<Organisation Name>

Cyber Security Policy [Template]

V0.5 2021-11-10



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 Overview 6](#_Toc87421158)

[1.1 Purpose 6](#_Toc87421159)

[1.2 Definitions 6](#_Toc87421160)

[1.3 Scope – People 7](#_Toc87421161)

[1.4 Scope – Infrastructure 7](#_Toc87421162)

[2 Personnel Responsibilities 8](#_Toc87421163)

[2.1 Personnel Management 8](#_Toc87421164)

[2.2 Cyber Security Training 8](#_Toc87421165)

[2.3 Cyber Security Awareness 8](#_Toc87421166)

[2.4 Cyber Security Events 8](#_Toc87421167)

[2.5 Cyber Security Manager 8](#_Toc87421168)

[2.6 Continual Improvement 8](#_Toc87421169)

[2.7 Confidentiality 8](#_Toc87421170)

[3 Approved Infrastructure 9](#_Toc87421171)

[3.1 Known and Approved 9](#_Toc87421172)

[3.2 Secured 9](#_Toc87421173)

[3.3 Protected 9](#_Toc87421174)

[3.4 Usage 9](#_Toc87421175)

[4 Access 10](#_Toc87421176)

[4.1 Systems and Applications 10](#_Toc87421177)

[4.2 Passwords 10](#_Toc87421178)

[4.3 Multi-Factor Authentication 10](#_Toc87421179)

[4.4 Networks 10](#_Toc87421180)

[4.5 Remote Access 10](#_Toc87421181)

[4.6 Physical Facilities and Infrastructure 10](#_Toc87421182)

[5 Infrastructure Management 11](#_Toc87421183)

[5.1 Physical Facilities and Infrastructure 11](#_Toc87421184)

[5.2 Data Protection 11](#_Toc87421185)

[5.3 Software Updates 11](#_Toc87421186)

[5.4 Software Upgrades 12](#_Toc87421187)

[5.5 Malware Protection 12](#_Toc87421188)

[6 Cyber Security Incident Management 13](#_Toc87421189)

[6.1 Management Process 13](#_Toc87421190)

[6.2 Cyber Security Incident Priorities 13](#_Toc87421191)

[6.3 Post-Incident Review and Report 13](#_Toc87421192)

[7 Documentation 14](#_Toc87421193)

[7.1 Various Related Documents 14](#_Toc87421194)

[7.2 This Cyber Security Policy Document 15](#_Toc87421195)

# Overview

Cyber Security is a core responsibility of <Organisation Name>. This document provides the cyber security policies adopted by <Organisation Name>. It covers people, process and technology.

# Purpose

This Cyber Security Policy has the following purposes:

* Protect the operational integrity and availability of <Organisation Name>’s normal operations facilitated by its personnel and IT resources
* Protect the confidentiality, integrity and availability of data and information managed and retained by <Organisation Name>
* Protect against external intrusion, denial of service, ransomware, and all other malicious breaches of <Organisation Name>’s IT environment, whether internal or external in origin
* Ensure all personnel are aware of potential cyber risks and are trained to detect, respond and recover from cyber events
* Prevent unauthorised and unapproved IT activity of any type within the <Organisation Name> IT environment
* Govern IT practices to ensure cyber security is a normal and expected part of the way <Organisation Name> operates internally, and with its clients and external suppliers and partners
* Manage and recover from any adverse cyber incident in the most effective and efficient manner to restore normal operations as quickly as possible
* Continually review and improve cyber security as <Organisation Name>’s IT environment and the real-world cyber security environment evolve

# Definitions

This Cyber Security Policy contains a variety of terms, some of which are defined here:

* IT System Hardware – IT hardware including computer equipment, servers, desktops, laptops, devices and accessories, whether “fixed” or portable
* IT Network Hardware – network hardware including routers, switches, modems and WiFi devices
* Mobile Devices – mobile telephones, tablets, and other portable communication devices
* IT System Software – computer software including operating systems, device drivers, firmware and BIOS
* IT Network Software – network software including network device operating systems
* Mobile Software – software installed on or used on Mobile Devices
* IT Application Software – application software including Microsoft Office and other Microsoft products, databases, web browsers, email servers and clients, purchased applications, freeware, open-source software, in-house developed software, collaboration tools, cloud-based software, etc
* Infrastructure – all items defined above; synonyms include “technology” and “equipment”
* Physical Facilities – physical facilities and locations in which IT infrastructure, as listed above, is stored, operated or used

