Technological, Organisational & Physical Security Controls

July 2026

Contents

Technological, Organisational & Physical Security Controls

User Endpoint Devices

All user endpoint devices are joined to the Office 365 environment.

Provided access is granted, company provided end user devices can be used to access files from the local on-site file server. Personal devices (or BYODs) are not permitted to be used to access company files unless authorised by Top Management.

Users are made aware of their responsibilities with regards to usage of company devices, including how to securely handle their devices and the restrictions imposed on the software that can be used. This is communicated in regular security training sessions.

User workstations with local accounts are protected by strong, unique passwords which are only known to the intended user.

Privileged Access Rights

By default, all users operate their workstations in non-administrative profiles. If a user wants to do something that requires elevated privilege levels (such as installing additional software) a request must be sent to Top Management for consideration and authorisation. If approved, a member of staff with elevated access will perform the task for the user, or an elevated role may be provided to a user on a time limited basis to fulfil their function. This is enforced manually via periodic review.

All standard users also have non-administrative accounts while accessing the Office 365/Google Workspace environments.

IT, and certain specified members of Top Management, have separate administrative accounts to perform admin functions on devices and Office 365/Google Workspace services.

Requests for elevated/privileged access rights are managed and retained via email.

Information Access Restriction

Access to information that sits behind applications is restricted in accordance with the Access Control Policy. The following restrictions are in place for such applications.

Application	Type	Permissions
Microsoft Office 365	Intranet/Emails	All Staff (MFA)
Google Workspace	Intranet	All Staff (MFA)
Cloud services/platforms administration pages	Admin/Config Pages	IT Support Staff/Top Management
Xero	Accounting Application	Accounts Department, Top Management

These applications are implemented with the following rules:

- Default usernames are removed and replaced with either staff usernames or abstract usernames.
- Default passwords are removed and replaced with strong, randomly generated passwords.
- Least privilege principal used where possible.

Secure Authentication

The use of multi-factor authentication is enforced on all user accounts with access to critical information systems. This is facilitated either using the Microsoft/Google Authenticator application on a user's mobile device (preferred option) or via a code sent via SMS message to the user.

Protection Against Malware

All systems, including servers and workstations must have up-to-date anti-malware software installed. This software should:

- Provide real-time protection against malware threats.
- Automatically update malware definitions to recognise the latest threats.
- Perform regular system scans for malware on a scheduled basis.

Email systems and web access points must be equipped with malware filters to block phishing emails, malicious attachments and infected websites.

Anti-malware tools must be configured to detect, quarantine and remove malicious software as soon as it is identified. In the event of a malware incident:

- Follow the Incident Response Procedure to contain, investigate, and remediate the malware infection.
- Isolate infected devices from the network to prevent the spread of the malware.
- Identify the source of the malware, assess the impact, and take corrective actions to prevent future incidents.

Logs should also be maintained of malware detection, quarantine and removal activities.

Protection Against Malware Procedure

ST4G/VDS uses Microsoft Defender to scan all inbound email messages for potential scam or phishing emails, as well as for any messages that may contain malware. Any messages that contain malicious content are not delivered to the intended recipient and are deleted or quarantined.

All workstations are protected from malware using Microsoft Defender. This software is automatically updated, and the updates are distributed automatically to each machine. Real-time detection is enabled and support by the tool's detection technologies.

All workstations are protected by Microsoft Defender's software firewall.

Information Backup

All information is stored locally via on-site NAS drives. Information from these drives is backed up daily (at midnight every night) to a separate, encrypted drive which is stored off site.

Backups are tested weekly to ascertain efficacy.

Backups are encrypted both in transit and at rest.

Redundancy of Information Processing Facilities

ST4G/VDS utilise onsite, local storage servers for information processing and storage, and onsite network equipment.

Redundancy of information processing and storage systems is ensured by keeping several spare drives in reserve if one was to fail. In this instance, the failed drive can be restored from backup and re-entered into service.

Redundancy of networking equipment is ensured by keeping spares of critical equipment, such as network access points and routers to ensure they can be hot swapped in the event of failure.

With regards to Microsoft/Google environments, redundancy is ensured as the cloud-based providers used have multiple locations from which our tenant can be hosted, meaning if one locations infrastructure were to fail, our tenant can be hosted on another site with minimal disruption.

Uninterruptable power supplies are in use throughout the office/warehouse locations if a location wide power outage were to occur.

All staff have been trained to use dongles available in the office/warehouse to connect to the internet if the primary internet connection fails.

Logging

Audit logs of user activity are available using Microsoft 365 Admin Centre and include:-

- User IDs;
- Dates & times of log-on and log-off;
- Records of successful and rejected logins;
- Computer/Device identification.

Logs are retained for a minimum of 6 months. These logs are only available to tenant administrators.

Logs are not editable or viewable by unauthorised persons.

