




Acceptable Use Policy

DOCUMENT AUTHORISATION

RESPONSIBLE OFFICER:		MANAGER OF ADMINISTRATION AND HUMAN RESOURCES			
REVIEWED BY:		MANEX			
REVIEW DUE DATE:		December 2025			
VERSION NUMBER:		1			
DOCUMENT NUMBER:		NA			
VERSIONS:	DATE:	RESOLUTION NO:	DESCRIPTION OF AMENDMENTS:	AUTHOR / EDITOR:	APPROVED / ADOPTED BY:
1	15/12/2022	7.12/22	New Policy.	MAHR	Council



 General Manager (Interim)

22.12.22

 Date

ACKNOWLEDGEMENT OF COUNTRY

Glen Innes Severn Council acknowledges and pays respect to the Ngoorabul people as the traditional custodians of this land, their elders past, present and emerging and to Torres Strait Islander people and all First Nations people.

PURPOSE

The purpose of this policy is to ensure that all computer systems and networks owned or managed by **Glen Innes Severn Council (GISC)** are operated in an effective, safe, ethical and lawful manner and it is the responsibility of every computer user to know these requirements and to comply with them.

APPLICABILITY

This policy applies to all employees, councillors, delegates, volunteers and contractors who use or operate GISC's computer systems and networks.

OUTCOMES

- A security and acceptable use framework is in place for GISC as an organisation;
- GISC's assets are protected;
- There is a uniform level of control and guidelines for management;
- A single ICT security message is provided for all users; and
- Users are aware of what the ICT security and acceptable use controls and guidelines are.

ROLES AND RESPONSIBILITIES

The General Manager has overall responsibility for the implementation of the Acceptable Use Policy and Council's ICT Strategic Plan.

Employees who use a Council owned or managed computer or mobile device must know the requirements set out in Council's Acceptable Use Policy and other relevant policies and procedures and comply with such requirements.

Employees are responsible for using mobile devices and communication systems owned or managed by Council in an effective, safe, ethical and lawful manner, and are responsible for reporting cyber incidents if they occur.

Managers are responsible for monitoring computer and mobile device usage within their respective areas of control and reporting anomalous use, and reporting cyber incidents if they occur.

The Chief Financial Officer is responsible for reviewing and approving, in conjunction with the relevant Director and Manager of Administration and Human Resources, requests for online business channels or online financial services provided via the Internet.

The Manager of Administration and Human Resources is responsible for:

- approving and recording remote access requests and connection methods;
- approving the storage of personally identifiable information on USB devices and other portable storage devices;
- approving the connection of personally owned communication devices to Council's computer systems or networks;
- approving requests for port scanning or security scanning;
- approving the installation or use of non-standard software;
- receiving and acting on disclosures of email spamming or other illegal email actions, security breaches or system malfunctions.
- approving requests for group or generic User IDs and passwords;
- reviewing and updating the Acceptable Use Policy; and
- any other specific ICT issue that requires approval under Council's policies.

DEFINITIONS

Cyber Incident	A breach of a system's security policy in order to affect its integrity or availability and / or the unauthorised access or attempted access to a system or systems.
Encryption	The process of converting information or data into a code, especially to prevent unauthorised access.
Endpoint	An endpoint refers to a device or node that connects to a LAN or WAN and accepts communications back and forth across the network. Examples include computer workstations, modems, routers and switches.
Information and Communications Technology (ICT)	ICT comprises the technologies that enable modern computing, and generally includes all devices, networking components, applications and systems that allow people and organisations to interact in the digital world. It includes the Internet, mobile networks, wired and wireless networks, telephones, radio and television services, Artificial Intelligence (AI), robotics, Internet of Things (IoT) devices and other technologies, and the use and application of such devices.
Internet	A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.
Local Area Network (LAN)	A collection of devices connected in one physical location, such as a building, office, or home, typically via Ethernet or Wi-Fi.

Malware	The collective name for malicious software developed by cyber-attackers, including viruses, ransomware and spyware, which can cause extensive damage to data and systems or be used to gain unauthorised access to a network.
Multi-factor Authentication (MFA)	Multi-factor authentication (MFA) is a security measure that requires two or more proofs of identity to grant user access. Typically, this would be a password and mobile phone.
Phishing Attack	A type of social engineering attack involving the sending of fraudulent communications, usually via email, that appear to come from a reputable source, usually with the intention of stealing user data.
Privileged Access	Access to a system (on-premise or cloud) which is above the benchmark of a regular user. Privileged access accounts have access to system critical resources and therefore need to be protected and monitored.

