End User Security Policy Template

Note: Delete this and the next page once you complete the template.

Who should use this template?

Any organisation who uses information technology in their business.

Why have an End User Security Policy?

The main benefits to having this policy are that it:

* Ensures all end users are aware of obligations in relation to selection, use and safety when utilising information technology within the business
* Is a proven way to help your managers and supervisors make consistent and reliable decisions
* Helps give each end user a clear understanding as to what you expect and allow.

It takes a little effort to complete, but brings definite long-term benefits, reduces risks, and clearly articulates staff responsibilities in keeping organisational information safe..

How to complete this template

This End User Security Policy template is made up of example topics. You can customise these if you wish, for example, by adding or removing topics.

To complete the template:

1. Guidance text appears throughout the document, marked by the word Guidance. Where you see a guidance note, read and then delete it. Guidance has been added to help you complete the template and should not appear in your final version.
2. Using MS Word's Replace function, search for [Organisation] and replace with your company name.
	1. In Word's Home ribbon, open the Find and Replace tool, choose Replace to open the Find and Replace tool. The Find and Replace dialog opens with the Replace tab selected.
	2. Enter [Organisation] in the Find what field.
	3. Enter your company name in the Replace with field.
	4. Click Replace All



1. Replace [items in square brackets] with your own wording.
2. Where you see a reference to other policies, insert a link to another example policy that applies in your business
3. Once you have finished work on the template, delete the first three pages of the document.
4. Lastly refresh the page numbers in the table of contents.
	1. Right mouse click on the table of contents
	2. In the small menu that appears, choose ‘Update Field’ and then ‘Update page numbers only’.



Other tips

* To stop this policy manual sitting on a desk collecting dust, make it a living document. How? Ask your staff for their thoughts on how to improve it. Then review it annually.
* Make explaining your policies and procedures an important part of your induction process and provide the policy to all employees during on boarding and get them to sign and acknowledge it. If already on board, communicate, educate and get them to sign the policy this new policy to demonstrate the importance of it.
* Obtain annual sign off on the policy from all employees so that they are aware of it and complying with the policy.
* The writing style doesn’t need to be formal or long winded to be effective. Use simple sentences and plain English to reduce the chance an End user or manager will be confused about the intent of your policy or the way to carry out a procedure.

Note: Delete this and the previous page once you complete the template.

Disclaimer

The information in this template is for general guidance only. The Digital Transformation Hub does not make any representations or warranties (expressed or implied) as to the accuracy, currency or authenticity of the information. The Digital Transformation Hub, its end users and agents do not accept any liability to any person for the information or advice given in this document.

[Insert Company Logo Here]

End User Security Policy

Version - 0.1

Effective Date: **<< Date Month Year>>**

Table of Contents

[1 Introduction 1](#_Toc77293612)

[2 Intended Audience 2](#_Toc77293613)

[3 Scope 3](#_Toc77293614)

[4 End User Controls 4](#_Toc77293615)

[5 Policy Governance 9](#_Toc77293616)

[6 Appendices 11](#_Toc77293617)

# Introduction

Guidance: Edit this section in accordance with licthe needs of your organisation. Insert text about introduction and purpose of this document

[Organisation]’s end user devices (e.g. desktop, laptops, tablets, USB memory sticks or mobile phones) are the primary sources of risk to the [Organisation]’s sensitive information and business applications. Implementation of appropriate information security controls for end user devices can mitigate the risk to [Organisation]’s information and IT systems. Consequently, end user protection is critical to ensuring a robust, reliable and secure [Organisation] IT environment. Failing to do so may result in an information security incident, causing financial or reputational loss to [Organisation].

The purpose of this policy is to set forth acceptable usage norms for [Organisation]’s end user computing resources and to provide guidance to end users on the proper use of these resources, including use of the Internet and BYOD (Bring your Own Device).

# Intended Audience

Guidance: Edit this section in accordance with the needs of your organisation. Insert text about who this document applies to.

