SponServe Group Pty Ltd

INFORMATION SECURITY POLICY

Information Security Policy

Table of Contents

Purpose

The purpose of this document is to ensure that appropriate measures are put in place to protect corporate information and the Information Technology Systems (ITS), services and equipment of the SponServe Group, and it's affiliates ("Company") and associated infrastructure.

The objectives of the Information Security Policy are:
• To secure the Company's assets against theft, fraud, malicious or accidental damage, breach of privacy or confidentiality; and
• To protect the company from damage or liability arising from the use of its ITS facilities for purposes contrary to policies of the Company.

Scope

This policy applies to all company staff and any other persons otherwise affiliated but not employed by the Company, who may utilise company ITS infrastructure and/or access company applications with respect to the security and privacy of information.

Definitions

Affiliates: Entities which sit within the SponServe Group of companies including but not limited to ServeRite Pty Ltd T/As SponServe, SponServe LTD and SponServe USA, Inc.
Application: A software package to perform a specific task (eg MS Word).
Backup: A means of making a duplicate copy of a system and / or data for the purpose of being able to restore a system should a failure or corruption occur.
Bluetooth: A short range (10 meters) personal wireless connection of compliant Devices.
Company: SponServe.

Computer Work Area: Is an area or office in which access to computer resources is made available.
DRP: Disaster Recovery Plan.
Incident: An occurrence of suspect or illegal activity.
Infrastructure: All components that make up the computing facilities of the Company.
ITS: Information Technology Systems.
LAN: Local Area Network.
Patch: Software updates intended to remove or reduce risks from known vulnerabilities.
PC: Personal Computer.
Portable Device: Any handheld, or smaller, device used to access Company systems or resources such as, but not limited to, iPhone, Smart phones, PDAs, iPad, mobile phones, laptop or notebook computers and the like.
SOE: Standard Operating Environment.
Users: Those who utilise the computing facilities of the Company.
User ID: Login details assigned to a user to enable them to use the ICT facilities.
Virus: A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
VPN: Virtual Private Network.
WAN: Wide Area Network.
Wireless: Computer devices that connect using radio signals rather than cables.

Policy Statement

The Information Security Policy determines how the ITS and infrastructure should be used in accordance with ITS industry standards and to comply with strict audit requirements.

The Company seeks to comply with the requirements of Australian Standard Information Technology: AÃ Code of Practice for Information Security Management. AS/NZS ISO/IEC 27001:2006.

Following are broad requirements of the overall Information Security Policy.

This Policy includes:

- Staff Security
- Acceptable Usage
- Logical Security
- Data Security
- Physical Security
- Mobile / Portable and Hand Held Devices
- Security Incident Management
- Business Continuity
- Breaches / Infringements

Staff Security

Specify what is expected from staff, both permanent and contracted, as information security is the responsibility of all who utilise the information technology services.

Staff Access
The Company provides staff with access to computing and communications services in support of its operational activities. These facilities include among other things access to email, Internet, file and print services.

Users are responsible for maintaining the use and security of their assigned User IDs and all activity associated with that ID. Knowingly disclosing passwords to others will be deemed a breach of policy and could be referred to disciplinary procedures.

The Company expects its staff and associates to take all reasonable steps to ensure the integrity and security of the Company's ITS and data.

HR Responsibilities
It is the responsibility of the Company to ensure correct termination dates are recorded for staff terminations. After a fixed number of days from the date of termination, the staff account will be disabled.

Following a further pre-determined number of days, the account will be deleted.

There are however, situations where an account may need to be disabled immediately and this can only be performed with the authorisation from the Managing Director or delegated officer.

Contract / Temporary Access
Where temporary access is required for a specific purpose such as, but not restricted to, contract workers and 'test' accounts, a user expiry date based on the completion date of the required tasks must be used to ensure the temporary account is not accessible after that date.

In the case of ongoing maintenance and support from 3rd party companies, access must only be granted to the relevant facilities within the system and be restricted to only the systems for which they provide support.

Reliance on People
All specialised computing staff are required to ensure that all systems and procedures are well documented and that there are others who can act in a backup capacity as required.

Executives and Managers
It is the responsibility of company executives and managers to be familiar with Information Security Policies and their requirements.

Acceptable Usage

Identification of what is deemed acceptable (or unacceptable) usage of network, communication and Internet Services.

Network Usage
The Company provides staff with access to computing and communications services in support of its operational activities.

By signing the appropriate forms for obtaining access to the Company's computing facilities, users agree to abide by all policies that relate specifically to the use of these facilities. Any breach of these policies will be

deemed an infringement and dealt with accordingly which could result in suspension of access privileges or in severe cases, legal authorities may be involved.