POLICY STATEMENT

Access Control

- 1.1 Users are only permitted to access information, applications and systems that they have been allocated access rights for. Rights are granted on the basis of business need and documented such that it defines the rules and rights for individuals or groups. Any other access is considered unauthorised and is in breach of this requirement.
- 1.2 Mobile phones, tablets, portable computers, laptops, USB devices or any other device must not be connected to GISC's internal computer systems or networks unless the device has been approved for use by the Manager of Administration and Human Resources.

Users should not access systems that contain personally identifiable information (PII) from mobile devices or save any PII information onto USB devices etc. unless approval has been given by the Manager of Administration and Human Resources.

- 1.3 Damaging, altering, or disrupting the operations of the computer systems and networks owned or managed by GISC is not permitted. Users must not carry out any activity with the intention of capturing or obtaining passwords, encryption keys, or anything that could facilitate unauthorised access by themselves or anyone else.
-

- 1.4 Before a user reaches a menu, system prompt or has access to system resources, utilities, databases or shares they must have successfully logged on and be validated as a legitimate system user. Authentication methods will depend on the sensitivity of the information or system being accessed, whether access is effected in-house or remotely and the level of privileges granted to the user.

Anti-Virus

- 2.1 Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise affect the performance of, or access to any GISC computer system or network.
- 2.2 Users must not open files or click on links in attachments, emails or social media if the source is unknown, suspicious or untrustworthy.

Communication and Mobile Devices

- 3.1 Mobile devices and communication systems supplied by the Council are provided to facilitate business activities. Reasonable and appropriate personal use is permitted as follows:
 - Minimal calls and text messages;
 - The data plan must not be exceeded due to personal use; and
 - Personal use must not cause the Council to incur any additional costs or impact staff productivity.

Managers may monitor use. Personal use may be required to be reimbursed.

A phone supplied by GISC may not be used in connection with any personal commercial business activities. The number may not be published in any publication or business card that is not related to the Council's business.

- 3.2 Mobile devices and communication systems owned or managed by GISC are to be used in an effective, safe, ethical and lawful manner. Use will be monitored and misuse will be handled in accordance with existing disciplinary procedures.
 - 3.3 Users of GISC's mobile phones and communication systems must not engage in any activity which violates or infringes the rights of others or which a reasonable person would consider to be abusive, profane, offensive or defamatory.
 - 3.4 Communications equipment supplied by GISC must not be altered or added to in any way including:
 - unauthorised upgrades;
 - addition of components;
 - removal of components - including transferring a Council SIM card to a personal phone;
 - altering configuration or security settings;
 - installation of non-approved applications; or
 - jailbreaking the device.
-

All devices will be centrally managed and any changes or maintenance carried out by the IT Helpdesk or designated agent.

- 3.5** Users of mobile devices must ensure that the device is protected by a PIN number or password and auto-lock. Voice authentication (if used) must be coupled with password or PIN authentication.
- 3.6** GISC maintains the right to conduct inspections of any mobile phone or other mobile device that it owns or manages without prior notice to the user or custodian. The device must be returned to the IT Helpdesk upon request for maintenance and when the user ceases to provide services to GISC.
- 3.7** Users should not lend mobile devices allocated to them for business activities to others external to the Council including friends and family.
- 3.8** Staff using communications devices must not return calls, text messages, respond to pager calls or subscribe to paid services where:
- the return number is a premium rate number;
 - charges beyond those for normal calls can be incurred (e.g. long distance calls);
 - the recipient is a competition, gambling or advertising entity; or
 - charges will be reversed back to the Council.

Any costs incurred relating to the above will be the responsibility of the staff member.

