SECURITY POLICY

# INTRODUCTION

The policy applies to all staff, contractors, and visitors using digital technology and Internet services provided by .

The transmission of information across networks and the Internet increases the company’s risk of exposure to accidental, or deliberate, unauthorised modification or disclosure. Adherence to this policy will ensure that our Information Systems (IS) are developed, operated, used and maintained in a safe and secure manner.

## Purpose

The purpose of this policy is to:

* Ensure that all staff are aware of computer security policies for maintaining a secure operating environment.
* Define acceptable and unacceptable use for staff using information systems and services.
* Define for staff the responsibilities they have for maintaining security when using and accessing information systems.

## Definition of Terms

|  |  |
| --- | --- |
| **IS Assets** | IS assets include but are not limited to: equipment such as laptop/desktop computers, servers, printers and peripheral devices that connect or have access to network. This also includes hand held devices like mobiles, tablets, and smart phones. IS assets also include all software, whether packaged, or custom built. IT media includes but is not limited to; USB keys, portable data drives, backup tapes and CD/DVDs. |
| **Restricted Information** | Restricted information is any data that is extremely sensitive and could cause extremedamage to the integrity, image or effective operation of . Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship and major economic impact. |

# POLICIES

## ACCEPTABLE USE POLICY

### ACCEPTABLE USE

The types of activities that staff, contractors and visitors are encouraged to participate in and considered acceptable practice when using IS systems include:

* Research on the Internet related to develop professional skills related to one’s position at .
* Acquiring or sharing information necessary or related to the performance of an individual’s assigned responsibilities.
* Reasonable use of computing facilities for personal correspondence, e.g. sending personal emails, and using Internet web sites so long as it does not interfere with productivity or consume sustained high volume traffic.

### UNACCEPTABLE USE

The types of activities that are considered unacceptable practice include:

* Use of digital technology and Internet services for illegal or unlawful purposes. This includes, but is not limited to: intentional copyright infringements, software license infringements, obscenity, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation and computer tampering (e.g. spreading computer viruses or destruction of data owned by others).
* Intentionally using digital technology and Internet services to visit Internet sites or receive information that contains obscene, pornographic, hateful or other objectionable material.
* Attempting to gain access to any computer system, information, or resources without the authorisation of the relevant owner.
* Knowingly or recklessly transmit or distribute any information or material which contains a virus, worm, Trojan Horse, or any other harmful component.
* Posting, publishing, transmitting, or distributing any unsolicited advertising through mass electronic- mail or other direct transmission.
* Using digital technology and Internet services to reveal or publicise restricted or propriety information which includes, but is not limited to: financial information, new product ideas, intellectual property, strategies and plans, databases and the information contained therein, staff details, product information, computer software and code, computer network and access details and business relationships.
* Internet use of a nature that consumes bandwidth at an unacceptable rate is specifically prohibited when there is no clear educational use. Examples include: illegal downloading of music, video or software; playing games online.

All use must comply with all applicable laws which include but is not limited to: the Privacy Act 1993, the Fair Trading Act 1986, the Copyright Act 1994, the Defamation Act 1992 and the Films, Videos, and Publications Classification Act 1993, the Unsolicited Electronic Messages Act 2007 as well as any advertising codes of practice which may be relevant.

### UNACCEPTABLE ACTIONS

Prompt action will be taken to deal with unacceptable actions by individuals or groups of people that infringe this policy or which undermine the integrity or performance of the network. This may include; suspension from using the Internet or removal of the service and removal of access to all digital technology.

ACCESS CONTROL POLICY

This defines the security practices that control access to information and computer systems at . The following apply:

* Only staff and authorised visitors are allowed to access and use IS services.
* User accounts are to be created and managed by , this includes:
	+ The creation and deletion of all user accounts.
	+ Periodic auditing of accounts to verify account status.
	+ Deleting accounts that have been disabled for a period longer than 6 months unless specifically authorised to remain disabled.
* IS accounts can be immediately disabled at the request of .

