<Organisation Name>

Cyber Security Essential Checklist [Template]

<Document Version & Date>



Copyright © 2021 <Organisation Name>

This document is based on a template document provided by Real World Technology Solutions.

Real World Technology Solutions grants permission for the template document to be modified in any manner <Organisation Name> wishes, provided this acknowledgement remains in place.

Document Owner: <Person’s Name>

Contact: <Person’s email and/or mobile telephone>

**How to use this template document**

This is a template document. It contains suggested or recommended content.

It is content that can be freely added to, moved, modified, or deleted.

Do not feel obliged to use the content as is if it does not suit your organisation.

You should read and adopt, adapt or remove, as appropriate!

What to do:

1. This document uses generic text for certain items that need to be updated by the organisation. These template text items are formatted in red with angle brackets (e.g. <Organisation Name> representing the organisation’s name), and should be updated to replace the template text with appropriate text specific to the organisation.
2. Using global replace, change <Organisation Name> to the organisation’s name
3. On the front page and in the page headers, change the Document Title to remove
“ [Template]” from the title, if present
4. On the front page and in the page footers, update the <Document Version & Date> to a new version of this document after your editing, and as you edit it in the future; e.g. V1.5 2025-05-05
5. Edit the document header to include the organisation’s logo, or remove the <Organisation Logo> template text
6. Find any other template text items and update them with the appropriate text for the organisation
7. Sometimes <there will be additional usage guidance formatted in blue like this comment> – it provides guidance and a reminder that the content can be freely edited to make it appropriate for your organisation
8. Review all the content and change anything as required to meet the organisation’s requirements and circumstances – sections and text can be modified, moved, deleted or added
9. Update the Contents table after updates by clicking on “Contents” and “Update Table…”; you may occasionally be prompted and can “Update entire table”
10. When ready, delete these instructions on this page and update the Contents again
11. Save the updated document

Contents

[1 Introduction 5](#_Toc88123108)

[2 Cyber Security Training 5](#_Toc88123109)

[2.1 Regular Training 5](#_Toc88123110)

[3 Software Up-to-date and Secured 5](#_Toc88123111)

[3.1 Operating Systems at Latest Release 5](#_Toc88123112)

[3.2 Operating Systems Updated Regularly 5](#_Toc88123113)

[3.3 Applications at Latest Release 5](#_Toc88123114)

[3.4 Applications Configured Securely 6](#_Toc88123115)

[3.5 Malware and Antivirus Software Active with Latest Definitions 6](#_Toc88123116)

[3.6 BIOS, Firmware and Drivers at Latest Releases 6](#_Toc88123117)

[4 Data Management 6](#_Toc88123118)

[4.1 Data 6](#_Toc88123119)

[4.2 Backups 6](#_Toc88123120)

[4.3 Data Security 7](#_Toc88123121)

[5 Access and Accounts 7](#_Toc88123122)

[5.1 Operating System Accounts 7](#_Toc88123123)

[5.2 Application Accounts 7](#_Toc88123124)

[5.3 Multi-Factor Authentication 7](#_Toc88123125)

[5.4 Remote Access 7](#_Toc88123126)

[5.5 Network Access 8](#_Toc88123127)

[6 Cyber Security Incident Preparedness 8](#_Toc88123128)

[6.1 Plans 8](#_Toc88123129)

[6.2 Monitoring 8](#_Toc88123130)

# Introduction

This is a Checklist of Essential Actions related to Cyber Security. Use it to prepare and maintain an IT environment to minimise the risk, impact and effects of cyber security incidents.

