|  |
| --- |
|  |
| **Title of the policy**  **Version control**  **author** |
|  |

# Table of Content

**Section: Page Number:**

[Table of Content 2](#_Toc111103510)

[Cyber security policy and procedure 3](#_Toc111103511)

[Background and Purpose 3](#_Toc111103512)

[1. What is Cyber security? 3](#_Toc111103513)

[Malicious software (Malware) 3](#_Toc111103514)

[Scam emails (Phishing) 3](#_Toc111103515)

[Ransomware 3](#_Toc111103516)

[OS and software updates 3](#_Toc111103517)

[Backups and Scheduling 3](#_Toc111103518)

[Multi-Factor Authentication 3](#_Toc111103519)

[Access control (logins and passwords) 4](#_Toc111103520)

[Sensitive data 4](#_Toc111103521)

[Training 4](#_Toc111103522)

[2. Australian and international legislations that are applicable to the organisation and why 4](#_Toc111103523)

[3. Current information on threats from the Australian government 4](#_Toc111103524)

[4. Policies that will need to be in place 6](#_Toc111103525)

[For individuals 6](#_Toc111103526)

[The network 6](#_Toc111103527)

[The cloud applications 6](#_Toc111103528)

[5. Procedures to enact the policies 7](#_Toc111103529)

[6. Implementing, promoting, and maintaining workplace cyber security 7](#_Toc111103530)

[Approach 7](#_Toc111103531)

[7. Practices to implementing and ongoing awareness for Workplace Cyber Security 7](#_Toc111103532)

[8. Promoting and ongoing awareness for Workplace Cyber Security 7](#_Toc111103533)

[10. Distribution of the policy 7](#_Toc111103534)

[How is the policy and its updates distributed? 7](#_Toc111103535)

[Who is the policy distributed to? 7](#_Toc111103536)

[Approaches and practices Signoff 8](#_Toc111103537)

# Cyber security policy and procedure

## Background and Purpose

Give the background of the policy and state its purpose

State the legislations this policy is based on.

## What is Cyber security?

## Malicious software (Malware)

## Scam emails (Phishing)

## Ransomware

## OS and software updates

## Backups and Scheduling

## Multi-Factor Authentication

## Access control (logins and passwords)

## Sensitive data

## Training

## 

## Australian and international legislations that are applicable to the organisation and why

## 

## Current information on threats from the Australian government

## Policies that will need to be in place

### 

### Policy Statement

State Uptown’s stand on this policy,

what the policy is for - protecting the personal information, Uptowns committed towards this policy - securing your data and keeping it confidential and how Uptown will do this.

If you have any questions about this Policy or our treatment of your personal information, please contact us at support@uptownit.com.au.

### For individuals

The policies that need to be in place for individuals are the following:

### The network

The policies that need to be in place for the network are the following:

### The cloud applications

The policies that need to be in place for the cloud applications are the following:

## Procedures to enact the policies

## Implementing, promoting, and maintaining workplace cyber security

### Approach

### Practices to implementing and ongoing awareness for Workplace Cyber Security

### Promoting and ongoing awareness for Workplace Cyber Security

1. **Maintaining and ongoing awareness for Workplace Cyber Security**

## Distribution of the policy

### How is the policy and its updates distributed?

### Who is the policy distributed to?

### Approaches and practices Signoff

|  |  |
| --- | --- |
| **Signoff** | |
| Policies have been approved by: |  |
| **Initial** | **Supervisor Initial** |
|  |  |