Where possible, operator logs are turned on within applications and service administration pages.

Use of Privileged Utility Programs

The use of utility programs is controlled by Top Management. Due to restricted permissions; users are unable to install utility programs on their workstations. If a user wishes to install a new piece of software, they must contact Top Management to do so, who will then get in touch with IT.

Installation of Software on Operational Systems

The principle of least privilege is applied to all ST4G/VDS user accounts and workstations. Only authorised software, as defined by Top Management, can be installed on company equipment.

Operational software is only installed and updated by IT. Software is appropriately assessed and tested before it is deployed.

Network Security

Host based firewalls are in place, centrally controlled, and active on each company provided workstation.

All routers and other networking equipment in use has had the default password changed.

Access Control Policy

ST4G/VDS controls access to information based on business and security requirements.

The basic principle is that access to all systems, services and information is forbidden, unless expressly permitted to individual users or groups of users.

The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

The access rights to each application consider:

- The sensitivity of information processed within that application and ensure that there is consistency between the sensitivity and access control requirements across the systems and network;
- Data protection and privacy legislation and contractual commitments regarding access to data or services;
- The ‘need to know’ principle (i.e. access ins granted at the minimum level necessary for the role);
- ‘Everything is generally forbidden unless expressly permitted’.

User access requests are subject to formal authorisation, to periodic review and to removal.

Information Transfer

Where possible, information that needs to be passed to a client or customer that is ‘Confidential’ is encrypted using password protection and sent as an attachment to an email. The password is sent separately either by SMS or telephone.

Physical Storage Media Transfer
ST4G/VDS prohibits the use of any physical storage media to transfer data unless prior approval is given.

Approved media containing files that are ‘Confidential’ must be sent by approved courier. Files must be encrypted whilst saved on removable media. Passwords are to be sent via a different channel.

It is the responsibility of the sender to obtain acknowledgement of receipt.

Verbal Transfer
To protect verbal transfer of information, personnel and other interested parties should be reminded that they should:

- Not have confidential verbal conversations in public places or over insecure communication channels since these can be overheard by unauthorised persons;
- Not leave messages containing confidential or sensitive information on voice messages since these can be replayed by unauthorised persons, stored on communal devices/systems or stored incorrectly because of misdialling;
- Be screened to the appropriate level to listen to the conversation;
- Ensure that appropriate room controls are implemented (i.e. closed door);
- Begin any sensitive conversations with a disclaimer so those present know the sensitivity and any handling requirements of what they are about to hear.

Identity Management

Users are registered as part of the induction process. New joiners are made aware of their obligations to information security and data protection upon joining the organisation. Once these steps have been taken, they are provided with an initial password for their user account. This password is provided to the individual in person by Top Management. The access rights for the user are agreed with the individual's line manager. Users are requested to change the initial password provided to them upon first login.

Users are de-registered immediately following their last day of employment. The Top Management Team will contact IT to notify them of the employees last day, and, upon cessation, IT will block the leavers user account from being able to sign in via O365 and change the password. This will stop users from being able to access emails and on-site infrastructure.

All users have their own, unique individual user accounts. No account sharing takes place.

Physical Security Perimeters

ST4G/VDS operate in an office/warehouse which has a secure perimeter. During non-working hours, the front door to the building is locked, and is armed with an intrusion detection alarm system. If the alarm is sounded, the Top Management team is alerted.

CCTV is available on the perimeter of the building, including the street outside. These recordings are retained for at least 30 days.

Working In Secure Areas

The use of video recording equipment, cameras of all types (including mobile phones) and other such items is not allowed without the express permission from Top Management.

Visitors and third-party personnel only have access to the secure areas as and when they are required to do so. Visitors and third-party personnel are accompanied by a member of staff where appropriate unless they or their organisation on their behalf has signed an appropriate non-disclosure agreement.

The host is responsible for ensuring that the visitors and third-party contractors are made aware of their security requirements and comply with them.

In general, the owner of a secure area and all those that are authorised to work within it, are required to only divulge details of the area and what is done within it to other staff on a need-to-know basis.

Clear Desk & Clear Screen

ST4G/VDS operates a clear desk and clear screen policy. This means that staff are required to lock their devices when they step away and are required to remove all sensitive information from their working area overnight, storing it in a secure location. Staff are made aware of their commitments and obligations with regards to this policy.

Encryption

File servers are encrypted using the industry standard AES-256 Bit encryption algorithm.

Emails from Outlook clients to servers are encrypted using TLS 1.3 SHA256 encryption.

Backup drives are encrypted with AES-256 Bit encryption.

All user accounts on cloud services are protected via strong, unique passwords and a multi-factor authentication method.

Staff are required to encrypt files containing confidential information so that they remain encrypted in transit and at rest. The preferred method for encryption in WinZip.