The target audience of this document is all [Organisation]’s employees (whether permanent, fixed or temporary), volunteers and any third party or sub-contractor that is provided with an electronic identity (e.g. a username and password) to access [Organisation] information services.

For the purpose of this policy, the term ‘employee’ or ‘end user’ includes all groups who have access to [Organisation] electronic resources. Electronic resources include, but are not limited to; personal computers (including laptops), convergent devices such as; tablets, smart phones, or servers, software, network access (including email, calendar, contacts and other related functions, other internal network resources and Internet access) and information stored on [Organisation]’s systems that is kept or used on-site or off-site, whether before, during or after work hours and/or provided by or at the expense of [Organisation].

# Scope

Guidance: Edit this section in accordance with the needs of your organisation. Insert text about scope of the document.

This policy applies to information assets owned or leased by [Organisation], or to devices that connect to the [Organisation] network or reside at [Organisation] sites. This policy applies to all end user devices and equipment issued by the Technology Department to [Organisation] staff, contractors or 3rd parties. It applies to all people using these devices and equipment in the [Organisation]’s offices, off-site, at home, at a client's premises or at any other location; and/or in situations where you are representing [Organisation] or any of its subsidiaries or may otherwise be identified as a [Organisation] end user or associate.

# End User Controls

## User Access and Password Security

Guidance: Edit this section in accordance with the needs of your organisation.

### Users of [Organisation]’s information systems are personally responsible for the use of their account, creating and protecting passwords that grant them access to resources and must:

* 1. Select lengthy (within reason)
	2. Select complex passwords and avoid use of simple passwords such as the name of the service itself, your name, “PASSWORD”;
	3. Use Multi-Factor authentication where possible;
	4. Change their password at first login;
	5. Change their password as soon as possible if they know or suspect that their account has been compromised;
	6. Keep passwords secure, and not reveal them under any circumstances;
	7. Don’t reuse old passwords or passwords used for other purposes. E.g., social media, banking, etc;
	8. Not attempt to use any account other than their own;
	9. Not share their user account with other individuals.

### Passwords must comply with [Organisation] password policies. Passwords must comply with the following requirements:

* + 1. [List password requirements as per the guidance below]

[Guidance: Organisation to define password policy that specifies password length, complexity and longevity, and which is (preferably) enforced by the technology infrastructure. Example:

* + Minimum length - at least eight (8) characters;
	+ Complexity - Combination of alpha and numeric characters and one special character (e.g., %,# )
	+ Multi-factor authentication must be used for public facing applications.
	+ Passwords must not be re-used between accounts
	+ Passwords must be changed at least every 365 days.]

### End users must lock the screen or log off when the device is unattended.

## Data Storage, Destruction and Disposal

Guidance: Edit this section in accordance with the needs of your organisation.

### End users must store all [Organisation] data in the appropriate shared location as provided by [Organisation].

### End users must regularly manage documents in shared locations and delete files and folders that are no longer required.

### [Organisation] IT retains the right to delete any personal media files stored in shared locations. The local storage of data on a personal device (e.g. laptops, desktops, mobile phones and tablets) will not be backed up, and the loss of any information (in the event of a device failure) will be the responsibility of the user.

### End users must take secure backups of files stored locally on personal devices (such as laptops, desktops, mobile phones and tablets) that are not backed up and will not be recoverable in the event that a device is exchanged or a local storage fails or is erased.

### Physical documents containing sensitive information must be shredded prior to disposal.

## Removable Media

Guidance: Edit this section in accordance with the needs of your organisation.

### Use of unencrypted removable media (e.g. USB drives, external hard drives, CDs/DVDs) to store sensitive [organisation to define the appropriate information classification levels such as “Confidential”, “Restricted”] information is prohibited.

### The use of personally purchased removable media is not permitted for business use, unless explicitly authorised to do so by the [organisation to define who can approve the use of personal media e.g. Chief Information Security Officer].

## Email and Internet Security

Guidance: Edit this section in accordance with the needs of your organisation.

### End users are responsible for all electronic activities initiated by them (e.g. email, web browsing, application usage) and electronic content stored by them on [Organisation] IT assets.