- 3.9** With the exception of purchases made from an approved online application store (e.g. Apple's App Store or Google's Play Store), games, freeware, shareware, movie clips or music may not be downloaded onto any Council mobile device unless its use is legal (does not breach copyright law) and it is specifically required for business purposes. Movie clips taken with the device for work purposes are exempt from this requirement.
- 3.10** Personally owned communication devices may not be connected to or synchronised with GISC's computer systems or networks unless approved by the Manager of Administration and Human Resources and the device owner agrees to the security requirements regarding the management of the device. BYOD security requirements include:
- agreement that the device will be managed by GISC; and
 - agreement for the Council security profile to be applied to the device.
- 3.11** The use of voice and video communication accounts must be approved. Voice and video systems are not to be used for any of the following:
- personal voice calling, video calling and instant messaging;
 - commercial announcements;
 - advertising material;
 - sexually explicit or sexually oriented material;
 - hate based material;
 - hacker related material; or
 - transferring of files.
-

All inbound and outbound communication must be channelled through corporate systems and accounts.

Computer Systems and Equipment Use

- 4.1** Users of computer systems or networks owned or managed by GISC shall not use these systems to engage in any activity which causes, or could be construed as causing, any form of harassment, discrimination or victimisation of another user including:
- race;
 - religious belief or activity;
 - sex;
 - age;
 - disability;
 - industrial association;
 - lawful sexual activity/sexual orientation;
 - marital, parental or carer status;
 - physical features;
 - political beliefs or activity;
 - pregnancy and maternity;
 - personal association with a person who has one of these personal characteristics;
 - gender; or
 - irrelevant criminal conviction.
- 4.2** The computer systems and networks owned or managed by GISC are to be used in an effective, safe, ethical and lawful manner. Misuse of IT resources will be handled in accordance with existing disciplinary procedures.
- 4.3** The computer systems are to be used for business purposes in the course of normal day to day operations. Personal use must be reasonable and appropriate and not impact on staff productivity, system performance or bring GISC into disrepute.
- 4.4** Users must not connect personally owned computing devices, computer peripherals, USB devices, digital cameras etc. to computer systems or networks owned or managed by the Council. If users do bring personal equipment to work, this is at their own risk and the Council is not responsible for the device or anything stored on it.
- 4.5** USB sticks or key fobs allocated by GISC are only for business use. Extra care is required when storing information on these devices due to their size and portability. Users should be aware of the following:
- Loss of the keys and the data is a problem due to the small size of these devices;
 - Increased chance of introducing a virus as they can be used on multiple devices;
 - Confidential information should not be copied to or stored on a USB storage device;
-

- USBs should not be plugged into any computer that does not have up to date security patches and anti-virus software;
- They must be stored and transported in a safe manner to reduce the chances of theft or loss; and
- USBs containing personally identifiable information (PII) should be protected by means of encryption.

4.6 Computer equipment supplied by GISC must not be altered or added to in any way including:

- unauthorised upgrades;
- addition of components;
- removal of components;
- altering configuration or security settings; or
- installation of non-approved applications.

All changes to configuration or maintenance of the device must be carried out by the IT Helpdesk or their designated agent.

4.7 Users must not lend computers, portable devices, tablets, mobile phones, laptops or any other equipment that has been allocated to them by the Council for business activities to anyone external to the Council including friends and family.

4.8 Any actions or activities, whether intended or accidental, which cause or could cause the computer systems, information or networks of the Council to be compromised in any way is considered serious misconduct, including:

- Security breaches or disruptions of network communications. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes;
 - Port scanning or security scanning. These activities are expressly prohibited unless sanctioned by the Manager of Administration and Human Resources for the purposes of testing network security;
 - Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal duties or has been duly authorised;
 - Circumventing user authentication or security of any host, network or account or running password cracking programs;
 - Interfering with or denying service to any user other than the employee's host (for example, denial of service attack);
 - Using any program/script/command, or sending messages of any kind, with the intent of interfering with or disabling a user's session using any means either locally or externally;
 - Downloading, installing or executing any file containing malware which may damage or compromise computer systems or data;
 - Copying or altering configuration or system files for unauthorised personal use or to provide to other people or users for unauthorised use;
 - Creating or using open mail relays maliciously, spoofing mail headers, initiating a mail bomb attack or otherwise interfering with the Council's or another organisation's email service;
-

- Downloading or introducing tools or utilities that may potentially be used for hacking activities and undertaking any such activity on any system whether owned or managed by the Council or not;
- Providing or selling Council information without approval and for personal gain; or
- Defacing websites, downloading and distributing pornography, running a gambling operation or undertaking any other activity using Council resources that would bring the Council into disrepute.

