Information Security Policy

INTRODUCTION

The Start Group Pty Ltd works extensively with Information Technology, and in particular, is a custodian of sensitive business and operational data on behalf of its customers. It is therefore critical that the organisation has a comprehensive Information Security Policy and is focused on its own, and its customers', data security. This policy establishes a high-level framework for the protection of information and systems.

This policy supports:

- Meeting customer requirements and statutory standards for information security and privacy;
- Provision of a 'duty of care' to the protection of client information, corporate information, information systems, and end-customer information.

Compliance with this policy is mandatory. Breaching this policy is a disciplinary offence.

Aim

The aim of this policy is to establish the high-level objectives concerning the security and confidentiality of all information, information systems, applications and networks owned, held or managed by The Start Group Pty Ltd and all of its subsidiaries. Information security is intended to safeguard three main objectives:

- **Confidentiality**
  Data and information assets must be confined to the people authorised to access them and not be disclosed to others;

- **Integrity**
  Data must be kept intact, complete and accurate and systems must be kept operational;

- **Availability**
  The information or system must be available for use by authorised users when required.

Scope

This policy applies to all information, systems, networks, applications, locations, equipment, devices and users within the Company. All staff, including part-time, full-time, and contracted staff, are covered by this policy.

DEFINITIONS

Terminology

MUST – This term means that the definition is an absolute requirement of the policy.

MUST NOT – This term means that the definition is an absolute prohibition of the policy.

SHOULD (NOT) – This term means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications, including risks, must be considered and understood.

Group / Company

The Start Group Pty Ltd, and all subsidiary entities whether partially or fully owned, including Start Services Pty Ltd.

Staff

Full-time and part-time individuals who are employed, or contracted, by the Company.

Product(s)

Software developed by the Company for resale, projects, one-off-solutions, or otherwise, in which the Company holds intellectual rights and which it typically intends to license for commercial gain. Products may be shrink-wrapped, hosted, SaaS, or hybrid-on-premise as best suits their purpose.

Corporate Network

The Corporate Network consists of the Company's wired and wireless networks that provide direct access to internal computers, services, and networks, including those physically located in Company owned or leased premises, as well as those hosted in 3rd party data centres on behalf of the Company and which are typically connected via the company WAN or VPN. Guest networks that do not provide access to internal company services are excluded.

Hosted Network(s)

The Hosted Network(s) consist of dedicated wired networks inside secure data centres, and isolated behind secure firewall appliances, which host systems on behalf of the Company's customers. The Hosted Networks are not physically connected to the Corporate Networks, and can only be accessed by physically attending the data centre, or by dedicated and secure VPN. There is no guest access to the Hosted Networks, nor any general staff access. Only authorised personnel may connect to the Hosted Networks. All customer access to data stored within the Hosted Networks is via browser connections over the public internet which are protected by encryption security (SSL) certificates (refer later).

Company Managed Device

A Company owned electronic device, such as a desktop computer, laptop, mobile phone, tablet, server, or appliance which is managed by Company System Administrators.

Staff Managed Device

A Company owned electronic device, such as a desktop computer, laptop, mobile phone, tablet, server, or appliance, that is managed by an individual staff member and not solely by the Company System Administrators.

Staff Owned Device

A staff owned electronic device, such as a desktop computer, laptop, mobile phone, tablet, server, or appliance, that is managed by the individual staff member, but which connects to the Corporate Network.

External Services

A service for which the Company is not the developer, service provider, nor system manager, e.g. Office 365, ClickUp, or GitHub, etc.

Sensitive Information

Information is considered 'sensitive' if it has, or should have, an official government classification (for example UNCLASSIFIED DLM (OFFICIAL), PROTECTED, SECRET or TOP SECRET), or if the information has commercial or privacy-related implications for the Company, Staff or customers.