Interfering, in any way, with the Company network or associated equipment, be it intentional or accidental, is not permitted. Any such interference will be acted upon and may result in removal from the Company network until an investigation can be completed and the source of the interference is removed.

Electronic Communications
The Company encourages staff to appropriately use electronic communication in order to achieve the mission and goals of the Company. The Company encourages the use of electronic communication to share information, to improve communication and to exchange ideas.

The electronic communications services must not be used for the distribution of material that may be deemed offensive, discriminatory or defamatory or the publishing or advertising of personal events or activities.

All usage must comply with the company employment policies.

Internet Usage
The Company encourages staff to use the internet in order to further the strategic and operational objectives of the Company.

Inappropriate usage of Internet facilities includes, but is not restricted to, accessing or posting of discriminatory, defamatory, offensive material or material that may create or promulgate a negative impression of the Company.

Any staff required, as part of their job function, to access information on the Internet that may be deemed inappropriate, must obtain written authorisation from the Managing Director.

Mobile Devices
Mobiles devices including, but not limited to, laptop and netbook computers, mobile phones, smart phones and tablet devices, are all subject to the same policies and procedures as for other computing and communication Devices.

In addition, any Company supplied mobile devices must be configured with a password or pin code in order to access the device. Preferably, a password or phrase should be used, but at a minimum, a four (4) digit PIN code is acceptable. This becomes essential if corporate data and/or email is held or accessed from the device.

Logical Security

Implementing a suitable environment that protects the integrity, availability and confidentiality of Company data by using logical or 'computerised' controls and processes.

Software Security
Software security specifically relates to access rights and protection of software packages supplied by, and for the use by, Company computer services infrastructure. All users of the network are supplied with a User Account for authentication and allocation of appropriate access rights to network facilities including software.

Access to such network facilities and software is also controlled by the use of secure passwords should be changed on a regular basis.

All Company staff PCs and laptops must be set with an inactivity screensaver which requires a unique password to reactivate the underlying session and has an idle time of no more than 10 minutes before activation.

As a means of allocating appropriate software packages to specific users, the use of an application deployment tool should be used. This can grant individuals or groups access to various programs and services in accordance to their duties and requirements through their user account.

Software Development

Software development must only be performed in a controlled, test environment until such time that all flaws, bugs and potential vulnerabilities are removed. Only then can the developed software be applied to a production environment.

Development team must be familiar with and adhere to the internal data access and data movement policies.

Passwords

It is essential that those requiring access to the Company computing facilities be issued with a unique login and password. This password is not to be shared with, or used by, any other individual and failing to comply will be treated as a serious breach of system security which may result in disciplinary action.

Staff Passwords are to meet complexity rules as set by the Identity and Access Management System. These complexity rules will include a minimum password length, character requirements and suitable password expiry Period.

In the event that access is required to Company data that is held under a specific staff members user id and password and that staff member is unavailable to access the data due to unforeseen circumstances, a request to have the password reset may be made with the authorisation of the Managing Director or delegated officer.

This will only be considered when all other avenues to access the data have been exhausted. At the completion of the task accessing the required data, the password MUST be reset again and the staff member notified as soon as is practical.

Patch Management

To ensure that all Company supplied desktop operating systems and applications are kept current and up-to-date, all machines will have windows update turned on and mandatory updates applied as required, at a minimum weekly, and Virus Protection subscriptions are to be set to automatically update and renew.

Data Security

Ensuring that the confidentiality of data contained on the information technology systems is maintained and access is made available to those who are authorised to see that data. This item should also be used in conjunction with confidentiality policies.

Confidential Data Security

To ensure the confidentiality and security of staff and client personal information contained on the Company ITS facilities, it is essential that only those authorised to access such data are permitted to do so. Those who are permitted to access such information are granted appropriate access, as required by their job functions. Anyone who gains access to such personal information through methods other than those granted

by the Company, shall be deemed as unauthorised and subject to disciplinary action.

Staff should be aware of their legal and corporate responsibilities in relation to appropriate use, sharing or releasing of information to another party. Any other party receiving restricted information must be authorised to do so and that the receivers of the data also adopt information security measures to ensure the safety and integrity of the data.

Physical Security
Ensure that any physical ITS devices are kept safe from inappropriate access. This includes the physical access to devices in both restricted and public access areas.

Physical Security

All offices, computer rooms and work areas containing confidential information, or access to confidential information must be physically protected. This means that during working hours, the area must be supervised, so that the information is not left unattended, and after hours, the area must be locked or the information locked away.

It is a requirement that any PC / Laptop / Portable computer be logged out and turned off at the end of the working day unless a specific request is made to leave equipment turned on for the purpose of distribution of overnight processing is required.

