netwrix

Data Security and Protection Policy Template

Having a documented data security policy is a best practice for every organization, especially those that are subject to today's increasingly stringent data privacy laws, such as the EU's General Data Protection Regulation (GDPR).

Often a part of a broader information security policy or privacy policy, a data security policy addresses such topics as data encryption, password protection and access control. However, the goal is not limited to describing security measures; a data security policy also works to show the company's commitment to meeting compliance requirements. In particular, the policy needs to outline organizational measures for protecting sensitive and critical data, such as personal information. The policy also needs to explain the roles and functions in the data protection process, such as the responsibilities of the data protection officer (DPO) for GDPR compliance.

Here is a data policy template for access control that you can adapt to meet your organization's unique legal requirements.

Data Security Policy: Access Control

Organizations create an access control data protection policy to make sure users can access only the assets they need to do their jobs — in other words, to enforce a least-privilege model. Typically, this policy is implemented with a combination of technical controls and training to educate users about their responsibilities for protection of data.

The data security policy template below provides a framework for assigning data access controls. Once you have developed your policy based on the template, be sure to expand it to cover new assets and operations as they are added to your business.

Data Security Policy Template

Here are the key sections to include in your data security policy and examples of their content.

1. Purpose

In this section, you explain the reasons for having this policy. Here is an example:

> *The company must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.*
>
> *It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data breach prevention.*

2. Scope

2.1 In Scope

In this section, you list all areas that fall under the policy, such as data sources and data types. For example:

> *This data security policy applies all customer data, personal data and other company data defined as sensitive by the company's data classification policy. Therefore, it applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with company IT services is also subject to this policy.*

2.2 Out of Scope

Here you define what does not fall under your data security policy. For instance:

> *Information that is classified as Public is not subject to this policy. Other data can be excluded from the policy by company management based on specific business needs, such as that protecting the data is too costly or too complex.*

3. Policy

This is the body of the policy where you state all policy requirements.

3.1 Principles

> *The company shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible.*

3.2 General

> ***a.*** *Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.*
>
> ***b.*** *The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.*

c. *Each user shall read this data security policy and the login and logoff guidelines, and sign a statement that they understand the conditions of access.*

d. *Records of user access may be used to provide evidence for security incident investigations.*

e*. Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.*

3.3 Access Control Authorization

Access to company IT resources and services will be given through the provision of a unique user account and complex password. Accounts are provided by the IT department based on records in the HR department.

Passwords are managed by the IT Service Desk. Requirements for password length, complexity and expiration are stated in the company password policy.

Role-based access control (RBAC) will be used to secure access to all file-based resources in Active Directory domains.

3.4 Network Access

a. *All employees and contractors shall be given network access in accordance with business access control procedures and the least-privilege principle.*

b. *All staff and contractors who have remote access to company networks shall be authenticated using the VPN authentication mechanism only.*

c. *Segregation of networks shall be implemented as recommended by the company's network security research. Network administrators shall group together information services, users and information systems as appropriate to achieve the required segregation.*

d. *Network routing controls shall be implemented to support the access control policy.*

3.5 User Responsibilities

a. *All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.*

b. *All users must keep their workplace clear of any sensitive or confidential information when they leave.*

c. *All users must keep their passwords confidential and not share them.*

3.6 Application and Information Access

a. *All company staff and contractors shall be granted access to the data and applications required for their job roles.*

b. *All company staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from higher management.*

c. *Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.*

3.7 Access to Confidential or Restricted information

a. *Access to data classified as 'Confidential' or 'Restricted' shall be limited to authorized persons whose job responsibilities require it, as determined by the Data Security Policy or higher management.*

b. *The responsibility to implement access restrictions lies with the IT Security department.*

4. Technical Guidelines

The technical guidelines specify all requirements for technical controls used to grant access to data. Here is an example:

> *Access control methods to be used shall include:*
>
> - *Auditing of attempts to log on to any device on the company network*
> - *Windows NTFS permissions to files and folders*
> - *Role-based access model*
> - *Server access rights*
> - *Firewall permissions*
> - *Network zone and VLAN ACLs*
> - *Web authentication rights*
> - *Database access rights and ACLs*
> - *Encryption at rest and in flight*
> - *Network segregation*
>
> *Access control applies to all networks, servers, workstations, laptops, mobile devices, web applications and websites, cloud storages, and services.*

5. Reporting Requirements

This section describes the requirements for reporting incidents that happen.