## PASSWORD MANAGEMENT POLICY

The following apply:

* Passwords must be kept confidential and are the responsibility of the individual. They are not to be shared or used by anyone else, even for a short period of time.
* Password construction must comply with the following minimum standards:
	+ All passwords at are required to be a minimum length of 8 characters, or for systems that do not allow 8 characters passwords, the highest level for that system.
	+ Password construction must include a combination of uppercase, lowercase, numbers and symbols where possible, and not contain a complete word including a person or company’s name.
	+ Passwords will be changed every 90 days.
	+ Login attempts will be restricted on all IS services after 5 unsuccessful login attempts; account will remain locked until unlocked by .
	+ When passwords are first issued users will be required to change their password on first use.
* Screen saver passwords will be enforced after a period of 15 minutes of no activity requiring the password to be re-entered.

## REMOTE ACCESS POLICY

Remote access to IS Services is provided for staff to work from home and access services remotely, for example remote access to email. The following apply:

* Remote access is only permitted through approved IS services; contact the for guidance on the remote access services available.
* Remote access can also be provided to contractors when approved by the and subject to the approval.

## APPLICATION AND SOFTWARE POLICY

This defines the security practices when developing, integrating or installing new software and what needs to be considered during the acquisition or evaluation of new software. The following apply:

* Only approved software is to be installed on devices. Advice on approved software is available from the IS. Non-approved software that is installed will not be supported by IS staff, and may be removed.
* All software must be licensed for use by and used only within the terms of that licensing.
* All shareware software must be licensed to .
* No software is to be installed when there are insufficient licenses available.
* are to register and manage all website domain addresses and website certificates on behalf of .

## ASSET AND MANAGEMENT POLICY

This defines the security practices to protect IS assets. The following apply:

* IS hardware issued by to staff remains the property of .
* IS are authorised to install and configure software and make configuration changes to IS services. This includes returning IS equipment back to its original build status to rectify faults and remove unlicensed software.
* Purchasing of IS hardware or software is to be made with the approval of the or nominated representative and coordinated by .
* The is to be advised of any software or hardware provided at no charge to .
* All IS assets are required to be recorded and identified with a unique asset number. This number is to remain visible and only are permitted to remove the asset identifier.
* All IS hardware and media are to be returned to IS when no longer required or staff terminate their association with .
* In the event of any IS hardware being lost, accidentally damaged or stolen the incident is to be reported to the immediately.
* All IS media (for example: disks, USB keys, portable drives) that contains restricted material are to be stored overnight in a locked cabinet, locked draw/room or a fireproof safe.
* When transporting restricted information on IS media, which includes laptop devices, it must be encrypted to reduce the risk of data being compromised in the event of the IS media being misplaced or stolen. will assist with encrypting IS media and the information stored on these devices.
* Only IS are authorised to dispose of IS equipment.

## COMMUNICATIONS AND OPERATIONS POLICY

This defines the security practices for the delivery of IS services and access to communication services including the Internet and email.

### ICT OPERATIONS POLICY

The following apply:

* All changes to IS services are to follow the Change Management procedures and .
* are authorised to monitor and complete security audits to assess the performance of IS services and detect potential or actual malicious intrusion.
* IS are authorised to update IS systems to maintain the operational security of IS services. IS are to coordinate specific periods to undertake systems patch in consultation with the but it is recognised that at times patches will need to be installed during operational periods to safeguard the integrity and available of IS services.
* IS are required to perform and maintain an organisational backup schedule to provide the level of protection against data loss/corruption required by .
* IS are responsible for testing the backup and system restoration processes to ensure the recovery times required by can be met.

