Blackall-Tambo Regional Council

Information Technology Security Policy

Policy Number: Stra 14	Effective Date: 20.04.2022
Version Number: Two	Review Date: 20.04.2024
Policy Compiled by: Information Technology Officer	
Policy Approved by: CEO / Internal Audit and Risk Committee	

PURPOSE OF THE POLICY

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets.

SCOPE

This policy applies to all employees, councillors, contractors, consultants, and other personnel at the Council, including those workers affiliated with third parties who access the Council's computer networks. Throughout this policy, the word "employee" is hereafter used to collectively refer to all such individuals. The policy applies to all computer and data communication systems owned by or operated on behalf of the Council.

GENERAL POLICY

All information traveling over the Council's computer network is treated as a corporate asset unless specifically identified as property of a third party. The Council prohibits unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of Council information. The Council shall also protect third party corporate confidential information and non-public personal information in the same manner as Council information.

RESPONSIBILITIES

An Information Systems Security Committee comprised of the Chief Executive Officer, Director of Finance, Corporate & Community Services, Manager of Finance, and the IT Officer will meet at regular intervals to discuss the following matters.

a) periodically review the status of the Council's computer and network security
b) as needed, review and monitor remedial work related to computer and network security incidents

c) authorize and later evaluate the results of major projects dealing with computer and network security
d) approve new or modified information security policies, standards, guidelines, and procedures, and
e) perform other high-level information security management activities.
f) regularly consider the most cost effective and efficient arrangements for maintaining the necessary level of IT security into the future.
g) consider and approve all IT equipment purchases more than $5,000.

The IT Officer is responsible for establishing, maintaining, implementing, and administering organization wide information systems security policies, standards, guidelines, and procedures. The IT Officer is also responsible for activities related to this policy. While responsibility for information systems security on a day-to-day basis is every employee's responsibility, specific guidance, direction, and authority for information systems security is centralized for all the Council by means of the IT Department. Accordingly, the IT Department will perform information systems risk assessments, prepare information systems security action plans, evaluate information security products, and perform other activities necessary to assure a secure information systems environment.

The Chief Executive Officer can authorise the IT Officer to conduct investigations into any alleged computer or network security compromises, incidents, or problems. All security compromises or potential security compromises must be reported to the Chief Executive Officer, Director of Finance, Corporate and Community Services and the IT Officer.

The System Administrator (IT Officer) is responsible for acting as the information systems security coordinator. The IT Officer is responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems administered. The IT Officer is also responsible for reporting all suspicious computer and network-security-related activities to the Chief Executive Officer and the Director of Finance, Corporate and Community Services. The administrator also serves as local information security liaisons, implementing the requirements of this and other information systems security policies, standards, guidelines, and procedures.

The IT Officer will issue circulars to all employees advising of the security procedures they are required to follow. Users are responsible for complying with this and all other Council policies defining computer and network security measures.

PROCEDURES

PHYSICAL SECURITY

For all servers and other network assets, the area must be secured with adequate ventilation and appropriate access through digital lock.

It will be the responsibility of the IT Officer to ensure that this requirement is always followed. Any employee becoming aware of a breach to this security requirement is obliged to notify the DFCCS and/or the MOF immediately who in turn will advise the IT Officer.

All security and safety of all portable technology, such as notepads, tablets, mobile phones etc. will be the responsibility of the employee who has been issued with the notepads, mobile phones etc. Each employee is required to use passwords, patterns, or pins and to ensure the asset is always kept safely to protect the security of the asset issued to them.

In the event of loss or damage, the Chief Executive Officer may assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

SYSTEM ACCESS CONTROL

END-USER PASSWORDS

Users must choose passwords which are difficult-to-guess. This means that passwords must NOT be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used. Where such systems software facilities are available, users must be prevented from selecting easily guessed passwords.

Users can choose easily remembered passwords that are at the same time difficult for unauthorized parties to guess if they:

a) string several words together (the resulting passwords are also known as "passphrases"),
b) Must have at least one capital letter, one number and be at least eight characters long,
c) recommendation is to use symbols in place of common letters or numbers,
d) create acronyms from words in a song, a poem, or another known sequence of words,

Users must not construct passwords that are identical or like passwords they have previously employed. Where systems software facilities are available, users must be prevented from reusing previous passwords.

Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them.

Passwords must not be written down and left in a place where unauthorized persons might discover them. Aside from initial password assignment and password reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized user, the password must be immediately changed.

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the disclosed password. If users need to share passwords, the user should use LastPass' Share Site Capabilities, this option allows for the site to be shared without exposing the password. The Share Site capability is also easily auditable by the systems administrator. This policy does not prevent the use of default passwords--typically used for new user-ID assignment or password reset situations--which are then immediately changed when the user next logs-onto the involved system.