Building Access
The following controls must be applied to restrict building access:
a. Access to computer work areas must be restricted by keys, cipher locks or proximity access cards during office hours and can only be accessible by authorised individuals after hours.
b. Combinations or access details must be changed / deleted when a staff member leaves or loses their card or key.
c. If door and keys have been used for other purposes, key cylinders must be replaced with a brand new lock and keys restricted to an absolute minimal number of persons.
d. Access to restricted computer work areas can only be given when an authorised staff member is inside and can and will supervise the visitor's movements completely or hand over to successive staff.
e. When unattended and after hours, doors must be secured.
f. Individual computer labs must be protected by timed door locks and also video surveillance.

Removal of Equipment
No computer equipment can be removed from Company premises unless specific authorisation has been received from an appropriate authority. This does not apply to laptop or notebook computers where one of their primary purposes is to allow the custodian to work while away from their normal working Location.

Any equipment taken from company premises without appropriate authorisation will be in direct violation of this policy and appropriate misconduct and / or legal action will be taken.

Security Incident Management

Reporting Security Problems
Any suspected inappropriate or illegal usage of Company systems and equipment should be reported to the Managing Director immediately. This information will then investigated by the Managing Director.

Emergency Plans
Disaster Recovery Plans, Business Continuity Plans, backup strategies and fail over plans for the core Company ITS and infrastructure are the responsibility of the ITS to ensure that any outages or disasters can be recovered from in the shortest possible time with a minimal amount of data or resource loss.

These documents must include step-by-step instructions for the restoration of each service to ensure that, if required, other personnel from the ITS Services are able to perform the recovery. These documents also form part of the Company Business Continuity Plan.

Escalation
The escalation process for the rating of each reported event will be determined by the relevant staff member in conjunction with the Chief Technology Officer, taking into account the event itself and other priorities at that time.

Monitoring and Reporting
Staff nominated by the Managing Director will be authorised to monitor all aspects of the Company network and associated infrastructure. They are also able to report any suspected inappropriate and / or illegal activity to the Managing Director in the first instance for further investigation in accordance with incident investigation procedures.

It is also the role of the Chief Technology Officer to actively monitor and analyse all network related activity included, but not restricted to, Internet Usage, email and dissemination and use of programs and data across the Company network infrastructure.

This monitoring will be done for the sole purpose of identifying and responding to any suspected inappropriate Activity.

"The content of e-mail and other electronic communications will only be accessed by the Chief Technology Officer-
1. after approval has been obtained from the Managing Director or delegated officer; and
2. if the access is permitted by law."

All information reported to the Chief Technology Officer shall be treated in the strictest confidence. Any reported information will be logged and relevant action taken, including reporting to relevant School or Section heads and other management as required.

Business Continuity

How to ensure that there will be minimal disruption to ITS services in the event of a disaster or the implementation of changes to systems and/or associated infrastructure.

Backup Requirements
All major systems within the Company computing infrastructure are backed up on a regular basis. Information Technology Services have a Backup Strategy which details the frequency of backups. It is also strongly advised
that all users save their work to their network drive as this drive is backed up and any loss or damage to files can
often be rectified by the restoration of the files from an existing backup.

Change Control
To ensure that the ITS facilities and services running within the Company infrastructure are maintained and kept running at maximum performance and functionality, it is often a requirement to perform maintenance and upgrades to equipment. To ensure that there is minimal disruption to essential services, appropriate Change Control procedures are to be followed. This is to ensure that the disruption is kept to a minimum and appropriate roll back procedures exist should there be issues during the system changes.

Disaster Recovery Plans
In the event of a disaster that impacts the ITS infrastructure and / or services, the implementation of a Disaster Recovery Plan is essential. The DRP provides step by step procedures and processes required to ensure that services are returned to normal operation in the shortest possible time. The production and maintenance of such plans are the responsibility of the various ITS staff assigned to any aspect of the network and ITS services.

Breaches / Infringements

Failure to abide by these terms will be treated as misconduct.

Minor Infringements
For a first time offence of a minor infringement, a warning will be issued. A second time offence will result in automatic denial of access to one or all facilities for a period of three (3) working days and up to two (2) weeks.

Serious Infringements
A serious infringement includes, but is not limited to, a third and subsequent offence of a minor infringement and will result in automatic denial of access to one or all facilities and will be referred to the Managing Director. This may result in:

- A prolonged denial of access to one or all facilities;
- Referral to the appropriate disciplinary procedures; and/or
- Referral to law enforcement agencies (where the infringement constitutes a legal offence).

Responsibility

The Managing Director of the company is responsible for the review and implementation of this policy and the maintenance of all associated documents.

Implementation

The “Information Security” Policy is to be implemented by the company via:
1. an ITS announcement to all the company staff;
2. an announcement on the company website;
3. inclusion in the Company's policy library.