Examples of Sensitive Information:

- Implementation details for Company Products and services (e.g. source code and programming strategies);
- Corporate processes and procedures, financial information, including charge rates, salaries, bids, overhead costs;
- Information owned by a customer or used in providing a service, including products, architectures, services provided, user accounts, unless permission is granted by the customer for publication;
- Identification information such as a person's name, address, or date of birth.

PREAMBLE

The Company recognises that its core competency is product development, and solution deployments. The environment in which software is deployed and used is changing rapidly and continually and it is our responsibility to identify and adapt to changing circumstances to continually provide the best protection of our own, and our customer's, data, information, intellectual property, and systems.

Hosted software solutions are becoming more common, and also more complex, with intrusion attempts occurring daily on most public-facing systems. Protecting these systems requires a multi-layered approach as outlined in this document, with a focus on physical isolation, logical isolation, and finally data protection techniques. Customer data, in particular, should only be accessible by specifically authorised personnel, and then only to assist our customers with their systems and never for personal or company gain.

The Company further recognises that some aspects of its deployment practice is best serviced by external professions who specialise in specific aspects of data security. Company firewall's, for example, are maintained by the firewall vendor (Meraki) and continually updated to ensure best-practice protection of our internal networks and systems. The Company has assessed and identified appropriate vendors and suppliers to fulfil specific aspects of its hosting and delivery solutions, and relies on those vendors and their information security policies as a standard part of the protection mechanisms.

This policy describes the responsibilities of our staff, and the general protection policies which our Company employs to safeguard information and systems. Implementation details of these policies is described elsewhere in documentation pertaining to each particular service, facility, design method, and product feature.

It is mandatory for all new staff to read this policy, and adhere to its directives.

PERSONNEL RESPONSIBILITIES

Managing Director

The Managing Director has ultimate responsibility for all undertakings in all of the offices of the company. The Managing Director is the Senior Executive who provides the business direction for the Company and strategic oversight over all decisions made within the Company. The person in this role holds the overall responsibility for ensuring that risk is managed according to best practice within the industry for all areas of exposure within the Company. The Managing Director provides strategic oversight into information security for the Company with

respect to business decisions, including overall responsibility for the architecture and implementation of information security policies across the Company.

The Managing Director holds Negative Vetting 1 security clearance from the ADF, authorising access to classified information and resources up to and including SECRET.

Operations Manager

The Operations Manager is the Senior Executive responsible for managing technical operations within the company, including the delivery of projects and appropriate handling of customer data. The Operations Manager is responsible for all aspects of the technical data safety, including infrastructure, hardware, software, networks, VPNs, WANs, and personnel. The Operations Manager is responsible for information technology security implementation on systems across the Company and manages the day-to-day operations of information security.

The Operations Manager holds Negative Vetting 1 security clearance from the ADF, authorising access to classified information and resources up to and including SECRET.

System Administrators

Systems Administrators report to the Operations Manager and implement technical solutions, under the guidance of the manager, which ensure that the strategic direction for information security is achieved within the company. The system administrators are responsible for the upkeep, configuration, and reliable operation of computer systems, including servers and data centres, physical and virtual, installed and hosted systems. The system administrators are also responsible for planning for and responding to system outages and other problems, including cyber security threats or incidents.

The Systems Administrators are responsible for ensuring the technical security of the systems by implementing and monitoring technical security measures. The System Administrators are responsible for the administration of Company Managed Devices and ensuring that they meet applicable security policies, processes and procedures for those devices. The Systems Administrators conduct vulnerability assessments and take actions to mitigate threats and remediate vulnerabilities; work with the Operations Manager to respond to cyber security incidents; assist with the selection of security measures with respect to disaster recovery and raise awareness of information security issues.

Project Leaders and Lead Solution Architect

The Project and Technical Leaders are highly experienced staff, usually Senior Developers, who have the skills and experience necessary to manage projects within the organisation. These staff take responsibility for ensuring that products and projects meet clients' expectations and delivery timelines, whilst ensuring that the systems supplied meet the company's high standards for security, availability and usability. These Leads manage teams of developers and engineers who work together to produce the products for the company, or the solutions for our customers. Leads will usually manage several projects concurrently, using the company's agile development framework and toolsets to stay abreast of work being undertaken by the teams on a daily basis, as well as getting frequent updates on progress and challenges during the day.