All passwords must be immediately changed if they are suspected of being disclosed or known to have been disclosed to anyone besides the authorized user.

PASSWORD SYSTEM SET-UP

All computers permanently or intermittently connected to the Council's networks must have password access controls. Multi-user systems must employ user-IDs and passwords unique to each user, as well as user privilege restriction mechanisms. Network-connected single-user systems must employ hardware or software mechanisms that control system access and that includes a no-activity lock screen.

Computer and communication system access control must be achieved via passwords that are unique to each individual user. Access control to files, applications, databases, computers, networks, and other system resources via shared passwords (also called "group passwords") is prohibited.

Wherever systems software permits, the display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

Wherever systems software permits, the initial passwords issued to a new user by the IT Officer must be valid only for the new user's first on-line session. At that time, the user must be forced to choose another password. This same process applies to the resetting of passwords if a user forgets a password.

All vendor-supplied default passwords must be changed before any device (desktop, notebook, tablet, or smart phone) is used for the Council business. This policy applies to passwords associated with end-user user-IDs, as well as passwords associated with systems administrator and other privileged user-IDs.

To make guessing more difficult, passwords must also be at least seven characters long. To ensure that a compromised password is not misused on a long-term basis, passwords must also be changed every 28 days or at more frequent intervals and cannot be used more than once a year. In addition, where systems software permits, the number of consecutive attempts to enter an incorrect password must be limited. After three (3) unsuccessful attempts to enter a password, the involved user- ID must be either suspended until reset by a system administrator, or temporarily disabled for no less than sixty (60) minutes.

Whenever system security has been compromised, or even if there is a convincing reason to believe that it has been compromised, the involved system administrator must immediately:

a) reassign all relevant passwords, and
b) force every password on the involved system to be changed at the time of the next log-in.

Whenever system security has been compromised, or even if there is a convincing reason to believe that it has been compromised, a trusted version of the operating system and all security-related software must be reloaded from trusted storage media or iso. The involved system(s) must then be rebooted. Similarly, all changes to user privileges taking effect since the time of suspected system compromise must be immediately reviewed by the systems administrator for unauthorized modifications.

MULTI-FACTOR AUTHENTICATION AND THE USE OF MICROSOFT AUTHENTICATOR

All Users will need to set up and use Multi-Factor Authentication (MFA) for all initial (first time login) domain and remote Microsoft 365 use. Multi-factor authentication is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their mobile phones or a fingerprint scan. The use of password only to authenticate a user, leaves an insecure vector for attack. If the password is weak or has been exposed elsewhere, an attacker could be using it to gain access. When you require a second form of authentication, security is increased because this additional factor is not something that is easy for an attacker to obtain or duplicate.

The Council will be recommending the use of Microsoft Authenticator App (MAA), the app is available on all Mobile Devices (Android, IOS, Windows). This app provides an extra layer of protection when you sign in, once enabled for your Microsoft accounts, the user will receive a notification from the app after trying to sign in. The user will have to tap to approve the login, for any other account, or if user is offline, MAA has a built-in security code generator.

LOG-IN/LOG-OFF PROCESS

All users must be positively identified prior to being able to use any multi-user computer. Positive identification for internal Council networks involves both a user-ID and a fixed password, both of which are unique to an individual user.

Positive identification for Remote Desktop involves the use of user-ID and fixed password, or other approved user authentication techniques.

Positive identification for users originating external real-time connections to the Council's systems or networks via public networks (like Internet), or any other external communications system must also involve user authentication techniques.

The log-in process for network-connected the Council's computer systems must simply ask the user to log-in, providing prompts as needed. Specific information about the organization, the computer

operating system, the network configuration, or other internal matters must not be provided until a user has successfully provided both a valid user-ID and a valid password.

If there has been no activity on a desktop, notebook, or tablet for a certain period, the system must automatically return to lock screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password. The recommended period is fifteen (15 minutes). An exception to this policy will be made in those cases where the immediate area surrounding a system is physically secured.

SYSTEM PRIVLEGES

LIMITING SYSTEM ACCESS

The computer system privileges of all users, systems, and independently operating programs (such as "agents") must be restricted based on the job function or need-to-know. This means that privileges must not be extended unless a legitimate business-oriented need for such privileges exists.

Default user file permissions must not automatically allow anyone on the system to read, write, or execute a file. Although users may reset permissions on a file-by-file basis, such permissive default file permissions are prohibited. Nonetheless, default file permissions granted to limited groups of people who have a bona fide need-to-know are allowed.

The Council's computer and communications systems must restrict access to the computers that users can reach over the Council's networks. These restrictions can be implemented via routers, gateways, and other network components. These restrictions must be used to, for example, control "passthrough"--where a user logging-into a certain computer then moves from that computer on to another.

