INFORMATION SECURITY POLICY

Adopted Date: 16 November 2010

Policy Number: GRC 0046

Policy Type: Administrative

Responsible Officer: Director Community and Corporate Services

Department: Community and Corporate Services

Version	Decision Number or CEO Approval	Decision Date	History
1	**GRC 0046**	**16 November 2010**	**Adopted**
2	**Amended**	**14 August 2012**	**Review August 2013**
3	**Reviewed**	**January 2014**	**Review January 2015**
4	**Reviewed**	**August 2015**	**Review August 2018**
5	**Amended**	**September 2018**	**Review October 2019**
6	**Amended**	**November 2019**	**Review October 2020**
7	**Reviewed**	**October 2020**	**Review October 2023**

1. BACKGROUND

The purpose of the information security policy is:

- To establish a Council-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of Council's data, applications, networks, computer and process control systems.
- To define mechanisms that protect the reputation of the Goondiwindi Regional Council and allows Council to satisfy its legal and ethical responsibilities with regard to its networks and computer systems connectivity to worldwide networks.
- To provide controls that protect the access and availability of Goondiwindi Regional Council's computer networks, business systems and process control systems.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

2. POLICY STATEMENT

2.1 Principles Used to Determine the Policy.

Council has an obligation to safeguard its information assets and assure the continued delivery of its services

2.2 Application of the Policy.

The Information Security Policy applies to all users of Goondiwindi Regional Council's information systems and networked process control systems.

Each Directorate within Council should apply this policy to meet their information security needs.

By information security, we mean protection of Council's data, applications, networks, computer systems and process control systems from unauthorised access, alteration, or destruction.

2.3 Strong Password

A Strong Password must conform to all of the following:

- The password must contain at least one (1) UPPER CASE letter;
- The password must contain a least one (1) LOWER CASE letter;
- The password must contain at least one (1) NUMERIC digit ie (1, ,2,3,4,5,6,7,8,9,0);
- The password must be at least Twelve (12) characters long;
- The password must contain a mix of alphanumeric characters; and
- The password cannot be changed to any of previous passwords.

2.4 Provisions

The following provisions apply:

2.4.1 Throughout the document the terms must and should are used carefully. Musts are not negotiable; should are goals for the Council. The terms data and information are used interchangeably in the document.

2.4.2 The terms system and network administrator are used in this document. These terms are generic and pertain to any person who performs those duties, no just those with that title or primary job duty. There are many staff members who are the system administrators for their own equipment e.g. laptops

The Policy is written to incorporate current technological advances. The level of technology installed on some systems may limit immediate compliance with the Policy. Instances of non-compliance must be reviewed and approved by the Information Technology & Communications Manager in consultation with the relevant Director, as appropriate.

The Information Technology & Communications Manager is responsible for implementing the policy and must see that:

2.4.3 The Information Security Policy is updated on a regular basis and published as appropriate.

2.4.4 Appropriate training is provided to data owners, data custodians, network and system administrators and end users.

2.4.5 The Information Technology & Communications Manager in consultation with the relevant Director, as appropriate, appoints a person to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, for example, information about virus infections risks.

2.4.6 The Council will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the Council's data, network resources, system resources and process control resources.

2.4.7 Security reviews of servers, firewalls, routers, monitoring platforms, SCADA systems and process control systems must be conducted on a regular basis. The reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

2.5 Recommended Practices

The following recommended practices have been determined:

2.5.1 Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis. At a minimum, testing should be performed annually, but the sensitivity of the information secured may require that these tests be done more often.

2.5.2 Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual, network administrator, system administrator, data custodian and end users.

2.5.3 Violation of the Information Security Policy may result in disciplinary action.

2.6 Data Classification

It is essential that all Council's data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity and importance. The following three classes are specified:

High Risk

High risk refers to any information for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation e.g. payroll, personnel and financial information are also in this class because of privacy requirements.

This policy recognises that other data may need to be treated as high risk because it would cause severe damage to the Council if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements. Information assets of a high risk nature also include process control systems which control critical infrastructure. It will be the process control systems owner's responsibility to implement the necessary security requirements

Confidential

Confidential information refers to data that would not expose the Council to loss if disclosed but that the data owner feels should be protected to prevent unauthorised disclosure. It is the data owner's responsibility to implement the necessary security requirements.

Public

Public information refers to data that is able to be freely disseminated.

All information resources should be categorised and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the Council.

The following are recommended practices for protection of data:

2.6.1 Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.

2.6.2 No Council-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.

2.6.3 Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.