Developer Team

The Company employs both Junior and Senior Developers. The developers report to the Lead Solution Architect. They are responsible for developing the products, implementing solutions, and providing enhancements and updates to the underlying codebases for ongoing customer benefit. Strategic security policies for software development are built into the products (e.g. server-side security validation on every client request) and mandatory for all new features. The Lead Solution Architect has final say in the software design of all products to ensure customer data safety is not compromised.

Engineering Team

The Company employs both Junior and Senior Engineers. The engineers report to the Operations Manager. They are responsible for implementing solutions, delivering projects, upgrading systems, and providing support to the company's customer base. The engineers come into contact with Customer Sensitive Information more than any other personnel in the Company, and are accountable for following this policy to ensure the safety and integrity of our customer's data.

Administration Team

Administration personnel are responsible for day-to-day business operations of the Company, and have access to the Corporate Network and related business systems, but no access to customer data or information. The Managing Director oversees the administrative staff and all administrative business functions. The administration personnel are responsible for maintaining security of administrative information, including safeguarding the privacy of individual staff members' detailed information and Company sensitive information.

All Staff

All company staff are responsible for:

- Understanding all company security policies, processes and procedures that apply to them.
- Appropriate management of any Company Managed Devices used by them (including keeping operating systems and applications patched and up-to-date).
- The security of any Staff Owned Devices used to connect to the Corporate Network and ensuring that they are configured and managed in accordance with suitable security principles.
- The actions of their guests and visitors.
- Ensuring that any external service (e.g. Kiteworks) that is used to store or transfer Company or customer information has been previously approved for use by the Operations Manager.
- Being vigilant for any security concerns and reporting them as soon as reasonably practicable.
- Reporting security incidents as soon as possible by contacting a systems administrator, the Operations Manager, or the Lead Solution Architect.

CYBER SECURITY STRATEGY

The Company has a cyber security strategy which governs all aspects of the Company's approach to managing information security. The Company recognises that the threat environment on the public Internet is constantly changing and that systems open to the public internet must be secured by appropriate measures, encryption, certificates, and firewalls. The Company further recognises that a breach of security may create significant commercial compromises for our customers, and ourselves and that the cost of such a breach cannot easily be ascertained. As such, the Company considers all public internet systems a threat, and requires appropriate precautions be taken by all staff, under all circumstances, to protect systems, data, sensitive information, and intellectual property.

The Company maintains the following policies which are mandatory and non-negotiable:

1. Staff must only install and use software which has been approved for use by management.

2. All devices which connect to the Corporate Networks or customer systems must have appropriate and up-to-date security protection software installed and active at all times.

3. All public-facing systems (e.g. demonstration websites or customer hosted systems) must be protected by encryption certificates, and protected by modern security appliances which regularly update their security provisions.

4. Firewalls which protect the Corporate Networks must be configured for port blocking by default, with only explicit ports opened and routed to appropriate services within the networks. No general access ports shall

be opened (e.g. RDP, Telnet, etc). Any remote access to systems within the Corporate Networks must only be performed via secure and encrypted VPN connectivity.

5. All on-premise connections to Corporate Networks or hosted systems must be protected by bespoke IP-specific firewall and routing rules, and must employ data encryption technologies.

6. Account details, including passwords, must not be saved in browser or operating system caches. Account details may be stored in the approved account management system, LastPass.

7. Staff must lock their devices whenever they leave their desk for any purpose. Devices must not be left in vehicles, nor left unattended at any location other than within the work place or home.

Remote Work

The Company supports a flexible working environment, and requires its staff to recognise that with this flexibility comes rules and governance to protect both the Company and its customers. Staff working from home must ensure that only Company approved devices connect to the Corporate Networks, and that those devices adhere with the security protection policies listed above.