# Scope – People

This Cyber Security Policy applies to all personnel, including those:

* Employed by <Organisation Name>
* Contracted by <Organisation Name>
* Volunteering for <Organisation Name>
* From third-parties engaged by <Organisation Name> in any manner

These various people are included in any reference to **personnel** or people in this policy document.

# Scope – Infrastructure

This Cyber Security Policy applies to all IT infrastructure owned or operated by <Organisation Name>, as well as IT infrastructure owned or operated by persons or organisations that interact with the <Organisation Name> IT environment, either within that environment directly or remotely. This includes, but is not limited to:

* IT System Hardware
* IT Network Hardware
* Mobile Devices
* IT System Software
* IT Network Software
* Mobile Software
* IT Application Software
* Physical Facilities

These various infrastructure items are included in any reference to infrastructure, technology or equipment in this policy document.

# Personnel Responsibilities

All personnel must be cyber security informed and aware. To facilitate and foster this, <Organisation Name> provides Cyber Security Training, as well as formal processes and procedures, and various other documentation that have cyber security “baked in”. All personnel have a responsibility to be cyber security aware in the activities they perform for <Organisation Name> and to follow documented requirements.

# Personnel Management

To engage new personnel internally, <Organisation Name> will:

* Prior to engagement, conduct background checks on the personnel at a level appropriate for the type of engagement; personnel who do not meet all relevant checks will not be engaged
* Once engaged, deliver Cyber Security Training to the personnel during onboarding

# Cyber Security Training

All personnel must undertake the Cyber Security Training provided by <Organisation Name> as required from time-to-time.

# Cyber Security Awareness

All personnel must perform any activities for <Organisation Name> with a cyber security mindset. This means being aware of the way in which any activities performed can affect or be affected by cyber security related matters. Personnel should endeavour to continue to learn about cyber security as a way of thinking about the activities they perform.

# Cyber Security Events

All personnel have a responsibility to report possible cyber security events as soon as is practical after detecting such events. The reports should be directed to the Cyber Security Manager or other appropriate personnel.

# Cyber Security Manager

<Organisation Name> has a Cyber Security Manager. That person is the primary point of responsibility for cyber security within the organisation. The Cyber Security Manager has the authority to make and implement cyber security related decisions. All personnel must follow any directions given by the Cyber Security Manager and other authorised personnel.

# Continual Improvement

As part of establishing and maintaining an effective and efficient cyber security environment, <Organisation Name> encourages personnel to raise concerns or make suggestions that could improve cyber security within <Organisation Name>. These matters should be raised with the Cyber Security Manager or other appropriate personnel.

# Confidentiality

All personnel must maintain appropriate confidentiality of <Organisation Name> information and activities to minimise the risk of inadvertently making <Organisation Name> vulnerable to a cyber security event.

# Approved Infrastructure

All infrastructure stored, operated or used by any personnel where that infrastructure interacts with the <Organisation Name> IT environment must be approved for use by <Organisation Approval Authority> and used in accordance with this Cyber Security Policy. For this purpose, various policies, processes, procedures, checklists and other documents specify matters related to cyber security and must be used as defined within those relevant documents.

# Known and Approved

All infrastructure must be known and approved by <Organisation Name>. This includes all existing infrastructure; and all new infrastructure that interacts with the <Organisation Name> IT environment, including for guest or short-term access, must be approved before connecting to or integrating with the <Organisation Name> IT environment.

This includes, but is not limited to, all infrastructure as listed in Section 1.4, Scope – Infrastructure, above.