2.6.4 High risk data must be encrypted during transmission over insecure channels.

2.6.5 Confidential data should be encrypted during transmission over insecure channels.

2.6.6 All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

2.6.7 Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of or repurposed data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

2.7 Access Control

2.7.1 Data must have sufficient granularity to allow the appropriate authorised access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorised purposes. This balance should be recognised.

2.7.2 Where possible and financially feasible, more than one person must have full rights to any Council owned server string or transmitting high risk data. Council will have a standard procedure that applies to user access rights for most instances, data owners or custodians may enact more restrictive practices for end user access to their data.

2.7.3 Access to network and application systems will be provided when appropriate user access control requests (refer intranet) are received from Managers and assessed as appropriate by system administrators. In the event that the system administrators raise concerns, these will be directed to the Information Technology Communications Manager to resolve with the relevant Director, as appropriate.

2.7.4 Routine reporting to system owners on user profile/access control levels must be provided.The applicant must have a personnel number which represents suitable personal identification prior to authorisation.

2.7.5 ITC are to maintain appropriate records of staff access requests, staff termination / transfer requests and changes made to a user's access levels both for general and application level accesses.

2.7.6 Access to the network and servers and systems will be achieved by individual and unique logins, and will require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognised forms of authentication.

2.7.7 Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorised use.

2.7.8 Passwords must be changed every 180 days where system password synchronisation or compliance is achievable. If the Operating System provides the facility, automatic Password Aging will be enforced.

2.7.9 All users of systems that contain high risk or confidential data must have a strong password – the definition of which will be established and documented by ITC. Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established in this policy.

2.7.10 Passwords must not be placed in emails.

2.7.11 Passwords must be of Twelve (12) characters minimum in length and must be alphanumeric in nature. Refer Definitions section of policy for detailed guidelines on password requirements.

2.7.12 Password validation will be limited to Five (5) attempts where system compliance is possible. In the event that attempts exceed this limit, then the systems must maintain logs of these attempts and lock out the user for a minimum duration of 10 minutes.

2.7.13 Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.

2.7.14 Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.

2.7.15 Users are responsible for safe handling and storage of all Council authentication devices. Authentication tokens (such as Smart Cards / Fobs) should not be stored with a computer that will be used to access the Council's network or system resources. If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled, where possible.

2.7.16 Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon termination. Where earlier notification has been made, the user account will be disabled / inactive during the afternoon of termination and the account rendered void within 30 days. Since there could be delays in reporting changes in user responsibilities, periodic user access review should be conducted by the network and application systems administrators.

2.7.17 It is the responsibility of Managers to ensure that appropriate notification of terminated staff is made prior to 48 hours of termination including advice on handover of appropriate hardware and software. (Refer also to the Staff Exit Procedures Instruction.)

2.7.18 Transferred employee access must be reviewed and adjusted as found necessary. Transferred employees should have their accounts reviewed upon transfer between council roles / departments. It is the responsibility of Managers to ensure that appropriate notification of transferred staff is made prior to 48 hours of transfer including advice on handover of appropriate hardware and software.

2.7.19 Monitoring must be implemented on all systems including, but not limited to, recording logon attempts and failures, successful logons and date and time of logon and logoff where allowable in the system configuration.

2.7.20 Activities performed as administrator or super-user must be logged where it is feasible to do so.

2.7.21 Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks. There should be a documented procedure for reviewing system logs.

2.7.22 When limited access to council related documents or files is required specifically and solely for the proper operation of Council department processes and where available technical alternatives are not feasible, exceptions are allowed under an articulated Department Policy that is available to all affected Department personnel. Each such policy must be reviewed by the Information Technology Manager and relevant Director for approval and appropriately documented and agreed prior to consent.

2.7.23 Decryption of passwords is not permitted, except by authorised staff performing security reviews or investigations. Use of network sniffers shall be restricted to network system administrators.

2.7.24 Systems administration of workstation computers will be maintained by ITC Services unless otherwise agreed. In the event that a Council Department requires specific privileges for administrator rights on a workstation computer, these must be requested through a user access request form available from the GRC Intranet. Each request will be reviewed by the Information Technology & Communications Manager in consultation with the relevant Director, as appropriate

2.8 Virus Prevention

2.8.1 Council uses anti-virus software , users must not interfere with or disable any process that constitutes the Anti-Virus software

2.8.2 Staff should contact ITC with any issues regarding the operation of the Anti-Virus Software.

2.9 Intrusion Detection

2.9.1 Intruder detection must be implemented on all servers and workstations containing data classified as high risk.

2.9.2 Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.

2.9.3 Server, firewall and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.

2.9.4 Intrusion tools should be installed where appropriate and checked on a regular basis.

2.10 Internet Security

2.10.1 All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified confidential.

2.10.2 All systems connected to the Internet should have a Council supported version of the operating system installed. Where possible, this provision should be applied to process control systems in acknowledgement that they usually operate on proprietary operating systems.