All remote connection to the Corporate Networks must be performed via secure, encrypted, VPN authorised and provided for by the Company. Such access is only provided for business purposes and only for staff. It is the responsibility of the staff member who is initiating the VPN connection to ensure that the accessing device they are using is appropriately secured.

The Company provides significant resources for use by staff in its data centre, as well as high-speed, secure VPN access to the Corporate Network from remote work locations. Any customer data provided to the company for any purpose should only ever be stored on the Company's secure data servers. Staff should not transfer Company data from the secure, central data centres to their local devices, and must not transfer customer data to their local devices without specific authorisation from management.

Hosted Systems

The Company provides hosted systems for use by its customers. These systems, by their nature, capture and store customer data. These systems are managed explicitly by the System Administrators to ensure that they comply with the Company's data security policies. These systems are not connected to the Corporate Networks, but are instead isolated within their own secure network in the Company's data centre. Staff must not create permanent connections between the Hosted Networks and the Corporate Networks, and must only connect to the Hosted Networks when authorised to do so, over a secure and dedicated VPN which is different to the Corporate Network VPN.

Hosted Systems have additional policies to the Company's standard data security policies as follows:

1. All Hosted Systems must have secure, encrypted (SSL) certificates for customer access.

2. Hosted Systems must only reside on the Hosted Networks, and must not be physically connected to the Corporate Network.

3. Only System Administrators may access the Hosted Networks and Hosted Systems. All staff access must be via a secure, encrypted VPN.

4. Customer login passwords shall never be stored by any Hosted Systems. Only an encrypted token may be stored, and only in a format whereby a password cannot be reverse engineered from the stored data.

5. Customer login passwords shall never be transmitted from the Hosted Systems. Users may reset their passwords via a two-step authorisation token within a limited time allowance only.

6. Customer's must not have VPN access to the Hosted Networks. Customer's can only access the public facing services provided by the Hosted Systems.

7. Hosted Systems may be shared amongst multiple customers, but must segregate data, security, and access as follows:
    a. Customer data must only reside within a database dedicated to that one customer. At no time shall a database store data on behalf of multiple customers.
    b. Each customer database must have a different system administrator account and password.
    c. Each customer system must have a different service account and password.
    d. On-Premise systems (at customer premises) which send data to the Hosted Systems must do so over encrypted connections, and must provide IP-specific firewall rules to protect against DNS spoofing and other hacking techniques.
    e. Customer authentication tokens and content must be stored on their dedicated web site within the Hosted System. At no time shall a single web site support more than a single customer.
    f. Database systems must be designed to protect against SQL Injection attacks.

8. Account details (excluding customer login details) pertinent to the Hosted Systems must be stored in the approved account management package, in a security group which accessible to System Administrators and Management only.

9. Customer data shall not be accessed by staff without express authorisation from the customer. Customer data must only be accessed for the purpose of diagnostics, validation, or at the explicit written request of the customer. Customer data must not be saved, exported, sent, or otherwise transferred to any individual, person, or entity without express written permission from an authorised and verified representative of the customer.

10. Backups of customer systems and data must be performed regularly, automatically, and without manual intervention. Backups shall remain within the Hosted Networks but be located on separate physical servers to the Hosted Systems, and only be accessible by System Administrators in the event of a disaster recovery scenario.

11. Unless expressly authorised by a customer, the physical location of the Hosted Systems relevant to each customer must be within the local geographic region. For the purposes of clarity, all Australian and New Zealand customers shall have their systems and data deployed in data centres which are physically located in Australia.

12. Customer data must not be stored or transferred to an alternate geographic region without express and written authorisation from an authorised customer representative.

13. Data requests made to the Hosted Systems must protect against account spoofing by revalidating the user's access rights with every client request made to the servers.