# Cyber Security Training

## Regular Training

Keep people up-to-date on cyber security matters:

* Effective training is conducted regularly, at least annually, and as the cyber security landscape changes
* Training is updated regularly to keep up-to-date with the evolving cyber security landscape
* Additional training is provided for people who have Administrator privileges, or who use remote access
* Specific training on phishing is regularly conducted, at least every three months
* People who join the organisation are required to go through the training

# Software Up-to-date and Secured

## Operating Systems at Latest Release

Operating systems on desktops, laptops and portable/mobile devices are at the latest major releases:

* Microsoft Windows 10 and Windows 11
* MacOS 14 or 15
* Android
* iOS 14 or 15 on iPhones and iPads

## Operating Systems Updated Regularly

Operating systems on desktops and laptops are kept up-to-date with regularly released updates, preferably automatically:

* Microsoft Windows 10 and Windows 11 run Windows Update regularly
* MacOS 14 or 15 is updated regularly

## Applications at Latest Release

Applications are kept at the latest releases:

* Microsoft Office
* Web browsers (Chrome, Edge, Firefox, Safari, etc)
* Malware and Antivirus software
* Email servers and clients
* PDF viewers and editors
* Other software (purchased, freeware, custom, etc)

## Applications Configured Securely

Applications are configured securely, following manufacturers’ or professional advice:

* Microsoft Office, including macros
* Web browsers (Chrome, Edge, Firefox, Safari, etc)
* Malware and Antivirus software
* Email servers and clients
* PDF viewers and editors
* Other software (purchased, freeware, custom, etc)

## Malware and Antivirus Software Active with Latest Definitions

Malware and Antivirus software is:

* Installed and starting automatically at system startup
* Automatically updating to the latest malware and antivirus definitions

## BIOS, Firmware and Drivers at Latest Releases

BIOS, firmware and driver versions on desktops and laptops are checked and updated as needed:

* BIOS
* Device drivers
* Device firmware

# Data Management

## Data

Data on the systems is understood:

* The scope and types of all data on systems is known
* Data has been classified to identify sensitive and high-value data
* Data needing to be restorable if lost or corrupted has been identified

## Backups

Backups of data are being taken:

* Backup software is installed and usable
* Backup devices and sufficient disk space (or other devices, e.g. tapes) are available
* Data to be backed up has been identified
* The schedule of regular backups has been decided
* Backups are automated, or the person to do backups assigned
* Regular backups are performed
* Backups are regularly tested to ensure the data can be restored and it is correct when restored

## Data Security

Data on the systems has appropriate safeguards:

* Sensitive and high-value data is protected against unauthorised access
* Sensitive and high-value data is encrypted when transferred or transported anywhere
* Sensitive and high-value data is securely destroyed when no longer needed

# Access and Accounts

## Operating System Accounts

All operating system accounts are controlled:

* All accounts must be approved
* Users have individual accounts – shared accounts are rarely, if ever, used
* Most accounts do not have Administrator privileges
* Only system administrators have accounts with Administrator privileges
* Accounts for people no longer with the organisation are disabled/deleted

## Application Accounts

All application accounts, if any, are controlled:

* All accounts must be approved
* Users have individual accounts – shared accounts are rarely, if ever, used
* Most accounts do not have Administrator privileges
* Only system administrators have accounts with Administrator privileges
* Accounts for people no longer with the organisation are disabled/deleted

## Multi-Factor Authentication

Multi-factor authentication is used where appropriate:

* Accounts and access requiring multi-factor authentication are identified
* Multi-factor authentication technology is available and understood
* Multi-factor authentication training is performed

## Remote Access

Remote access is used where appropriate:

* Accounts and access requiring remote access are identified
* Remote access technology is available and understood
* Remote access training is performed
* Remote access logs are reviewed regularly (at least every month)

## Network Access

Network access is secured:

* Access to manage network devices is protected by username and strong password
* WiFi access is restricted by needing a strong password to connect to the network
* Default passwords have been changed to strong passwords
* A Guest network with appropriate restrictions is available, if appropriate

# Cyber Security Incident Preparedness

## Plans

Plans exist or are being created for:

* Responding to a Cyber Security Incident
* Recovering from a Cyber Security Incident and restoring all normal activities
* Communicating during a Cyber Security Incident

## Monitoring

There is monitoring to detect Cyber Security Incidents:

* Automated technology tools, where reasonable
* Human monitoring, where reasonable and effective