP控制的组织提供指导。调整此政策，特别是根据可用性的要求，或根据您需要保护的法规或数据。该策略为可能需要监视的数据类提供了一个框架。你应该根据你持有的资产类型，将它们扩展到涵盖你业务中的敏感资产。

## 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.

防止数据泄漏的目的是让用户知道他们正在传输的数据可能是敏感或受限制的。

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.

<公司X>必须保护受限制的、机密的或敏感的数据免受损失，以避免声誉受损，避免对我们的客户造成不利影响。范围内数据的保护是一项关键的业务需求，但是访问数据和有效工作的灵活性也是关键的。

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.

预计该技术控制不能有效地处理恶意盗窃场景，也不能可靠地检测到所有数据。它的主要目标是用户意识和避免意外损失场景。该策略概述了数据泄漏预防的要求、策略的重点和基本原理。

* 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. 任何处理客户数据、敏感数据、个人识别信息或公司数据的<Company X>设备。任何经常用于电子邮件、网络或其他与工作相关的任务，并不是专门为合法的商业或技术原因豁免的设备。
     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. <Company X>信息安全政策将界定处理信息的要求和用户行为要求。这项政策是为了加强资讯安全政策与技术控制。
     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)*. 豁免:如果需要从该策略中豁免业务(太昂贵、太复杂、对其他业务需求产生不利影响)，则必须在安全管理部门的授权下进行风险评估。参见风险评估流程(参考您自己的风险评估流程)。
  2. Policy
     1. <Company X’s> data leakage prevention (DLP) technology will scan for data in motion. < X公司的>数据泄漏预防(DLP)技术将扫描动态数据。
     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)*. DLP技术将识别范围内数据的大量(因此，敏感的高风险和如果处理不当可能产生重大影响)。大量的记录被定义为<完整的适当的>(根据您的企业的立场量身定做，例如1000条记录)。

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)* 范围数据定义为:(您应该调整它，以反映您所管理的数据，或者可能对您的组织造成最大损害的数据。下面是一个适合许多组织的模板)

* + - 1. Credit card details, bank account numbers and other financial identifiers信用卡信息，银行账号和其他财务标识
      2. E-mail addresses, names, addresses and other combinations of personally identifiable information 电子邮件地址，姓名，地址和其他个人身份信息的组合
      3. Documents that have been explicitly marked with the ‘<Company X> Confidential’ string. 显式标记为' <Company X> Confidential '字符串的文档。
    1. DLP will identify specific content, i.e.: LP将确定具体内容，即:
       1. Sales data – particularly forecasts, renewals lists and other customer listings 销售数据——特别是预测、续订名单和其他客户名单
       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)*. 在受控系统外导出个人可识别信息(这是您特别担心丢失的数据，并希望确保DLP策略检测到的数据)。
    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. DLP将被配置为在可疑的敏感数据传输事件中向用户发出警报，并将向用户提供授权或拒绝传输的选择。这允许用户在不中断业务功能的情况下做出明智的决定来保护数据。DLP产品配置的变更将通过 <Company X> IT变更流程处理，并经安全管理部门批准，以确定调整信息安全政策或员工沟通的需求。

* + 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)*. DLP将集中记录事件以供审查。IT团队将对事件进行一级分类，识别可能敏感的数据，以及在哪些情况下其转移是经过授权的，以及存在不恰当使用的问题。这些事件将升级到人力资源部门，通过正常流程进行处理，以保护个人。(你需要为你的组织量身定做。通常情况下，将数据的执行交给业务所有者，而不是由It来进行分类)。
    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)*. 如果存在对数据泄露的积极关注，则使用IT事件管理流程，并根据需要向<complete >(例如人力资源、法律和安全管理)提供具体通知。
    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. 为了保护员工的隐私，访问DLP活动的权限将仅限于指定的一组个人。DLP事件并不构成员工故意或意外丢失数据的证据，但提供了充分的调查基础，以确保数据得到适当的保护。
  1. Technical guidelines

Technical guidelines identify requirements for technical implementation and are typically technology specific. 技术指南确定了技术实现的需求，通常是特定于技术的。

* + 1. The technology of choice is <complete as appropriate> 所选择的技术是完全的适当的
    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. 该产品将被配置为识别浏览器、IM客户端、电子邮件客户端、海量存储设备和可写CD媒体的动态数据。
  1. Reporting requirements
     1. Weekly reports of incidents to <complete as appropriate> 每周的事故报告，如有需要，请填写到
     2. High priority incidents discovered by IT should be immediately flagged with <complete as appropriate> 它发现的高优先级事件应该立即标记为<complete(适当的>)
     3. Monthly report showing % devices compliant with DLP policy

每月报告显示符合DLP政策的设备百分比

# 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.

此示例策略旨在为希望实现或更新其全磁盘加密控制策略的组织提供指导。调整此政策，特别是根据可用性的要求，或根据您需要保护的法规或数据。

## Background to this policy

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

全磁盘加密现在是一项关键的隐私增强技术，这是我的许多监管指导方针所强制要求的。

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. <公司X>必须保护受限制的、机密的或敏感的数据免受损失，以避免声誉受损，避免对我们的客户造成不利影响。一组全局规则(如适当的>中的<complete)也需要对广泛范围的数据进行保护，该策略通过限制对适当的>设备上托管的数据的访问来支持这一点。根据众多合规标准和行业最佳实践的定义，需要全磁盘加密，以防止资产丢失时的暴露。该策略定义了全盘加密的要求