The above strategy meets the security hardening principals of Isolate, Secure, & Protect as follows:

a) Physical access to the Hosted Systems is protected by the (outsourced) data centre security which provides physical access to servers only to authorised personnel, and only to the physical racks to which they are authorised to access.
b) Logical access to the Hosted Systems is protected by secure and encrypted remote VPN tunnels which are logically segregated from the Corporate Networks and other systems.
c) Electronic access to the Hosted Systems is protected by dedicated, fit-for-purpose firewalls with enterprise-grade security, as well as encryption, certificates, and user-specific logins.
d) User accounts are protected by never storing passwords on the Hosted Systems, and never transmitting passwords electronically other than during the encrypted login process. Authorisation tokens must expire after a nominated time requiring users to login again after an idle period of no interaction.
e) Customer data is protected via multiple layers as follows:
    a. Physical isolation
    b. Firewall protected security

c. Encrypted and secure communications
d. Isolated databases
e. Isolated web sites and services
f. Customer login details are never stored

The above strategies are reviewed periodically by the Operations Manager and Lead Solution Architect, and are to be updated as appropriate to provide continued data safety in a changing environment.

Access to Information

Access to information must be restricted to authorised users who have a *bona fide* business need to access the information. Customer requests for their own data will only be facilitate for validated and authorised customer personnel. The Leads are responsible for maintaining a list of authorised customer representatives on a project-by-project basis.

Confidentiality

Staff will have access to Sensitive Information about the company, its clients or their customers as appropriate for their role within the Company. Irrespective of whether this information has been classified and protectively marked, staff have a responsibility to maintain the confidentiality of this information.

Staff must not make Sensitive Information available to the public or other interested parties without explicit authorisation. Staff must be aware when information is subject to the 'need-to-know' principle and when customers have specific requirements that relate to their information and systems.

Staff shall be aware of their surroundings outside of the office. Staff must refrain from discussing Sensitive Information where they could be overhead in a public place and staff must ensure that sensitive documents (physical or on an electronic device) cannot be seen by others.
Staff must not upload or post Sensitive Information to a public site or arbitrary cloud services, including mailing lists, forums and social networks. Staff must ensure that Sensitive Information has been masked or removed.
Physical documents containing Sensitive Information must be locked in a drawer or filing cabinet, or destroyed as soon as they are no longer required.

Files and Documents

The Company maintains files and documentation in two primary locations: A file server within the Corporate Network, and on the Corporate Sharepoint / OneDrive. Files should only be pulled to local devices on an as-needed basis, and whenever works are complete, should be reset to reside on the host location only. Staff are reminded that unnecessary duplication of content significantly increases the risk of unauthorised access to such content.

Laptops and personal devices should have data encryption enabled to protect against data access due to theft or loss of the equipment.

Change Management Process

The change management process is underpinned by cloud-hosted SaaS software (currently ClickUp) which records all projects, development, tasks, assignments, labour investments, design details, and other proprietary information which is sensitive to the Company. In some cases, it contains customer information to track bugs, issues, incidents, and other data which allows the Company to better support their customers. Customer data should never be stored in the Change Management environment.

Version Control

The Company uses GitHub as the version control repository for its product development, and in some cases for version control of customer configurations (not data). As a policy, Company data within GitHub is private, available

only to authorised and licensed staff. The Git repository retains a history of all code changes across the entire life of our products, and is the master repository for the Company's intellectual property as it pertains to trade secrets, designs, methodologies, and strategic benefits. Staff are reminded that this information is commercially sensitive to the Company and cannot be shared with any other personnel or entities.

The Company maintains an automatic build-and-test landscape for its product development leveraging TeamCity. This is hosted within the Corporate Networks and is accessible only to trained and authorised staff members.

Cyber Security Incident Management

To date, the Company has never experienced a Cyber Security Incident. The safeguards documented herein are key to the security and protection of our own information, as well as our customers. Should an incident occur, it will be documented and tracked, including the response, follow-up, and modifications of provisions to prevent recurrence, in our Change Management register.

As soon as the incident is confirmed it will be handled by the Operations Manager and System Administrators whose response will be tailored to the individual circumstances of the incident.