# Secured

All infrastructure must be securely configured as defined by <Organisation Name>. This includes, but is not limited to:

* Operating systems, including server, desktop and laptop
* Network devices, including routers, switches, modems and WiFi devices
* Mobile devices
* Collaboration Tools, including Microsoft 365, Google Workspace, etc
* Microsoft Office, including approval of macros within documents
* Email Servers and Clients
* Web Browsers
* Application software
* Malware Prevention software

# Protected

All infrastructure must be protected against cyber incidents. This includes, but is not limited to:

* Installing approved malware and antivirus software
* Configuring the malware and antivirus software to run automatically at device startup
* Enabling comprehensive real-time malware and antivirus scanning
* Ensuring malware and antivirus software definitions are updated automatically at least daily

Where WiFi access is available, there must be a dedicated Guest network, separate from the main <Organisation Name> network, that is used by all personnel who are external to <Organisation Name>, except where functional or operational requirements necessitate otherwise (e.g. approved third-party maintenance). This Guest network must be configured with minimal access rights.

# Usage

All infrastructure must be stored, operated and used only as approved by <Organisation Name>. Infrastructure must not be used for minor, “other than incidental” personal work, and social media must not be accessed except for organisational purposes.

# Access

Various practices related to accessing the resources in an IT environment so as to maintain good cyber security are identified below. There are approved policies, processes, procedures and other documents associated with these.

# Systems and Applications

IT systems and applications will have controlled access aligned with the purpose of the item. The controls must include some form of authentication of the user (e.g. login). Where appropriate, multi-factor authentication may be required.

# Passwords

IT systems and some applications will have controlled access using a login with a username and password. Passwords must adhere to the following standard:

* Use a combination of uppercase and lowercase letters, digits and special characters
* Include at least one each of uppercase and lowercase letters, digits and special characters
* Be at least eight characters in length, preferably longer
* Not be easily guessed by association with the person creating it
* Changed at least annually, or more frequently if the nature of the access is more sensitive
* Passwords should be different for separate systems and applications, not the same
* Passwords should not be written down in “clear text” or in any way that allows them to be guessed
* Passwords must not be shared with others, except where operationally required

# Multi-Factor Authentication

Multi-Factor authentication is required where data or resources that can be accessed are of a sensitive or high value nature. When required, it will be implemented using only methods and technologies approved by <Organisation Name>.

# Networks

IT networks will have controlled access aligned with the purposes of <Organisation Name>. The controls must include some form of authentication of the user (e.g. login). Where appropriate, multi-factor authentication may be required.

# Remote Access

Remote access to infrastructure will be controlled – only approved personnel using approved remote access methods and technology will be permitted.

Remote access to critical systems shall use a one-time use access code.

# Physical Facilities and Infrastructure

Personnel have a responsibility to safeguard the Physical Facilities and Infrastructure of <Organisation Name>. They must abide by all physical access requirements for <Organisation Name> facilities and infrastructure.

# Infrastructure Management

Various practices related to establishing and maintaining an IT environment with good cyber security are identified below. There are approved policies, processes, procedures and other documents associated with these.

# Physical Facilities and Infrastructure

Physical facilities will be protected as follows:

* Physical barriers must restrict access to critical infrastructure (e.g. dedicated, secure computer room, locked doors, etc)
* Removable disks must be physically secured to prevent tampering or unauthorised removal
* Network devices, except WiFi access points, must be located in a secure, locked cabinet or room
* Swipe card access is implemented and managed in accordance with physical access requirements

# Data Protection

All users of <Organisation Name> systems and IT services will ensure data is protected, accessed and used in accordance with defined data protection requirements, including, but not limited to:

* Data security classifications must be defined
* All data must be classified in accordance with defined data security classifications
* Data must be protected in accordance with its assigned data security classification
* Allowed access to data must align with its data security classification
* Methods used to access data must align with its data security classification
* Data must be destroyed, when appropriate, using methods aligned with its data security classification, including, where necessary, secure data destruction procedures
* Methods used to transport data must align with its data security classification; in particular, sensitive and high-value data must be securely encrypted when transported

# Software Updates

Updates, sometimes called patches, are released by manufacturers and producers of software from time-to-time, usually quite regularly. All infrastructure, most notably IT systems and applications, as well as network devices, must be updated with appropriate updates and patches provided by the manufacturers and suppliers of the infrastructure as soon as practical after release. Where possible and operationally practical, updates should be applied automatically.

