



UNIT 3

Data Security Policy & Personal Data

Learning Objectives:

By the end of this unit the learner will be able to:

- Understand and write a data security policy
- Understand and write a personal data protection policy

Unit 3

Data Security Policy & Personal Data Protection Policy

The Data Security Policy outlines the overall security management framework for an organization. A good data security policy will help protect the personal information you hold, and will help prevent a data breach. Proper data security relies on good practices on both an organizational level, and on a day-to-day operational level. The policy should cover both levels.

The data security policy should include details of the following:

- Who has responsibility for data security in your organization: is it your IT manager, or Operational Officer, etc.
- Guidelines on the staff usage of computers or information storage tools, including use of work computers, control and monitoring, usage restrictions, and consequences for non-compliance.
- Where your organization backs up its online data, and how often this is done.
- The security measures that are in place in the organization, including any encryption, firewalls, anti-virus, secured servers, etc.

TEST YOUR KNOWLEDGE

Develop a comprehensive Data Security Policy with as much detail as possible. Be sure to consider both high-level and day-to-day processes in the policy.

Data Security Policy

CONTENTS OF THE PERSONAL DATA PROTECTION POLICY

General staff guidelines – rules that should be followed by all employees in the course of their work:

- How data should be handled (no unauthorized access/disclosure)
- How data should be properly disposed
- Training requirements

Proper data storage expectations:

- Where physical documents should be stored
- Where electronic documents should be stored (for example, on a work computer or external hard drive)
- How often, and in what way, data should be backed up
- Other data security features that are in place

RESPONSIBILITIES FOR PRIVACY

Everyone in the company has responsibilities for privacy. Certain key roles (like CEO, IT Manager, Privacy Officer, etc.) will have more specific responsibilities, but all employees have a responsibility to ensure and uphold the privacy of the personal data they work with, and should report concerns to the appropriate members of the organization. The specification of responsibility should be reflected in the personal data protection policy.

It is important that each person sees themselves in this section. This is part of getting buy-in for the Privacy Plan.