Continued Intrusions

The Company will not allow an external intrusion to continue even for the purposes of scoping the incident. The legal risk to the Company, as well as the risk to our customers sensitive information, is such that it is not worthwhile. The Company will always act first to secure data and access to systems, and then assess and investigate the incident.

Notifiable Data Breaches

According to the provisions of the Australian Privacy Act 1988, under certain circumstances, where personal information is concerned, data breaches must be reported to both affected individuals and the Office of the Australian Information Commissioner (OAIC), and may need to be reported to other relevant authorities including financial services providers, law enforcement bodies, professional associations and regulatory bodies. The steps detailed below should be taken with respect to applicable data breaches. Such data breaches may occur as the result of malicious action, human error or a failure in information handling or security systems.

In the case of any cyber security incidents where the following eligible data breaches occur:

- A device, or paper record, containing individual's personal information is lost or stolen; OR
- A database containing personal information is accessed by malicious actors or persons not authorised to access the information; OR
- Personal information is mistakenly provided to the wrong person

the breach must be contained, assessed and reported if it is likely to cause harm to the person. Such harm is defined as including the risk of financial fraud, identity theft, personal harm or intimidation, and negative impacts to a person's reputation. Suspected data breaches should be assessed to see if there is potential for harm to any individuals as a result of the breach and whether such potential harm can be remediated. If possible, the lost information should be recovered before it can be accessed or changed. The affected person or organisation must be consulted and included in decisions concerning prevention of harmful consequences. If there are other possible steps that can be taken to make the possibility of serious harm no longer likely, then these should be undertaken and if risk of harm is deemed to have been addressed, then there is no need to report the breach. If serious harm cannot be prevented, then the breach should be reported to the OAIC. Following such a breach, the incident will be reviewed as for any other cyber security incident.

Inductions

The Company requires all new staff, including short-term contractors, to read this policy and familiarise themselves with their obligations and responsibilities with regards information security for both the Company and our

customers. The employee / contractor induction pack requires a signature to confirm that the staff have read the policy and will abide by its provisions.

As new information comes to light, it will be communicated to staff by the Operations Manager or Lead Solution Architect, and if appropriate, included in this policy as an updated revision.

This policy is available to all staff under the Policies and Guidelines folder on the Company's Sharepoint site.

PHYSICAL SECURITY

Network Access

All equipment connected to the Corporate Network must meet any applicable requirements. Equipment that is staff managed must be suitably configured and managed securely by the individual. All systems connected to the Corporate Network must have appropriate security software installed and be fully patched, subject to the requirements for a functional production service and any particular requirements of a client specific patching policy for a system.

Any equipment that is required to connect to a customer network must meet the authorisation requirements of both the Company and the customer.

Third Party Equipment

Customer and third-party equipment that is not managed by the Company or its staff must be authorised before connecting to the Corporate Network.

Visitor / Guest Access

Visitors must be restricted to approved 'guest' systems, including guest wireless networks and training computers. Any visitors who requires additional access to Company systems must read and accept this policy before access is authorised. Such access must be given on a principle of least-privilege.

Network Monitoring

All use of the Internet, including email and web, may be monitored.

Corporate Networks

The Company has both internal and external networks. The Guest network is an external network, which provides limited access to the internet and no access to the Company's internal systems. The Corporate Network provides access to the internal systems. The Corporate Network is accessed via direct physical cable or wirelessly when within the Company's premises, or remotely via VPN. Once on the internal network, authorised access can be gained via authenticated login to internal services such as file systems, build servers, and application servers.

Network Devices

Network devices and their configurations are described in the appropriate network documentation. Network devices are configured for security, and all default accounts must be changed or removed immediately upon installation.

Password Policy

The Company requires staff to adhere to the following rules in regards accounts and passwords:

1. The primary authentication mechanism to internal Corporate Networks and systems is via Active Directory login. Users are required to change their password periodically, and must not share their personal login account details with any person, including other staff or managers.