### End users should not use corporate email for personal use.

### [Organisation] end users must not:

* 1. Follow web-links or instructions provided by email, unless certain of their origin and function;
	2. Send [Organisation]’s information through unauthorised messaging applications or social media platforms (e.g. WhatsApp, Facebook, etc.)
	3. Send messages or download content that support illegal or unethical activities;
	4. Change the security settings of their email software or Internet browser on a [Organisation] device (e.g. laptop, desktop);
	5. Send sensitive [organisation to define the appropriate information classification levels such as “Confidential”, “Restricted”] information via unencrypted email;
	6. Send emails containing passwords in clear text, or account information such as log-on ID and password combinations;
	7. Use corporate devices or identities to browse, search or interact with the dark web, such as those that require the Tor web browser.

## Social Media Use

Guidance: Edit this section in accordance with the needs of your organisation.

### End users are trusted to act responsibly when using social media sites such as Facebook, Twitter, wikis, blogs, YouTube, and LinkedIn.

### [Organisation] information must only be shared over official, authorised communication channels. [Organisation] information must not be shared on social media sites.

### When accessing social media sites on [Organisation] computers or devices:

* 1. End users may be subject to logging and monitoring checks;
	2. Access may be restricted to social media sites; and
	3. Inappropriate social media websites will be blocked.

### When accessing or contributing on social media sites, end users must:

* 1. Not place comments representing or giving the impression of representing [Organisation], unless explicitly authorised to do so.
	2. Exercise good judgement when blogging or posting.
	3. Not post or view material that is illegal, obscene, defamatory, threatening, harassing, discriminatory, racist, or hateful to another person or entity.
	4. Be aware that information hosted on social media is unverified and must not be used without confirming its authenticity for decision making.

### [Organisation] information must not be sent via unauthorised messaging platforms based on its classification and sensitivity (e.g. WhatsApp, Facebook Messenger, WeChat, etc.) and must only be transmitted using [Organisation] approved and authorised messaging systems.

## Mobile Computing Devices

Guidance: Edit this section in accordance with the needs of your organisation.

In this policy, the term “Mobile Device” refers to an easily portable computing device. These devices can typically process and store information and have an ability to connect to a network. The most common Mobile Devices are laptops, tablets, smartphones and wearables.

Mobile Devices are designated as either “[Organisation] Owned” or “Privately Owned or BYOD”.

### Personal devices or BYOD devices are to only be used where controls have been implemented to manage [Organisation] Information on such devices, e.g. information storage policies, Mobile Device Management (MDM) software etc.

### Only authorised devices are permitted for professional use. Only the owner of the device may be permitted to use approved BYODs to access [Organisation]’s resources. Users must not grant access to their devices to unauthorised individuals.

### The end user or the owner of the mobile device must:

* 1. Allow [Organisation] to install [Organisation]’s mobile device management software onto his/her device.
	2. Employ reasonable physical security measures for the mobile device and is expected to secure it whether or not it is actually in use or being carried.
	3. Inform [Organisation], upon termination of employment, of any approved mobile devices contract or agreement, to be submitted for inspection prior to departure, if required.

### To ensure the integrity and security of our information system and assets, the following requirements must be observed with respect to the use of all Mobile devices.

* 1. Mobile Device Management software should be installed and enabled and must not be removed or tampered with. This software enables the IT department to enforce minimum security features on mobile devices.
	2. Mobile devices must not be used to store unencrypted passwords. To ensure security of [Organisation] systems, encryption should be applied (for example, through an encrypted password management application).
	3. Mobile devices should never be used to store sensitive information, such as health information about clients.
	4. Mobile devices carrying confidential [Organisation] information must not be left unattended and should be physically secured.
	5. Mobile devices must not be used to store pirated software or illegal content.
	6. Users must not bypass access controls on device operating systems added by suppliers.
	7. Mobile device use should be in accordance with all relevant laws, including road traffic laws (which place restrictions on the use of mobile devices while driving) and work health and safety laws. For the avoidance of doubt, [Organisation] will not pay for any fines imposed due to breach of laws.

