<Organisation Name>

Cyber Security Human Resources Policy [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 Cyber Security Human Resources Policy 5](#_Toc88122918)

[1.1 Overview 5](#_Toc88122919)

[1.2 Scope 5](#_Toc88122920)

[1.3 Personnel Responsibilities 5](#_Toc88122921)

[1.4 Human Resources Responsibilities 5](#_Toc88122922)

[1.5 Change of Engagement 6](#_Toc88122923)

[1.6 Ceasing Engagement 6](#_Toc88122924)

# Cyber Security Human Resources Policy

This document is the Cyber Security Human Resources Policy. It applies to the management of personnel within <Organisation Name>.

## Overview

<Organisation Name> makes cyber security one of its most important priorities. To that end, personnel being engaged on any basis are subject to review and management for compliance with good cyber security practices. Where third-parties are engaged for provision of services, they too will be informed of their cyber security obligations.

## Scope

All personnel engaged by <Organisation Name> are within the purview of this Policy. These include personnel performing any role or activities who are:

* Employed, contracted or volunteers
* Full-time, part-time or casual
* Third-parties performing services for <Organisation Name>.

## Personnel Responsibilities

All personnel engaged by <Organisation Name> have responsibilities for cyber security. These include:

* Participate in all Cyber Security Awareness Training as may be required from time-to-time
* Abide by all <Organisation Name> policies, and follow all established processes and procedures
* Acting at all times, as much as is reasonably possible, to safeguard organisational data and information to preserve its confidentiality, integrity and availability
* Preventing, wherever possible, the unauthorised disclosure, modification or destruction of organisational data and information
* Safeguarding the physical infrastructure of the organisation.

## Human Resources Responsibilities

<This list includes items that should be considered essential, as well as those that are suggestions.
As always, feel free to add, modify, delete as appropriate for the organisation.>

<Organisation Name> Human Resources also have responsibilities for cyber security. These include:

* Defining and documenting the roles and responsibilities of the personnel being engaged
* Undertaking suitable background and security checks on potential personnel, appropriate to the role and activities the personnel may perform
* Engaging only personnel who pass all relevant background and security checks
* Providing potential personnel with the terms and conditions of engagement, as well as policies and processes related to cyber security
* Ensuring any relevant formal engagement documentation is completed (e.g. contract, Cyber Security Declaration, etc)
* Providing relevant Cyber Security Awareness Training during onboarding
* Providing appropriate access to organisational assets and any relevant equipment (e.g. multi-factor authentication devices).

## Change of Engagement

When a person changes how they are engaged by <Organisation Name>, Human Resources will ensure that immediately after engagement formally changes:

* Human Resources records are updated appropriately
* Access to IT resources is reviewed and changed, if appropriate
* Any relevant equipment (e.g. multi-factor authentication devices) is issued or surrendered, as appropriate.

## Ceasing Engagement

When a person ceases to be engaged by <Organisation Name>, Human Resources will ensure that immediately after engagement formally ceases:

* Human Resources records are updated appropriately
* Access to IT resources is suspended or removed
* Any relevant equipment (e.g. multi-factor authentication devices) is surrendered.