2. Passwords must never be written down, or stored in unencrypted files. Passwords should contain at least 12 characters, including at least one number and one symbol.

3. A number of internal systems are 'shared resources' to support teams who are collaborating and sharing development, build, database, and coding systems. Wherever possible, staff should access these systems using their personal Active Directory account. Where this is not possible, and it is not feasible to leverage individual accounts for every staff member, a shared, internal account is allowed to be used, with the provision that this account is destroyed as soon as the shared system access is no longer required.

4. Where staff access cloud-hosted services as part of their role in the Company (e.g. financial systems, GitHub, ClickUp, etc), these must be accessed using their company email account, and every system must have a different password from all others. Staff may leverage the approved password management software to help manage these accounts.

5. In the event that a staff member believes their account has been compromised, or their password become known to others, they must change their password at the first available opportunity, and notify the Operations Manager of the incident.

Non-Disclosure

The Company is a signatory to numerous non-disclosure agreements with various parties, including a number of its customers. Staff are signatories to the Company's NDA policy, and are reminded that all customer information should be considered confidential unless specifically identified as publicly available by the customer. Handling of sensitive information should follow these rules:

- Never be printed, unless absolutely necessary
- Physical copies securely disposed of as soon as they are no longer required
- Physical copies should only be transferred via registered post, and must include a return address
- Physical copies should not be left unattended and unsecured, even within the office environment
- Encrypted, if it is required to be stored anywhere other than on the Company's internal systems
- Encrypted, if it is to be transferred electronically
- Deleted (and purged) from external systems as soon as it is no longer required
- Never be shared with any unauthorised person

Staff are reminded that our duty of care recommends that we avoid transferring such information if at all possible.

System Security Protection

All devices that connect to Corporate Networks, Company Systems, Hosted Networks, Customer Systems, or which store Sensitive Information must have appropriate software protection installed and active, depending on the nature and role of the device. As a minimum this includes threat and virus protection, with regularly (daily) updates.

Staff must lock their devices when they leave their desk for any reason, and are recommended to shutdown their devices when leaving them for any extended period.

Backups

The Company employs a variety of information backup systems depending on the purpose, location, and type of system being managed. This includes:

- Virtual Machine backups
- Database backups
- File backups
- Manual backups
- Offsite backups for customers (under explicit support agreements)

All standard system backups for internal Company systems and components are retained within the Company's Corporate Networks in secure data centres as appropriate. Internal system backups are taken daily or weekly depending on the system in question. Offsite backups of these items are taken periodically to facilitate disaster recovery processes in the event of a catastrophic failure of the data centre. Offsite backups are stored with senior management in physical vaults on encrypted drives to ensure their security.

Backups of Hosted Systems which contain customer data are facilitated within the Hosted Networks, and must not leave the data centre unless expressly provisioned for in customer support agreements. Hosted System full backups are performed daily, and database backups performed incrementally throughout the day allowing recovery to within a small time-window as needed. Because of the system design, which allows for reprocessing of data from the originating on-premise source, generally even in the event of a full disaster recovery to the previous day's backup, there should be no loss of data on the in-production system for the customer.

Disaster Recovery processes are multiple and variant to cover the various systems, applications, and data, and are documented individually for each type of system covered by those processes.

Media Control

- Avoid using removable media (USB sticks) if at all possible.
- If using removable media, data should be encrypted.
- Removable media must be sanitised before they are re-purposed for use with another system.
- Removable media must be sanitised and securely disposed of at the end of their life.

Online Services and Acceptable Use

Online services include services which are used by the Company (e.g. video conferencing, file sharing), as well as services which are personal in nature (e.g. social media, personal email, etc). Staff are requested to keep personal use of online services to a minimum during work hours. The Company does not actively monitor staff's use of online services. It is expected that staff adhere to the policies concerning use of such services and inappropriate use will result in disciplinary action. Staff are made aware of the policies concerning use of these services, and disciplinary consequences for misuse, during induction and any subsequent information security awareness training.