> ***a.*** *Daily incident reports shall be produced and handled by the IT Security department or the incident response team.*
>
> ***b.*** *Weekly reports detailing all incidents shall be produced by the IT Security department and sent to the IT manager or director.*

c. High-priority incidents discovered by the IT Security department shall be immediately escalated; the IT manager should be contacted as soon as possible.

d. The IT Security department shall also product a monthly report showing the number of IT security incidents and the percentage that were resolved.

6. Ownership and Responsibilities

Here you should state who owns what and who is responsible for which actions and controls.

- **Data owners** are employees who have primary responsibility for maintaining information that they own, such as an executive, department manager or team leader.
- **Information Security Administrator** is an employee designated by the IT management who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources.
- **Users** include everyone who has access to information resources, such as employees, trustees, contractors, consultants, temporary employees and volunteers.
- **The Incident Response Team** shall shall be chaired by an executive and include employees from departments such as IT Infrastructure, IT Application Security, Legal, Financial Services and Human Resources.

7. Enforcement

This paragraph should state the penalties for access control violations.

Any user found in violation of this policy is subject to disciplinary action, up to and including termination of employment. Any third-party partner or contractor found in violation may have their network connection terminated.

8. Definitions

This paragraph defines any technical terms used in this policy.

- ***Access control list (ACL)*** *— A list of access control entries (ACEs) or rules. Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied or audited for that trustee.*
- ***Database*** *— An organized collection of data, generally stored and accessed electronically from a computer system.*
- ***Encryption*** *— The process of encoding a message or other information so that only authorized parties can access it.*
- **Firewall** *— A technology used for isolating one network from another. Firewalls can be standalone systems or can be included in other devices, such as routers or servers.*
- ***Network segregation*** *— The separation of the network into logical or functional units called zones. For example, you might have a zone for sales, a zone for technical support and another zone for research, because each group has different technical needs.*
- ***Role-based access control (RBAC)*** *— A policy-neutral access-control mechanism defined around roles and privileges.*
- ***Server*** *— A computer program or a device that provides functionality for other programs or devices, called clients.*
- ***Virtual private network (VPN)*** *— A secure private network connection across a public network.*
- ***VLAN (virtual LAN)*** *— A logical grouping of devices in the same broadcast domain.*

9. Related Documents

This section lists all documents related to the policy and provides links to them. This list might include:

- Data Classification Policy
- Password Policy
- *Data Loss Protection Policy*
- *Encryption Policy*
- *Incident Response Policy*
- *Workstation Security Policy*
- *Data processing agreement*

10. Revision History

Every policy revision should be recorded in this section.

Version	Date of Revision	Author	Description of Changes
1.0	June 12, 2019	J.Smith, IT Manager	Initial Version

Conclusion

Using this template, you can create a data security access policy for your organization. Remember that security policies must be both strong and feasible, and they should also be accessible, concise and easy to understand. Strive to achieve a good balance between data protection and user productivity and convenience.

About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.
www.netwrix.com.

Corporate Headquarters:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

netwrix.com/social

Powerful Data Security Made Easy

- Focus your data protection efforts on your truly valuable content.
- Minimize the risk of a data breach.
- Promptly detect data security threats.
- Make more informed incident response decisions.
- Facilitate the recovery of key data and learn from past incidents.
- Achieve and prove regulatory compliance.

Download Free 20-Day Trial