TECHDUDS3

# Apply enhanced security procedures to protect data

## Overview

This standard is about applying enhanced security procedures to protect a digital device and the data it may contain or access.

It involves configuring digital devices to reduce cyber security risk and improve resilience at start-up and during operation. It includes implementing multi factor authentication to access digital devices and using encryption to secure data, files and drives on digital devices.

It also includes reducing risk by adopting the principle of least privilege user status to enhance the security of digital devices during everyday use.

This standard is for those who need to apply enhanced security procedures to protect data on or accessed through digital devices to meet their own needs or as part of their duties.

## Performance criteria

*You must be able to:*

1. Review and configure digital device settings to disable or modify those features not required to reduce the cyber security vulnerabilities in line with organisational procedures
2. Encrypt the storage drive that stores and hosts the digital device operating system to maintain cyber resilience
3. Implement and configure secure boot at start-up in line with organisational procedures
4. Add multi factor authentication access measures to access digital devices to provided enhanced security of systems and data
5. Operate the principle of least privilege to restrict system access to only those authorised in line with organisational policies
6. Use encryption to send confidential data safely by email and other digital communication methods
7. Secure web browsers by updating default settings to an enhanced state of protection in line with organisational policies

## Knowledge and understanding

*You need to know and understand:*

1. The cyber security challenges faced by organisations
2. The different types of security personnel and their roles in organisations
3. The security measures that can be taken to reduce vulnerabilities in digital devices
4. How to configure digital devices to reduce cyber security risk and improve resilience at start-up and during operation
5. How to check network connection security status
6. The role of multifactor authentication in improving security resilience
7. How to add biometric access privileges to enabled digital devices
8. The role of data, file and drive encryption to protect devices and data
9. How to implement encryption for emails, local files and folders
10. How to encrypt the main operating system software drive
11. The ways in which cyber security attacks can be detected
12. The ways in which organisations respond to cyber security attacks
13. The behaviours that minimise the risk of a successful cyber security attack

TECHDUDS3

# Apply enhanced security procedures to protect data

| | |
|---|---|
| **Developed by** | e-skills |
| **Version Number** | 1 |
| **Date Approved** | 30 Mar 2022 |
| **Indicative Review Date** | 30 Mar 2025 |
| **Validity** | Current |
| **Status** | Original |
| **Originating Organisation** | ODAG Consultants Ltd. |
| **Original URN** | TECHDUDS3 |
| **Relevant Occupations** | ICT for Users |
| **Suite** | IT Users |
| **Keywords** | information security, data security, cyber security |