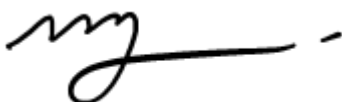


IT Security Policy

2024-2025

Prepared by	Authorised by	Board Signature
Name: Aqib Hussain/Solaas	Name: Name Here	Name: Name Here
		Name: Warwick Nash 
Date last reviewed:	31/07/24	
Effective from:	01/08/24	
Date of new review:	31/07/25	

Purpose

The purpose of this document is to specify and communicate minimum requirements for access to information processing facilities and data. It is independent of any hardware and software environment and should be used as a generic baseline for the implementation of security for any system or application. It is the policy of Apprentify that all information it manages shall be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

Scope

The policy applies to all Apprentify personnel irrespective of status, including temporary staff, contractors, consultants, and third parties who have access to Apprentify data and systems. There may be circumstances where it is not possible to fully apply the policy in which case a risk assessment should be conducted in accordance with the Risk Control process.

Statement of Policy

The access control policy of Apprentify is as follows:

- All access will be in accordance with the minimum privilege principle in that access to systems and information is denied except where it is specifically required for business purposes.
- Access to Apprentify information facilities, systems and data will be controlled. All access procedures must be fully documented.
- Access to Apprentify information facilities, systems and data that are not in the public domain are to be subject to a confidentiality agreement, either in a contract or as a condition of employment.
- All users will be authenticated and accountable for their actions on Apprentify systems.
- All system access architecture, software and hardware will be configured such that opportunities for unauthorised access or denial of service are minimised.

Roles and Responsibilities

Chief Operating Officer duties and responsibilities include the below:

- Running regular check on network and data security.
- Developing and implementing IT Security Policy and best practice guides for the organisation.
- Overseeing and determining timeframes for major IT Projects including system updates, upgrade, migration, and outages to systems.
- Conducting regular system audits.
- Identifying and acting on opportunities to improve and update software and systems.
- Testing all new software to ensure capability to Apprentify systems.
- Antivirus software Defender and Guardz installation on all systems. Annual review and re-evaluation of low-risk systems and appliances not considered affect by malicious software based on current best practice.

Access Control

The objective of information security is to achieve and maintain a condition where all information is always available to all those who need it, cannot be corrupted, or disclosed to unauthorised persons and its origin is authenticated. This involves the preservation of:

- Confidentiality - ensuring that information is only accessible to authorised persons.
- Integrity - safeguarding the accuracy and completeness of information and processing methods.
- Availability - ensuring that authorised users have access to information and associated assets when required. Non-repudiation - the reasonable assurance that, where appropriate, a user cannot deny being the originator of a message after sending it.

Access to all information will be controlled and will be driven by business requirements. Access will be granted, or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed and will include consideration of multiple factors as appropriate.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented, where practical.

It is the policy of Apprentify to ensure that information assets are protected from all threats, whether internal or external, deliberate, or accidental. The policy therefore requires that

access to information systems is controlled. This is achieved through implementation of a combination of independent but mutually supportive technical controls and procedures that are designed to detect, deter, and delay security attacks and facilitate investigation.

Password Guidelines

- Change default passwords and PINs on computers, phones, and all network devices
- Don't share your password with other people or disclose it to anyone else
- Don't write down PINs and passwords next to computers and phones
- Use strong passwords
- Change them regularly
- Don't use the same password for multiple critical systems
- Users should be forced to change their password upon initial logon and after their password has been reset by an administrator. This will ensure that the password is unique and known only to the owner. Once the user has changed their password, they are responsible for its use and confidentiality.
- Passwords should not be displayed on the screen in clear text. This prevents any unauthorised viewing.
- Passwords will be managed by Password Keeper with a full audit trail.

Data Protection Officer

The Data Protection Officer is responsible for ensuring that Apprentify Ltd and its constituent business areas always remain compliant with Data Protection, Privacy & Electronic Communications Regulations, Freedom of Information Act, and the Environmental Information Regulations. The Data Protection Officer shall:

- Lead on the provision of expert advice to the organisation on all matters concerning the Data Protection Act, compliance, best practice and setting and maintaining standards.
- Provide a central point of contact for the Act both internally and with external stakeholders (including the Office of the Information Commissioner).
- Communicate and promote awareness of the Act across Apprentify.
- Lead on matters concerning individuals right to access information held by Apprentify and the transparency agenda.

Apprentify's DPO is Aqib Hussain.

Antivirus

All workstations and servers will have Antivirus & Firewall (Defender and Guardz) installed to block unnecessary access to networks and computers, improving user security awareness, early detection, and mitigation of security incidents, preventing and addressing computer virus, worm, spyware, malware and other types of malicious software.