4.9 Users must use the standard applications for which GISC is licensed. Do not install any software program, application, script or executable code on equipment in your care. Only software approved by the Manager of Administration and Human Resources may be installed on computer equipment owned by GISC and all installations must be carried out by the IT Helpdesk.

4.10 Users working in the Council's premises are not permitted to connect to the internet using mobile broadband cards, pairing hotspots, external modems, wireless USB, or any other mechanisms that bypass official corporate systems.

Devices provided by GISC have been configured to connect to network resources (including the internet) using approved wired or wireless mechanisms. Use of mobile computing facilities (e.g. mobile broadband cards, wireless USBs or pairing hotspots) may be used when working remotely.

4.11 If printing confidential or potentially sensitive information the following must be observed:

- The person authorised to view the information must be present at the printer during printing to ensure no one else reads the document; or
- The printer is located in a secure area; or
- The document is printed to a storage area on the printer and a code entered or card swiped to initiate the print when the authorised person is present.

The same applies to scanners, fax machines and photocopiers.

Email

5.1 The email system is predominantly for business use. Personal use must be reasonable and appropriate and not impact on staff productivity, system performance or bring GISC into disrepute. Misuse will be handled in accordance with existing GISC disciplinary procedures.

5.2 The email system must not be used for any unlawful activity and must not be used to compromise the security or operation of any computer system or network whether it is owned or managed by GISC or not.

5.3 Users must not create, send or forward any email messages which contravene human rights legislation, and which may be considered discriminatory, defamatory, or intend harassment or hatred on the basis of:

- Race;
- Religious Belief or Activity;
- Sex;
- Age;
- Disability;
- Industrial Association;
- Lawful Sexual Activity/Sexual Orientation;
- Marital, Parental or Carer Status;
- Physical Features;
- Political Beliefs or Activity;
- Pregnancy;
- Personal Association with a person who has one of these personal characteristics;
- Gender; or
- Irrelevant criminal conviction.

Any of the above actions will be handled in accordance with existing disciplinary procedures.

- 5.4** The email system is regarded as an official means of communication and, as such, messages must conform to the same corporate rules for grammar and content as other business communications.

It is not appropriate to use abbreviations (as used in text messages) or profanities, obscenities, derogatory or sexually explicit remarks in business email messages. Such remarks, even when made as a joke, may upset some people. Special caution is warranted because backup and archival copies of email may be more permanent and more readily accessed than traditional paper communications.

- 5.5** GISC has a legal requirement to retain corporate email. Users must regularly move corporate emails from email folders to **TechnologyOne CI Anywhere (ECM)**. Corporate email is defined as:

- E-mail that forms part of the corporate record. It is e-mail that documents the business activities of the Council, e.g. a direction for an important course of action, business correspondence received from outside the Council or a communication between staff members in which a formal approval is recorded.

Ephemeral emails can be destroyed as part of normal administrative practice. Ephemeral email is defined as:

- E-mail used to facilitate the Council's business, but which does not need to be retained for business purposes, e.g., notice of meetings, staff movements, copies of reports or newsletters, advertising material and any other publicly available material.

Personal email should be destroyed as soon as it is no longer required. Personal email is defined as:

- E-mail of a personal nature that has no relevance to the business of the Council.
-

- 5.6** Files received from an unknown, suspicious or untrustworthy source must be deleted immediately without opening. Under no circumstances should users click on links contained within an email message sent from an unknown source.

Information Management

- 6.1** Data and information created, modified, saved, transmitted or archived using the corporate systems of GISC remains the property of the Council.
- 6.2** All corporate information and data must be stored in approved corporate information repositories. This includes ECM, corporate applications and other approved shared repositories. Information is not to be stored on local drives of PCs or workstations, USB devices, laptops or copied onto portable media such as CDs or DVDs unless these copies are made in addition to saving it in an approved corporate file system.
- 6.3** Electronic information must be protected based on its sensitivity, value and criticality regardless of the type of media that holds the information, its location, the systems used to process it or the processes it is subjected to. Staff should be trained to recognise unclassified information, especially when it personally identifies individuals.
- 6.4** The user must notify their Manager immediately if confidential or sensitive information is lost, disclosed to unauthorised parties, or is suspected of being lost or disclosed.
- 6.5** Users must not delete or dispose of potentially important Council electronic records or information without the approval of the information owner and without following standard document management procedures for disposing of information.