2.10.3 All systems connected to the Internet must be current with security patches.

2.10.4 The Information Technology Usage Instruction applies.

2.11 System Security

2.11.1 System integrity checks of host and server systems housing high risk Council data must be performed. Exception reporting on system integrity checks to be provided to Information Technology & Communications Manager routinely to all relevant Managers of high risk business and process control systems.

2.11.2 Restricted access will apply to all computer and communications hardware including SCADA, PLCs and field equipment used to access / update systems. Exceptions to this rule must be granted in writing by Information Technology & Communications Manager and relevant Director, as appropriate.

2.11.3 Detailed procedures for management of security on servers, firewalls, routers and other platforms must be maintained. These controls will be outlined in detail in the System Security procedures.

2.11.4 Appropriate controls must be employed to protect physical access to resources, commensurate with the identified level of acceptable risk. These controls will be outlined in detail in the Systems Security procedures.

2.11.5 Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc. Where hazardous environments exist, eg treatment plants, pumping stations, etc, the security provided and equipment used in these environments needs to match the hazard level of the environment, ie industrial grade equipment.

2.11.6 Appropriate environmental controls must be employed to protect information technology resources, commensurate with the identified level of acceptable risk, eg air temperature and humidity must be controlled to within acceptable limits. These controls will be outlined in detail in the Systems Security procedures.

2.11.7 No food and drink are to be taken into the computer server environment.

2.11.8 Adequate protection for power must be provided to the computer server room by way of uninterruptible power supply and backup generators.

2.11.9 Business continuity plans for Information Technology resources are appropriately maintained and applied.

2.11.10 Remote "Dial in" type access will be granted to staff who have appropriate authorisation and that have been granted council owned and configured workstation computers.

2.11.11 Dial in type services for external service providers must comply with detailed security procedures

2.12 Acceptable Use

2.12.1 Council computer resources will be used in a manner that is compliant with Council policies and State and Federal laws, regulations and ISO standards.

2.12.2 It is considered non-compliance to install or run software requiring a license on any council computer without a valid licence.

2.12.3 No software will be copied and distributed unless this action complies with licence conditions.

2.12.4 Use of the Council computing and networking infrastructure by Council employees unrelated to their Council positions must be limited in both time and resources and must not interfere win any way with Council functions or the employee's duties. It is the responsibility of employees to consult ITC, if they have any questions in this respect.

2.12.5 Uses that interfere with the proper functioning or the ability of others to make use of the Council's networks, computer systems, applications and data resources are not permitted.

2.12.6 Use of Council computer resources for personal profit is not permitted.

2.13 Auditor Access

Internal and external auditors are authorised to inquiry only access to all administrative information and systems. Access will be granted on permission from Information Technology & Communications Manager. Auditors are responsible for:

2.13.1 Evaluating Council's information security policy and procedures compliance during operational and administrative audits.

2.13.2 Evaluating the effectiveness of Council's security procedures and other internal controls.

2.13.3 Reviewing audit trails provided by System Administrators to determine whether activity is adequately documented.

2.13.4 Assisting management in the investigation of suspected incidents of security breach or improper activity.

2.13.5 Providing advice regarding internal controls.

2.14 Exceptions

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

2.14.1 Required commercial or other software in use is not currently able to support the required security features;

2.14.2 Legacy systems are in use which do not comply, but near-term future systems will and are planned for;

2.14.3 Costs for reasonable compliance are disproportionate relative to the potential damage.

2.14.4 In such cases, a written explanation of the compliance issue and a plan for coming into compliance in a reasonable amount of time must be submitted to the Information Technology & Communications Manager for written approval where appropriate

2.15 Violations

Violation of any provision of this policy may cause Council to:

2.15.1 Limit the individual's access to some or all Council systems.

2.15.2 Initiate legal action, including, but not limited to, criminal prosecution under appropriate state and federal laws.

2.15.3 Require the violator to provide restitution for any improper use of service.

2.15.4 Enforce disciplinary sanctions in accordance with the relevant Council policy as outlined in the Code of Conduct.

3. DEFINITIONS

Security can be defined as “the state of being free from unacceptable risk”. The risk concerns the following categories of losses:

i.) Confidentiality of information;
ii.) Integrity of data;
iii.) Assets;
iv.) Efficient and appropriate use;
v.) System availability; and
vi.) Control process failure (leading to serious harm or injury).

4. REVIEW DATE

October 2023

5. RELATED DOCUMENTS

N/A

6. ATTACHMENT

N/A