The following procedures should be followed:

- Virus protection software (Defender/Guardz) must not be disabled or bypassed.
- Setting of the virus protection software (AVG Business) must not be altered in a manner that will reduce the software effectiveness.
- Automatic update frequency cannot be altered to reduce the frequency of updates.
- All devices must have Defender and Guardz installed and be setup to detect and clean viruses.
- Any threat that is not automatically cleaned, quarantines and subsequently deleted by malware protection software (Defender and Guardz) constitutes a security incident and must be reported to the Chief Operating Officer.

Two Factor Authentication

All users will be instructed to log into their designated device via a Two Factor Authentication application (Duo) this is to protect users and Apprentify assets from unauthorised use, this will require an application installation on the user's mobile device.

Data Storage

Devices and Media Portable mass storage devices (e.g., portable hard drives) have considerable data storage capacity and are particularly suited for transporting and backing up large amounts of data when backup to a server is not possible. However, due to the universal connectivity of such devices, uncontrolled use and lack of user diligence can lead to introduction of unauthorised software, malicious software (malware), and inappropriate content on PCs and potentially the Apprentify network. Further, such devices are prone to loss and theft and loss or compromise of data.

The following are the security requirements relating to the use of portable mass storage devices:

- Only devices provided, supported, and maintained by the Apprentify are to be used. The storage of Apprentify data on privately-owned devices is forbidden. All devices are the responsibility of the user, which includes the prevention of loss and theft.
- All users must be made aware of the specific security risk relating to portable mass storage devices.

- All data held on portable mass storage devices is to be on a temporary basis only for the specific business purpose of transferring or backing up data where access to a server is not possible. The period for which data is retained on such devices must be kept to a minimum, and all data should be backed up to a server at the earliest opportunity.
- Generally, Apprentify sensitive or personal information should not be transferred to or stored on portable mass storage devices. Where this is unavoidable, only a device with an encryption and authentication capability is to be used. These will be provided by Apprentify based on business justification.
- USB Flash drives (commonly known as “memory sticks”) have increasingly large storage capacity and are particularly suited for transferring data from one computer to another without the need for any connectivity. However, such devices are particularly prone to loss leading to loss or compromise of data. In addition to the security requirements relating to the use of portable mass storage devices, all data held on USB Flash drives is to be on a temporary basis only for the specific business purpose of transferring data. Permanent or long-term retention of data on USB Flash drives is forbidden.

Safety Online

Apprentify staff are given training as part of their safeguarding induction to help them understand the issues of radicalisation. Staff can recognise the signs of vulnerability or radicalisation and know how to refer their concerns. Staff will be updated as necessary in staff meetings, by email and other appropriate means.

The internet provides access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used on the Apprentify network block inappropriate content, including extremist content.

Apprentify is aware that many learners have unfiltered access to the internet when using their mobile phones, and staff are aware of the need for vigilance when students are using their phones.

Apprentices and staff are advised as part of their induction how to report internet content that is inappropriate or of concern.

Searches and web addresses accessed via Apprentify network are monitored automatically, and the Chief Operating Officer will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.

Where staff, students or visitors find unblocked extremist content they must inform the Chief Operating Officer and the Designated Safeguarding Team.

Any apprentices who have concerns about the potential radicalisation of fellow students using the Apprentify IT systems and networks to communicate or access information that has the potential to radicalise; should contact a safeguarding officer to report their concerns to be dealt with. This is irrespective of if they are using their own or the Apprentify computing facilities. This also includes apprentices posting on social media (inside or outside of Apprentify premises) materials to radicalise, or if they are signed up to receive such communications, to report this to Apprentify Designated Safeguarding Team immediately.

Internet Use

Use of internet by employees of Apprentify are permitted and encouraged where such use supports the goals and objectives of the business.

Apprentify staff must ensure that they:

- Comply with current legislation.
- Use the internet in an acceptable way.
- Do not create unnecessary business risk to Apprentify by their misuse of the internet.

The following is deemed unacceptable use or behaviour by employees:

- visiting internet sites that contain obscene, hateful, pornographic, or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, film, or music piracy
- using the internet to send offensive or harassing material to other users

- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material about Apprentify, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format
- revealing confidential information about Apprentify in a personal online posting, upload, or transmission - including financial information and information relating to our customers, business plans, policies, staff, and/or internal discussions
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of malicious software into the corporate network

Internet Use Monitoring

Apprentify accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

In addition, all the company's internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

User Accounts

- Each user must be uniquely defined in the system to ensure accountability and control of user actions.
- A consistent naming structure must be maintained to ensure that each user is identifiable. For example, if users are identified on the Apprentify network using the first name followed by their surname, then Bob Smith would have a username of bob.smith. Where there is duplication, a number can be added (e.g., bob.smith1).
- User IDs must not contain any sensitive information e.g., such as a government issued National Insurance ID number in part or in whole.
- Applications being hosted at third parties (e.g., Software as a Service) must not use Apprentify user credentials (i.e., Usernames or Passwords) for authentication.

Review

This policy will be reviewed annually or earlier if required.