Deleting the Council's records without following the proper procedures is considered a serious breach of this requirement particularly if the records cannot be recovered. Such actions will be handled by Human Resources in accordance with existing disciplinary procedures.

It should be noted that document retention should be in accordance with the NSW State Records Act 1998.

Internet Use

- 7.1** The internet is primarily available for business use. Personal use must be reasonable and appropriate, not impact on staff productivity or system performance or bring GISC into disrepute. A web content control system monitors and controls website visits.
- 7.2** GISC monitors and logs web sites visited, files downloaded and social networking accounts controlled by the Council. Managers can request reports that allow them to monitor and moderate Internet use. Users viewing or downloading content that is deemed inappropriate for the workplace may be subject to disciplinary actions up to and including dismissal.
-

7.3 Users of the internet are not permitted to visit, interact with, or download content from websites that are offensive, obscene or contain indecent material such as pornography or violence. Users must not access, publish or download material which promotes hatred or discrimination on the basis of:

- Race;
- religious belief or activity;
- sex;
- age;
- disability;
- industrial association;
- lawful sexual activity/sexual orientation;
- marital, parental or Carer status;
- physical features;
- political beliefs or activity;
- pregnancy;
- personal association with a person who has one of these personal characteristics;
- gender; or
- irrelevant criminal conviction.

The above activities should be reported to your Manager or Human Resources. All reports will be investigated and handled in accordance with existing disciplinary procedures.

7.4 The internet connection must not be used for any illegal or unethical activity or personal business activity and must not be used to compromise the security of any computer system or network whether owned or managed by GISC or not.

Misuse must be reported to a Manager or Human Resources immediately. Reports of misuse will be investigated and handled in accordance with existing disciplinary procedures. Examples of unacceptable internet use include:

- computer hacking (accessing another's electronic data or computer without permission);
 - providing access to unauthorised persons (including minors);
 - impersonation;
 - file downloads (except for work related reasons);
 - use of the Internet for personal gain;
 - gaming, wagering or betting;
 - playing games;
 - the intentional transmission in any way of viruses or files that cause a negative impact on computer systems (e.g. unauthorised email attachments such as video, audio and executable files);
 - downloading or distributing information subject to copyright requirements (such as licensed software or protected internet applications);
 - disclosing private or confidential information including passwords or other information that may compromise the security of the computer systems; or
 - engaging in any illegal activity, including dissemination of material in breach of legislation.
-

- 7.5 Peer to peer file sharing is not permitted. This requirement includes sharing or downloading of movies, music, ebooks, applications, games etc. using torrent sharing, torrent clients and file sharing connections.
- 7.6 When working on their desktop within the Council's premises, users must use the Internet connection provided from this equipment. Users must not circumvent Internet security by using USB modems, personal hotspots, USB mobile wireless devices and mobile broadband cards. These alternative methods of connecting to the internet will be allocated to users working remotely and the Manager of Administration and Human Resources will record all instances where alternative methods of connecting to the internet have been provided.
- 7.7 The Internet shall not be accessed from another employee's PC, unless the user is logged on with their own username and password. Administrative and privileged access accounts must not be used when accessing any website or email system.
- 7.8 Personal use of social media sites is permitted using Council equipment during the employee's own time. This use must be reasonable, appropriate, not impact on staff productivity, system performance or bring GISC into disrepute. Social media sites include:
- Social media and news sites, for example, Facebook and Twitter;
 - Video and photo sharing sites such as YouTube and Instagram; or
 - Collaborative information sites like Wikipedia.

Access to manage or publish to social media on behalf of the Council is only permitted with the approval of a Manager. Participation in work related social media groups, chat groups, list servers or collaborative sites must be conducted in accordance with the Policies and any applicable guidelines.

- 7.9 Users must not use social media to cause annoyance or anxiety, to harass, to defame or to transmit unsolicited commercial or advertising material. These actions must be reported to Human Resources and will be handled in accordance with existing disciplinary procedures.
- 7.10 Employees are not permitted to create or maintain a blog, wiki or social networking site on behalf of the Council without the express permission of the General Manager. Any blog, wiki or shared workspace must have a moderator and an approved code of conduct.