If material is received by email, or downloaded from the Internet (intentionally or unintentionally) that is illegal in the local jurisdiction, this must be reported as a security incident as soon as reasonably practicable.

The provision of Internet access, including email functionality, is to support the Company's business activities. Staff should adhere to the following policies when accessing online services on Company devices, or when their device is connected to the Corporate Networks, Hosted Networks, or customer systems, and must behave in an ethical manner and in accordance with all applicable local laws at all times.

- When posting information under the Company's official social media accounts, or business profiles, staff must maintain professional, courteous, and factual content and responses in all circumstances
- Email services are provided by the Company for staff use in relation to their duties within the Company. Corporate email accounts should not be used for personal or social purposes.
- Emails which contain attachments should be treated with caution, and only accessed when the email and contents can be explicitly identified as valid from a known source. Staff are advised to never click on links or

attachments which are unexpected, from an unknown sender, or which appear suspicious in any way. Virus and threat protection software must be enabled for all emails and web access.
- Video conferencing services are provided by the Company for staff use in relation to their duties within the Company. Use of these services should not be used for personal or social purposes.

The following is a non-exhaustive list of activities that are expressly not permitted:
- Using email or other services to intentionally distribute spam or a virus;
- Accessing or publishing pornographic material;
- Accessing or publishing discriminatory material;
- Intentionally accessing websites that promote terrorism or discrimination (as determined by government laws and policies);
- Causing a breach of copyright terms by downloading or sharing copyrighted material such as DVDs of Hollywood films;
- Usage of Company equipment and systems for personal gain, for example mining bitcoins;
- Hacking into a website (Company internal, hosted external, or non-Company external) without permission;
- Publishing any views, opinions, statements of fact, or otherwise which do not pertain, or which are counter to, the Company's business interests.

External Services

Only those external services explicitly authorised and approved by the Company should be used by staff (e.g. file sharing must not use unauthorised file-drop services). The Company authorises use of services which have been assessed and considered secure for both the Company and its customers, and use of alternative services compromises the safety and security of the business.

Record Management

Electronic communications, including emails, with external customers/clients/partners/stakeholders should be kept and not be deleted. These should be archived within an appropriate shared mail folder on the server. This is to provide an audit trail of communication with customers and third-parties and compliance with appropriate legislation for record management.

Equipment

All Company managed or connected laptops must have firewall, virus, and threat protection software installed and enabled, with inbound exceptions only enabled for essential services. The equipment must be kept up-to-date and patched at both the operating system and application levels. Screen locks must be used by all staff whenever the device is left unattended, even for short periods of time.

Staff computers and laptops should be shut down at the end of the day, unless requested by a system administrator to leave it running. Most staff have laptops, which can be taken home if needed. Staff are responsible for the safety and security of any Company equipment which is removed from Company offices.

Staff should switch off all monitors at the end of the day both to save power, and to reduce equipment wear. The last person to leave should switch off the lights.

Equipment and / or components that reach end of life or replacement remain the property of the company and will be securely erased and destroyed.

Infrastructure

The Company uses some external infrastructure, especially cloud services and data centres, to host and manage client systems. This includes Microsoft Azure infrastructure. The setup and configuration of such infrastructure must be undertaken in such a way as to maximise security of the information contained therein. System-specific

requirements and documentation must be followed. Standard operating procedures for infrastructure should be updated regularly.

All infrastructure is managed by the system administrators. If you have any questions about infrastructure, speak to a system administrator.

Summary

The Start Group Pty Ltd takes a very proactive approach to managing information security across all aspects of the organisation. We believe in following best practice security guidelines in all aspects of the work we do. We believe that it is our duty of care to provide our staff and our clients with the most sensible, secure systems possible. Over fifteen years of operations, we have never experienced an information security breach, virus intrusion, nor any customer data loss. Strict adherence to our software design principles, engineering practices, and security policies will ensure we continue to deliver strong outcomes for our customers, and ourselves.