* 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)*. 所有<Company X>工作站-台式机和笔记本电脑(取决于你持有的数据类型和物理安全，一些组织调整这只涵盖笔记本电脑)。
     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)*. 豁免:如果需要从该策略中豁免业务(太昂贵、太复杂、对其他业务需求产生不利影响)，则必须在安全管理部门的授权下进行风险评估。参见风险评估流程(参考您自己的风险评估流程)。
  2. Policy
     1. All devices in scope will have full disk encryption enabled. 范围内的所有设备都将启用全磁盘加密。
     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. <公司X的>可接受使用政策(AUP)和安全意识培训必须要求用户在怀疑自己不符合该政策时，适当通知<complete >。
     3. The AUP and security awareness training must require users to notify <complete as appropriate> of any device which is lost or stolen. AUP和安全意识培训必须要求用户在任何设备丢失或被盗时及时通知>
     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. 加密策略必须通过<complete作为适当的>进行管理和符合性验证。机器需要向中央管理基础设施报告，以使审计记录能够根据需要演示合规性。
     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. 如果无法进行管理，且配置了独立加密(只有经过风险评估批准后)，设备用户必须提供当前加密密钥的副本。
     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)*.

<Complete as appropriate>有权访问任何加密设备，以进行调查、维护或没有一个拥有主文件系统访问权限的员工。<在适当情况下完成，AUP和安全意识培训将通知用户这一要求。(取决于您的AUP，或与员工的协议，您将希望改变这一政策要求的立场)。

* + 1. The encryption technology must be configured in accordance with industry best practice to be hardened against attacks. 加密技术必须按照行业最佳实践进行配置，以防止攻击。
    2. All security related events will be logged and audited by <complete as appropriate> to identify inappropriate access to systems or other malicious use. 所有与安全相关的事件将被记录下来，并由<complete as appropriate>审计，以识别不适当的访问系统或其他恶意使用
    3. 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. 适当的<完成>服务台将允许发行一个带外挑战/响应允许访问系统在发生故障时,失去了凭证或其他业务阻塞需求。只有在使用密码策略中记录的质疑和响应属性可以确定用户身份的情况下，才会提供这种质疑/响应。
    4. *(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)*. (一些企业可能需要实践一种分层的数据安全方法。这可能涉及一组具有特别敏感数据并需要更高安全性的用户。如果这不是你的业务要求，你可以删除它)。

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. 一组敏感数据/VIP用户将被限制数据策略识别。这个组的用户需要一个<complete as appropriate>的成员(如高级管理人员或IT人员)授权来进行关键的更改或挑战响应。未经授权，不允许帮助台访问上述系统。这些系统被识别为可以访问高度敏感的、受限制的使用数据，并有职责分离的要求。在认证和受限制数据策略识别的地方，系统/用户将被要求使用两因素认证

* + 1. Configuration changes are to be conducted through the <complete as appropriate> change control process, identifying risks and noteworthy implementation changes to security management. 配置变更应通过<完全的适当的>变更控制过程进行，识别风险并注意安全管理的实施变更。
  1. Technical guidelines

Technical guidelines identify requirements for technical implementation and are typically technology specific. 技术指南确定了技术实现的需求，通常是特定于技术的。

* + 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. 必须采用强大的行业最佳实践定义的加密标准。AES-256是一个被认可的实现。
    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. BIOS将配置一个安全的密码(由密码策略定义)，并由它存储。引导顺序将被固定到加密的硬盘上。如果用户在维护或紧急情况下需要覆盖，帮助台可以 对用户进行认证，然后提供BIOS密码。目标是避免攻击者冷启动并攻击系统。

* + 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. 将配置与Windows凭据的同步，以便预引导环境与用户的凭据匹配，并且只需要一次登录。
    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)*. 将使用预引导环境进行身份验证。凭据将用于根据 <complete和适当的>密码安全策略对用户进行身份验证。(有些企业有使用两个因素的要求，这应该按要求在这里体现出来)。

* 1. Reporting requirements
     1. A monthly report that identifies the % of encrypted systems versus assets in scope每月报告，确定加密系统与范围内资产的比例
     2. A monthly report that identifies the compliance status of managed, encrypted systems 月度报告，识别受管理的加密系统的合规状态
     3. A monthly report that identifies the number of lost assets and validation that lost devices have been handled appropriately. 月度报告，确认丢失资产的数量，确认丢失设备已得到妥善处理。

United Kingdom and Worldwide Sales Tel: +44 (0)8447 671131

Email: [sales@sophos.com](mailto:sales@sophos.com)

North American Sales Toll Free: 1-866-866-2802

Email: [nasales@sophos.com](mailto:nasales@sophos.com)

Australia and New Zealand Sales Tel: +61 2 9409 9100

Email: [sales@sophos.com.au](mailto:sales@sophos.com.au)

Asia Sales

Tel: +65 62244168

Email: [salesasia@sophos.com](mailto:salesasia@sophos.com)

Oxford, UK | Boston, USA

© Copyright 2014. Sophos Ltd. All rights reserved.

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2058-11.14DD.na.simple