Legal Compliance

- 8.1 Users must not disclose any confidential information belonging to the Council or otherwise coming into their possession during the course of their employment, except as expressly permitted under any of the Council's Policies or as required by law. Users may be required to sign a confidentiality or non-disclosure agreement. Information may be classified as follows:
-

- Not to be Stored - Information which may not be captured or saved in electronic systems;
 - Confidential - Information restricted to a small number of people;
 - Internal Use Only - Information which may be known by staff, but not by anyone external to the Council; and
 - Public - Information that is approved for public dissemination.
- 8.2** All intellectual property (including patents, copyrights, trademarks, inventions, designs or other intellectual property) created and/or developed by the Council's employees while at work or while using the Council's equipment is the exclusive property of the Council and must be recorded in a register.
- 8.3** Third party software in the possession of GISC must not be copied or installed multiple times unless this is allowed by the licence agreement. In all other cases the number of installations should be equal to the number of licences held. Systems will be monitored to ensure software licence conditions are being complied with and licence numbers are not being exceeded.
- 8.4** Information held in all computer systems and networks owned or managed by GISC is subject to the provisions of Privacy legislation and users should be aware of their obligations in respect of managing and using the information and providing information to third parties.

Online Services

- 9.1** When using the Council's computer systems, or when conducting the Council's business, staff must not deliberately misrepresent themselves and, where possible, provide full contact details.
- 9.2** Unless approval has been obtained in advance from the Chief Financial Officer and Director, users are prohibited from establishing online business to business arrangements or signing up to online services provided via the Internet.
- Where the online system involves payments or receipts, a secure platform for processing transactions must be approved. Examples include electronic purchasing, personnel management systems, on-line database services, drop box, iCloud, Skype etc. Requests for a new online business channel or online service should be made through the Chief Financial Officer and Director.
- 9.3** Users must not publish corporate information (applications, internal documents or files, press releases, price lists etc.) on any public facing computer system (e.g. website, social media site) unless the item has been authorised by the appropriate Manager for public consumption.
- 9.4** Financial transactions transacted online must comply with legal requirements, be within approved limits of delegated authority for expenditure and meet the requirements of the Council's financial auditors.
-

Password and Authentication

- 10.1** User IDs and passwords must not be disclosed to anyone or shared with anyone.

Group or generic User IDs and passwords are prohibited as a rule, but in special circumstances may be approved by the Manager of Administration and Human Resources who will keep a written record of the exceptions.

- 10.2** Passwords must not be written down and left in a place where unauthorised persons might discover them.
- 10.3** Staff that use a computer at home should use different login credentials for work and home.
- 10.4** Users are responsible for all activity performed with their personal user IDs and passwords. Users must not allow others to perform any activity with their user IDs and are not permitted to perform any activity with IDs belonging to other users.

Personnel Management

- 11.1** All breaches of IT Policies and procedures will be handled by Human Resources in accordance with GISC's disciplinary procedures. If the action is inadvertent or accidental, is not unlawful and does not affect GISC's financial position or reputation or that of any other organisation or individual, a first breach may result in a formal warning.

The offender will be provided with training to ensure that the error does not occur again. Subsequent breaches, including those considered willful or intentional will be considered serious misconduct and will be subject to internal disciplinary actions that may include termination of employment and/or legal proceedings.

- 11.2** Staff must avoid actual or potential conflicts of interest in their capacity as an employee and conducting business on behalf of the Council and if there is any doubt about a particular situation, they should consult their Manager.

Remote Access

- 12.1** Remote users are only permitted to access applications and systems they have been approved to access for the purposes of fulfilling obligations to GISC. All other access is unauthorised. No access is permitted unless the following documentation has been completed:

Internal Users

- The Acceptable Use Policy is signed; and
- The Staff Remote Access Request Form is completed.

External Users

- The Application for Remote Access is completed; and
 - The Remote Access Agreement has been signed.
-

- 12.2** Users must not be remotely connected to GISC while concurrently connected to another network or initiate a connection to another network during the period they are connected to the Council. This practice is called split tunneling.
- 12.3** The Council reserves the right to monitor and audit the use of remote access connections. Logs containing details of user activities may be retained.