### EMAIL ACCESS AND COMMUNICATIONS POLICY

The following apply:

* Email messages within the bounds of email service are the property of .
* The permanent re-directing of emails to a private email account (for example, Yahoo, Hotmail or Gmail), rather than using remote access to email is unacceptable practice.
* Email access will be terminated when the employee or third party terminates their association with , unless an extension has been agreed by the .
* Email is not to be used for unsolicited mass mailings, political campaigning, dissemination of chain letters, and use by non-employees sending chain emails, malicious data (viruses), solicitation emails or any offensive material.
* Email accounts are provided for employees’ sole use, it is not appropriate to send, reply or modify another employee’s email account without the delegated authority from the account owner or .
* Confidential or restricted email messages are not to be sent outside of without authority of the originator or owner of the information contained within the email. Permission is required, from the originator of the message, to forward attachments that contain restricted or confidential material.

### INTERNET ACCESS AND COMMUNICATIONS POLICY

The following apply:

* Access to the Internet and browsing websites is to comply with the Acceptable Use Policy defined in this document.
* allows limited personal use of the Internet so long as it does not interfere with staff productivity, consume sustained high volume traffic or hinder others in their use of the Internet.
* Employees must not transmit confidential institution information or information that is classified as restricted through the Internet unless the information is encrypted to reduce the risk of data being compromised. The can advise of secure methods than can be used to transmit information across the Internet.
* The has the right to block Internet sites that do not comply with the Acceptable Use Policy.

### SOCIAL MEDIA POLICY

The following apply;

* Using Social Media (like Facebook and Twitter) to discuss, promote or comment on business activities or express an opinion on staff, customers or the organisation is prohibited unless the use of social media is related to one’s position at and approval has been gained from .
* Personal use of social media is to comply with the Acceptable Use Policy.
* IS staff are authorised to monitor and complete reviews on social media activity.

## PHYSICAL AND ENVIRONMENTAL POLICY

This defines the security practices to protect IS facilities and equipment from environmental changes, accidental damage or theft. The following apply:

* Access to IS facilities is restricted to authorised individuals whose job responsibilities require access.
* Visitors requiring access to IS facilities are required to complete a visitors’ log recording arrival time, departure time, purpose of visit and who authorised visit. The visitors log is to remain within the IS facility.
* IS facilities are to be protected against environmental changes in power, cooling and flooding.
* All removable media (for example: disks, USB keys, portable drives) much be scanned and approved by IS before being connected to ‘s network or devices (like laptops, computers, etc).

## HUMAN RESOURCES POLICY

### INDUCTION & TERMINATION POLICY

This defines the security practices during employment: from recruitment, on-going training to termination of employment. The following apply:

* Staff are required to complete an IS induction before receiving access to IS services. The IS induction will explain: the Acceptable Use Policy and Security Policy; confidentiality and privacy regulations, what constitutes a security incident and the incident management process.
* IS Staff who are responsible for the administration of restricted IS services or complete IS security audits are to sign a confidentiality agreement.
* Staff must report a security incident (either suspected or confirmed) to IS and follow the incident management process.
* Upon termination of an employee’s contract at , all accounts will be disabled on the last day of employment and IS will complete an account end of employment process to close down access to IS systems and services. An extension can be requested by the for the account to remain open for a set period of time.
* Individual IS staff, who are formally authorised, are permitted to search, collect and report on IS activity for the purposes of a specific security audit or investigation.
* Investigations on IS activity are to be instigated through the . No investigations are permitted without authority from the .
* Misuse, non-compliance or undertaking of prohibitive activities may be regarded as a serious offence and disciplinary action may follow. Depending on the nature of the misconduct, this may result in the removal of access to IS services or dismissal from .

### THIRD PARTIES

* Third parties engaged to provide IS services at are to be bound by a Third Party Support Agreement that includes a service level agreement.
* All IS third parties are to acknowledge and accept the *Security Policy* before commencing work at .
* IS are responsible for completing third party support agreement reviews every 6 months to ensure validity of the agreement and that contractual obligations are being met.
* Misuse, non-compliance or undertaking of prohibitive activities may be regarded as a serious offence and disciplinary action may follow. Depending on the nature of the misconduct, this may result in the removal of access to IS services or termination of contract.