# Software Upgrades

From time-to-time, major new releases of software are made available by software manufacturers and producers. Most notable are major releases of operating systems (e.g. Microsoft Windows 8.1 to Windows 10). The following apply:

* Upgrades must be investigated to understand the impact of the upgrade on the existing infrastructure and operations of the organisation
* The resources required to upgrade existing infrastructure must be estimated, including labour, time, necessary infrastructure changes, and any consequential financial outlay
* Where possible and not operationally or financially prohibitive, upgrades must be planned, scheduled and implemented within 12 months of official public release, unless otherwise directed by <Organisation Group Name>.

# Malware Protection

All IT systems, including those owned and operated by <Organisation Name> and those not owned by <Organisation Name> but used for <Organisation Name> purposes, will have active, up-to-date malware protection.

# Cyber Security Incident Management

Various practices related to the management of a cyber security incident are identified below. There are approved policies, processes, procedures and other documents associated with these.

# Management Process

Cyber Security Incidents will be managed as follows:

* Management of cyber security incidents is the responsibility of the Cyber Security Manager or delegate and will follow the Cyber Security Incident Management process, and the Cyber Security Incident Response and Recovery Plans
* The <Organisation Group Name> shall be notified of Cyber Security Incidents lasting longer than four hours or that impact critical systems or data

# Cyber Security Incident Priorities

Cyber Security Incidents and incidents suspected of being Cyber Security Incidents will have the following priorities:

* Critical IT services will be recovered and restored first, along with any required dependent services, before non-critical services
* Restoration of IT services will otherwise follow the priorities defined in the <Organisation Name> Business Continuity Plan

# Post-Incident Review and Report

Every Cyber Security Incident will be reviewed after the incident has been effectively managed and IT services restored. For every incident, this includes:

* A formal post-incident review to determine root cause and other lessons that can be learned from the incident will be conducted as soon as operationally reasonable after the incident, and no more than three days after restoration of IT services
* Presentation of a formal, written report to <Organisation Group Name> within seven days of restoration of IT services
* For events that affect critical systems or data, if the final formal report is not complete, an interim formal report shall be given to <Organisation Group Name> within 48 hours of the restoration of services

# Documentation

<Organisation Name> has many documents that are relevant for the implementation of this Cyber Security Policy. They include various other policies, processes, procedures, technical information documents, and registers for activities, materiel and other information such as risks and threats. These documents must be used as defined within each document to implement and manage cyber security.

# Various Related Documents

These documents include, but are not limited to:

* <This is an example list of documents – add, delete, modify as needed>
* Allowed Applications Register
* Computer and Application Account Approval Process
* Configuring Antivirus and Malware Prevention Software
* Cyber Security Declaration (All Roles)
* Cyber Security Declaration (Board)
* Cyber Security Human Resources Policy
* Cyber Security Manager Role Description
* Cyber Security Phishing Awareness Campaign Material
* Cyber Security Policy [this document]
* Cyber Security Responsibilities (All Roles)
* Cyber Security Responsibilities (Onboarding)
* Cyber Security Responsibilities Register
* Cyber Security Training Material
* Data Classification Register
* Data Classification Scheme
* Data Protection Procedures
* IT Asset Register
* Malware Protection Checklist
* Malware Protection Register
* Mobile Software Checklist
* Mobile Software Register
* Organisational Data Management Policy
* Physical Access Requirements
* Protecting Data and Infrastructure When Travelling
* Remote Access Agreement
* Securing Application Accounts
* Securing Applications (Miscellaneous)
* Securing Collaboration Tools
* Securing Computer Accounts
* Securing Email Servers and Clients
* Securing Microsoft Office
* Securing Web Browsers (Chrome)
* Securing Web Browsers (Edge)
* Securing Web Browsers (Firefox)
* Securing Web Browsers (Safari)
* Securing WiFi
* Other documents as detailed throughout this policy and other cyber security documents

# This Cyber Security Policy Document

This Cyber Security Policy document will be reviewed at least annually, revised as appropriate, and formally approved by the <Organisation Group Name>.