LEGISLATION AND SUPPORTING DOCUMENTS

Relevant Legislation, Regulations and Industry Standards include:

- *Essential Eight Maturity Model – Australian Cyber Security Centre;*
- *ISO 27002: Information security – Security Techniques – Code of Practice for Information Security Controls;*
- *Local Government Act 1993;*
- *Privacy and Personal Information Protection Act 1998;*
- *Health Records and Information Privacy Act 2002;*
- *Independent Commission Against Corruption Act 1988;*
- *Government Information (Public Access) Act 2009;*
- *State Records Act 1998;*
- *Workplace Surveillance Act 2005;*
- *Anti-Discrimination Act 1977; and*
- *Local Government (State) Award 2020.*

Relevant Council Policies and Procedures include:

- *Glen Innes Severn Council Disaster Recovery Plan;*
- *Glen Innes Severn Council Data Breach Readiness Solution;*
- *Glen Innes Severn Council Internal Penetration Test Report – July 2020;*
- *Glen Innes Severn Council Data Risk Assessment Report – April 2021;*
- *Glen Innes Severn Council Code of Conduct for Council Staff;*
- *Glen Innes Severn Council Code of Conduct for Councillors;*
- *GISC Unsatisfactory Performance / Disciplinary Procedures Policy;*
- *GISC Workplace Discrimination and Bullying / Harassment Policy;*
- *Glen Innes Severn Council Risk Management Policy;*
- *Glen Innes Severn Council Procurement Policy;*
- *Glen Innes Severn Council Social Media Policy;*
- *Glen Innes Severn Council Business Continuity Plan; and*
- *Glen Innes Severn Council ICT Policies and Procedures:*
 - *Glen Innes Severn Council Access Control Policy;*
 - *Glen Innes Severn Council Anti-Virus Policy;*
 - *Glen Innes Severn Council Business Continuity / Disaster Recovery Policy;*
 - *Glen Innes Severn Council Communication and Mobile Devices Policy;*
 - *Glen Innes Severn Council Computer Systems and Equipment Use Policy;*
 - *Glen Innes Severn Council Computers for Councillors Policy;*
 - *Glen Innes Severn Council Cyber Crime and Security Incident Policy;*
 - *Glen Innes Severn Council Email Policy;*
 - *Glen Innes Severn Council Information Management Policy;*
 - *Glen Innes Severn Council Internet Use Policy;*

- *Glen Innes Severn Council Laptop and Tablet Security Policy;*
- *Glen Innes Severn Council Legal Compliance Policy;*
- *Glen Innes Severn Council Online Services Policy;*
- *Glen Innes Severn Council Password and Authentication Policy;*
- *Glen Innes Severn Council Personnel Management Policy;*
- *Glen Innes Severn Council Physical Access Policy; and*
- *Glen Innes Severn Council Remote Access Policy.*

VARIATION AND REVIEW

The Acceptable Use Policy will be reviewed every three (3) years, or earlier if deemed necessary, to ensure that it meets the requirements of legislation and the needs of Council. The term of the Policy does not expire on the review date, but will continue in force until superseded, rescinded or varied either by legislation or a new resolution of Council.

Appendix A



Employee Acceptance

I have read, understood, and agree to abide by the Glen Innes Severn Council **Acceptable Use Policy**.

I acknowledge that any inappropriate use of the Council's computer facilities may be investigated and may be subject to disciplinary action, including termination of my employment and/or any civil or criminal legal action.

I agree that my use of these services and facilities will be in strict accordance with Council's Acceptable Use Policy and acknowledge that:

1. I have been given notice in accordance with Section 10 of the *Workplace Surveillance Act 2005 (NSW)*;
2. My use of Council's computer services and communication devices may be subject to monitoring or surveillance by Council, using software and / or hardware intended for this purpose;
3. Such surveillance may be carried out on a continuous and ongoing basis;
4. Surveillance will commence on my date of employment with Council or from the date I sign this agreement, whichever is earlier; and
5. Monitoring and surveillance will be in accordance with Council's Acceptable Use Policy.

Signature: _____ Date: _____

Name of Employee: _____

Department: _____

Please **return this signed page** to Human Resources and **retain the policy** for your reference.