PROCESS FOR GRANTING SYSTEM PRIVILEGES

Requests for new user-IDs and changed privileges must be in writing and approved by the user's manager before a system administrator fulfils these requests. To help establish accountability for events on the related systems, documents (in electronic form) reflecting these requests must be retained for a period of at least a year.

Individuals who are not the Council's employees must not be granted a user-ID or be given privileges to use the Council's computers or communications systems unless the advance written approval of a Director or Chief Executive Officer has first been obtained.

Privileges granted to users who are not Council employees may be granted for a maximum period of 30-days. As needed, users who are not Council employees must have their privileges reauthorized by the sponsoring department head every 30 days.

Third party vendors must NOT be given Remote Desktop access to the Council's computers and/or networks unless the system administrator determines there is a bona fide need. These privileges must be enabled only for the period required to accomplish the approved tasks (such as remote maintenance). If a perpetual or long-term connection is required, then the connection must be established by approved extended user authentication methods (VPN).

All users wishing to use the Council's internal networks, or multi-user systems that are connected to the Council's internal networks, must sign the Accepted Use Policy prior to being issued a user-ID.

PROCESS FOR REVOKING SYSTEM ACCESS

All user-IDs must automatically have the associated privileges revoked after employment termination. Management must promptly report all significant changes in worker duties or employment status to the system administrator responsible for user-IDs associated with the involved persons. For all terminations, the Human Resources Officer must issue a notice of status change to the system administrator who will process the change on the system on which the involved worker has a user-ID.

ESTABLISHMENT OF ACCESS PATHS

Changes to the Council's internal networks include loading new software, changing network addresses, reconfiguring routers, and the like. Except for emergency situations, all changes to the Council's computer networks must be:

a) documented in a work order request, and
b) approved in advance by the Chief Executive Officer. Emergency changes to the Council's networks must be approved by the Chief Executive Officer or in his/her absence by the Deputy Chief Executive Officer in consultation with the IT Officer. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to "employees" as defined in the Scope section of this policy, but also to vendor personnel.

All Council computers that intermittently or continuously connect to an internal or external network must employ password-based access controls. Multi-user computers must employ software which restricts access to the files of each user, which logs the activities of each user, and which has special privileges granted to a systems administrator. Single-user systems must employ access control software that includes user-ID/password control and an automatic lock screen that is invoked after a certain period of no keyboard (or other input device) activity. Portable computers and home computers which contain the Council's information are also covered by this policy, as are network devices such as gateways, routers, and bridges.

To stop unauthorized system access and related problems, all inter-processor commands from non-Council locations are prohibited unless a user or process has first properly logged in. An example of such commands is remotely initiated requests for a list of users currently logged in.

NFORMATION SECURITY

All relevant data to be backed up is either hosted on the servers as sensitive, valuable, or critical business data and all other data is on Office 365 (One Drive and SharePoint). The Council does not back-up desktops, notebooks, or tablets; users must use Microsoft OneDrive or SharePoint to save all data. Users should not save any data (documents, spreadsheets etc.), to the local drive of their device (desktop, notebook, or tablet).

It is the responsibility of the IT Officer to ensure that data back-ups are performed automatically every 4 hours and is kept in Microsoft Azure Storage blobs. This is accomplished using Veeam BaaS (backup as a service). The Veeam BaaS uses 3-2-1 methodology for backups of all data.

All technology that has internet access must have the ECS+ Secure software suite installed. This suite encompasses SentinelOne and ConnectWise security operations centre. It is the responsibility of the IT Officer to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

The IT Officer is to backup both the Practical Plus financial data year to date and the warehouse of MAGIQ files every Friday onto a HDD. The Manager of Finance will collect the HDD Saturday morning from the office and store it off-site. The four HDDs purchased for backup will rotate on a weekly basis always ensuring these records can be recovered.

All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements. Any employee breaching this will be referred to their director.

TECHNOLOGY ACCESS

Every employee will be issued with a unique user login to access the business technology and will be required to set a password for access every 30 days.

Each password is to be at least eight characters long which includes the use of at least one capital letter and one number and is not to be shared with any employee within the business.

The IT Officer is responsible for the issuing of the unique user login and initial password for all employees.

Where an employee forgets the password then the IT Officer is authorised to reset the password. The employee will be required to be changed the temporary password when the employee logs in after reset.

The following table provides the authorisation of access:

Technology – Hardware/ Software	Roles authorised for access
Microsoft365/Active Directory	IT Officer
PCS+	IT Officer and Finance Manager

POLICY REVIEW

This policy will be reviewed when any of the following occur:

a) As required by legislation

b) Other circumstances as determined by the Chief Executive Officer

Notwithstanding the above, this policy is to be reviewed at intervals of no more than two (2) years.

VERSION CONTROL

Version 1	New Document 21-04-21

RECORDS

When completed and approved, the original signed hard copy of the policy is filed in the Master File. Electronic copies are saved in the appropriately labelled folder in MAGIQ.