### In the event a device is lost or stolen, end users or device owners must report the incident immediately.

### In an event of loss, theft or sale of a mobile device, [Organisation]’s IT team must remotely wipe the device and/or [Organisation] corporate information that may be stored on it.

### Where possible, if end users are required to work outside of usual hours of business, or outside of their usual place of business, they should do so on [Organisation]’s systems. However, if an end user is required to perform work on a BYO device (e.g. staff owned and operated, personal computers, laptops, tablets, personal digital assistants, and other mobile devices) they should ensure that:

* 1. The personal device has adequate virus protection; and
	2. No confidential information or data is stored on the personal device, and any data created, formed, or stored on the personal device is deleted once it is no longer required by the end user for their work function;

## Remote access

Guidance: Edit this section in accordance with the needs of your organisation

### When working from home or at an offsite location, end users:

* 1. Must never provide their login or email password to anyone, not even family members;
	2. Must keep conversations confidential. Don’t discuss work issues where others may hear, including elevators and lobbies;
	3. Must not use personal email or cloud storage accounts for work;
	4. Must make sure their home WiFi is password protected;
	5. Must always lock laptop screen before stepping away — and use a laptop lock if in an unsecured area.

## System and Network Security

Guidance: Edit this section in accordance with the needs of your organisation.

### [Organisation] end users must not:

* + 1. attempt to compromise the security of a computer;
		2. access data, a server, or an account for any purpose other than for [Organisation] duties or business, even if access is authorised, unnecessary access is prohibited;
		3. export software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate management should be consulted prior to export of any material that is in question;
	1. introduce malicious programs into the network or server (e.g. viruses, worms, Trojan horses, email bombs, etc.);
	2. reveal account passwords to others or allow use of individual accounts by others. This includes family and other household members when work is being done at home;
	3. use a [Organisation] system / asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction;
	4. make fraudulent offers of products, items, or services originating from any [Organisation] account;
	5. breach security controls or disrupt network communication (except for IT or security staff responsible for maintenance and troubleshooting). For the purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
	6. port scanning or security scanning is expressly prohibited with the exemption of the IT team;
	7. execute any form of network monitoring that will intercept data not intended for the end user’s host, unless this activity is a part of the end user’s normal job/duty;
	8. circumvent user authentication or security of any host, network, or account;
	9. introduce honeypots, honeynets, or similar technology on the [Organisation] network (with the exception of the Security team or equivalent);
	10. interfere with or deny service to any user other than the [Organisation]’s host (for example, denial of service attack);
	11. use any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user’s terminal session, by any means, locally or via the internet/intranet/extranet’
	12. provide information about, or lists of, [Organisation] end users to parties outside [Organisation] unless already classified as “public”, and;
	13. Attempt to attach any unauthorised device to the [Organisation] business network.

## Security Incident Reporting

Guidance: Edit this section in accordance with the needs of your organisation.

Security Incidents are adverse events which pose a threat to [Organisation]’s information systems and services. Security incidents can originate from intentional (deliberate actions against an information system) or unintentional actions (human error).

Examples of potential security incidents include abnormal computer behaviour, which may be caused by a computer virus, malware, worm, a non-escorted guest, disclosure of information to a unauthorised person, lost or stolen physical access cards, removable media, laptops and passwords and unauthorised access to an information system or physical premise.

### In case [Organisation]’s end users observe any unfamiliar activity on their workstation, they shall immediately disconnect the system from the network and report the incident to the IT service desk or their immediate supervisor (or equivalent). The following steps enumerate the actions to be taken by end users on encountering an incident:

* 1. Immediately report any unfamiliar activity or suspected security incident to the [Organisation]’s IT service desk on [insert contact details] or email [email address].
	2. End users shall comply with the directions given by the IT service desk to facilitate a quick response, repair of the system, restoring the service and analysis of the incident.

### End users must not:

* 1. perform an action (e.g. delete system files) to eradicate or contain a suspected security incident unless explicitly instructed by the [Organisation]’s IT service desk or security team; and
	2. disclose information relevant to security incidents to unauthorised entities.

## Copyright and Intellectual Property

Guidance: Edit this section in accordance with the needs of your organisation.

### When using [Organisation] or own devices, networks or storage media [Organisation]’s end users must not:

* 1. store, transmit, or make available unauthorised copies of copyrighted material using [Organisation] resources or IT systems; or
	2. use peer-to-peer file transfer services or take actions likely to promote or lead to copyright infringement.

### When using [Organisation]’s resources and IT systems, end users must:

* 1. only use licensed software officially installed/registered and owned by [Organisation];
	2. only use the applications to which they have authorised access;
	3. comply with the terms of license signed by [Organisation] for software programs, online databases, online software packages, etc; and
	4. ensure copyright material is only retrieved, copied or used with the permission of the copyright owner under the terms of a copyright licensing agreement, or as permitted by law.

### [Organisation] end users must not:

* 1. install or use any unauthorised software;
	2. make/use illegal copies of licensed software;
	3. use software that they suspect to be unlicensed; or
	4. download, copy, store, transmit, and stream material such as music, video, movie, or other copyrighted files without the express permission of the copyright holder or as permitted by law.

# Policy Governance

Guidance: Edit this section in accordance with the needs of your organisation.

## Policy Enforcement

Each member of staff is expected to fully comply with this policy. If there is any failure to observe the policy, disciplinary measures may be taken. The measures taken will vary according to the breach and the circumstances of the breach. However, the right is reserved to immediately terminate the employment of any staff member who is in serious breach of this policy.

## Handling Exemptions

The control exception process allows [Organisation]’s end users (where technological or operational constraints or a legitimate business requirement exists) to request an exception from a defined control within this Policy. Exemptions requests must be reviewed and assessed by the [insert relevant job title here] and approved by the [insert relevant job title here]. All control exemptions must be documented with a rationale and reported to the [insert relevant committee/title here]. Control exemptions are to be reviewed on a periodic basis.

## Review of Information Security Policy

The Policy document must be reviewed on an [Organisation to define the frequency of review e.g.,annual basis] basis and updated if required, to ensure standards remain up-to-date and continue to meet the requirements of [Organisation].

In addition to the annual review cycle, the Policy must be able to evolve in order to meet changing internal and external requirements, which may include:

* changes to [Organisation] business and IT environment;
* changes to tolerance to risk or risk appetite;
* changes to legal and regulatory requirements;
* changes to contractual requirements; and
* changes to adapt to emerging risks and threats.

## Endorsement and Approval

Unless otherwise noted, this policy is effective from the date of approval.

This policy has been approved and endorsed by:

|  |
| --- |
| Document details |
| **Name of document** | [Insert approved name of this Policy] |
| **Version** | [Insert current version] |
| **Author** | [Insert Name and title of the person who prepared this policy] |
| **Reviewed By** | [Insert Name and title of the person who reviewed this policy] |
| **Approved By** | [Insert Name and title of the approver of this policy] |
| **Date of Approval** | [Insert Date Month Year] |
| **Date of Effect** | [Insert Date Month Year] |
| **Assigned Review Period** | [12 Months] |
| **Date of Next Review** | [Insert Date Month Year] |

This policy is due for review by the date shown above, after which it may become invalid. Policy users should ensure that they are consulting the currently valid version of the document.

# Appendices

Guidance: Edit this section in accordance with the needs of your organisation.

## Appendix A - References

The following documents are relevant to this document.

|  |  |  |  |
| --- | --- | --- | --- |
| Ref | Title | Version | Author |
| 1 | [Insert related document such as Privacy Policy, Information Security Policy] |  |  |
| 2 |  |  |  |
| 3 |  |  |  |

## Appendix B - Document Change Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Change Description | Reviewed By | Approved By | Date |
| 1.0 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Appendix C – Acronyms/ Definitions

Guidance: Insert definitions and information relating to key terms and acronyms referred to in this Policy.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |