POLICY REGISTER

INFORMATION & COMMUNICATION TECHNOLOGY SECURITY POLICY

Document Control

Issue.	Prepared/Revised by and Date	Action/Amendment Description	Approved By and Date
1.0	May 2022	First Edition	Council Minute No. 2022/96

Note:
This policy has been developed from Balranald Shire Councils ICT Policy, Federal and State Government requirements. Council acknowledges that the policy as presented has been taken and amended to meet NSW local government requirements. Reference should be made to the Federal Government (ACSC) publication -Information Security Manual 2017

Objective

To provide a governing framework for the security and management of electronic information within Council.

Definitions/Application

Application

This Policy governs access to and use of the Council's electronic information and any information and communication technology (ICT) assets which create, process, store, view or transmit information.

Policy Statement

Balranald Shire Council is responsible for a significant amount of information held in electronic formats, and it is critical that this information be protected appropriately.

This policy seeks a consistent approach to the implementation of information security to protect information assets and any ICT assets which create, process, store, view or transmit information against unauthorised use or accidental modification, loss or release.

Council will adhere to the following ten ICT Security Principals:

ICT SECURITY PRINCIPLES

Principle 1 - Policy, planning and governance

Council management will recognise the importance of and demonstrate a commitment to maintaining a robust Council information security environment. At a minimum, Council will:

- develop an Information Security Policy Implementation Plan, ensuring alignment with Council business planning, general security plan and risk assessment findings.
- establish and document information security internal governance arrangements (including roles and responsibilities) to implement, maintain and control operational information security within the Council.
- establish and document information security external governance arrangements to ensure that third party service level agreements and operational level agreements clearly articulate the level of security required and are regularly monitored.

Principle 2 - Asset management

Council will implement procedures for the classification and protective control of information assets. As a minimum, Council will ensure:

- all information assets are assigned appropriate classification and control
- all ICT assets that create, store, process or transmit security classified information are assigned ICT asset custodians and are also assigned appropriate controls.

Principle 3 - Human Resources management

Council will minimise the risk of loss or misuse of information assets by ensuring that security controls are incorporated into Council human resource management, including the development of supporting policies and processes. At a minimum, Council will:

- implement induction and ongoing training and security awareness programs, to ensure that all employees are aware of and acknowledge the Council's ICT Security Policy, their security responsibilities and associated

security processes

- document and assign security roles and responsibilities where employees have access to security classified information or perform specific security related roles, and ensure that security requirements are addressed in recruitment and selection and in job descriptions
- develop and implement procedures for the separation of employees from, or movement within, the Council.

Principle 4 - Physical and environmental management

The level of physical controls implemented will minimise or remove the risk of equipment or information being rendered inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation. At a minimum, Council will ensure that:

- policies and processes are implemented to monitor and protect the use and/or maintenance of information assets and ICT assets away from premises.
- policies and processes are implemented for the secure disposal or reuse of ICT assets which are commensurate with the information asset's security classification level.

Principle 5 - Communications and operations management

Operational procedures and controls will be documented and implemented to ensure that all information assets and ICT assets are managed securely and consistently, in accordance with the level of required security. Council will at a minimum ensure:

- review ACSC guidelines at https://www.cyber.gov.au/
- the ACSC Information Security Manual (as amended) is used to ensure the security of data during transportation over communication networks.
- a network security guideline is developed and documented in line with the ASCS to guide network administrators in achieving the appropriate level of network security.
- adequate controls are defined and implemented for the prevention, detection, removal and reporting of attacks of malicious code on all ICT assets.
- comprehensive systems maintenance processes and procedures including operator and audit/ fault logs, information backup procedures and archiving must be implemented.
- operational change control procedures are implemented to ensure that changes to information processing facilities or systems are appropriately approved and managed.
- methods for exchanging information within Council and with third parties are compliant with legislative requirements.
  processes are developed and implemented to periodically review and test firewall rules and associated network architectures to ensure the expected level of network perimeter security is maintained.

Principle 6 - Access management

Control mechanisms based on business requirements, assessed/accepted risks, information classification and legislative obligations will be in place for controlling access to all information assets and ICT assets. At a minimum, Council will ensure that:

- authentication requirements, including on-line transactions and services, are assessed
- policies and/or procedures for user registration, authentication management, access rights and privileges are defined, documented and implemented for all ICT assets.
- control measures are implemented to detect and regularly log, monitor and review information systems and

network access and use, including all significant security relevant events.

Principle 7 - System acquisition, development and maintenance

During system acquisition, development and maintenance, security controls will be established and will be commensurate with the security classifications of the information contained within, or passing across, information systems, network infrastructure and applications. Council will at a minimum ensure:

- security requirements are addressed in the specifications, analysis and/or design phases and internal and/or external audit are consulted when implementing new or significant changes to financial or critical business information systems.
- processes (including data validity checks, audit trails and activity logging) are established in applications to ensure development and support processes do not compromise the security of applications, systems or infrastructure.
- authentication processes are consistent.
- processes are developed and implemented to manage software vulnerability risk for all IT security infrastructures.

Principle 8 - Incident management

Effective management and response to information security incidents is critical to maintaining secure operations. Council at a minimum will:

- ensure information security incident management procedures are established to ensure appropriate responses in the event of information security incidents, breaches or system failures.
- ensure all information security incidents are reported and escalated (where applicable) through appropriate management channels and/or authorities (ELT).
- establish and maintain an information security incident and response register and record all incidents.
- ensure that information security incidents caused by employees are investigated and where it is found that a deliberate information security violation or breach has occurred, that formal disciplinary processes are applied.

Principle 9 - Business continuity management

A managed process including documented plans will be in place to enable information and ICT assets to be restored or recovered in the event of a disaster or major security failure. At a minimum, Council will:

- establish an information and ICT asset disaster recovery register to assess and classify systems to determine their criticality.
- establish plans and processes to assess the risk and impact of the loss of information and ICT assets on Council business in the event of a disaster or security failure.
- develop methods for reducing known risks to Council information and ICT assets.
- ensure business continuity and information and ICT asset disaster recovery plans are maintained and tested to ensure systems and information are available and consistent with Council business and service level requirements.

Principle 10 - Compliance management

Council will ensure compliance with, and appropriate management of, all legislative and reporting obligations relating to information security. Council at a minimum will:

- ensure that all reasonable steps are taken to monitor, review and audit Council information security compliance.
- all Council information security policies, processes and requirements including contracts with third parties, are reviewed for legislative compliance on a regular basis and the review results reported to appropriate Council

management (ELT).

Review Triggers

This Policy is reviewed internally for applicability, continuing effect and consistency with related documents and other legislative provisions when any of the following occurs:

(1) The related documents are amended.
(2) The related documents are replaced by new documents.
(3) Amendments which affect the allowable scope and effect of a Policy of this nature are made to the head of power.
(4) Other circumstances as determined from time to time by a resolution of Council.

Notwithstanding the above, this Policy is to be reviewed at least once every two years for relevance and to ensure that its effectiveness is maintained.

Responsibility

This Policy is to be:

(1) implemented by all officers and Councillors; and
(2) reviewed and amended in accordance with the "Review Triggers" by the General Manager and ICT Consultant.

ICT Security Procedure Requirements

General Introduction

The ICT Security Procedures is to be read in accordance with the ICT Security Policy. Any inconsistency between the policy and procedure shall be read as if the policy dominates as to direction to be taken.

Principles to be Established through Procedure

Principle 1 - Policy, planning and governance

Principle	Action	Date	By Who	Completed
develop an Information Security Policy Implementation Plan, ensuring alignment with Council business planning, general security plan and risk assessment findings.	Policy developed	July 2021	Executive staff	
establish and document information security internal governance arrangements (including roles and responsibilities) to implement, maintain and control operational information security within the Council.	1. That an ITC Map of staff delegations and hierarchy is prepared to reflect authority for access. 2. That Councils Internal Auditor review the ICT map annually and check the allocation and removal of responsibility during the year.	1. August 2021 2. Annual Review	1.insert position 2. GM / Internal Auditor	
establish and document information security external governance arrangements to ensure that third party service level agreements and operational level agreements clearly articulate the level of security required and are regularly monitored.	Develop a written agreement to be provided and signed by third party suppliers and maintainers of Councils ICT systems.	February 2022	<insert position>	

Principle 2 - Principle 2 - Asset management

Principle	Action	Date	By Who	Completed
all information assets are assigned appropriate classification and control	Review ICT assets and assign controls e.g. programs updates	December 2022	GM & ICT Consultant	
all ICT assets that create, store, process or transmit security classified information are assigned ICT asset custodians and are also assigned appropriate controls.	Review ICT assets and assign controls e.g. programs updates, site management, access needs, relief employee assignment.	December 2022	GM & ICT Consultant	

Principle 3 - Human Resources management

Principle	Action	Date	By Who	Completed
implement induction and ongoing training and security awareness programs, to ensure that all employees are aware of and acknowledge the Council's ICT Security Policy, their security responsibilities and associated security processes	i.Staff policy developed as to Social Media and general IT use. 2.New staff package to include Social Media policy and acknowledgement form including required disciplinary advice as per Principle 8.	1.September 2021 2. September 2021	1. GM 2. GM	
document and assign security roles and responsibilities where employees have access to security classified information or perform specific security related roles, and ensure that security requirements are	1.That an ITC Map of staff delegations and hierarchy is prepared to reflect authority for access. 2. That Councils Internal Auditor review the ICT map annually and check the allocation and removal of responsibility during the year.	1. August 2021 2. Annual Review	1.GM 2. GM / Internal Auditor	
addressed in recruitment and selection and in job descriptions				
develop and implement procedures for the separation of employees from, or movement within, the Council.	1. That an ITC Map of staff delegations and hierarchy is prepared to reflect authority for access. 2. That access approval for changes in staff are made in writing and signed off by the senior manager of that section.	1. August 2021 2. December 2021	1. GM & ICT Consultant 1. Executive staff	

Principle 4 - Physical and environmental management

Principle	Action	Date	By Who	Completed
policies and processes are implemented to monitor and protect the use and/or maintenance of information assets and ICT assets away from premises.	1.Staff policy developed as to Social Media and general IT use. 2.New staff package to include Social Media policy and acknowledgement form	1. August2021 2. September 2021	1. GM 2. GM	
policies and processes are implemented for the secure disposal or reuse of ICT assets which are commensurate with the information asset's security classification level.	Develop an ICT cleaning procedure to remove Council information and factory reset all ICT assets before disposal. That a sign off process to check cleaning and reset has occurred.	September 2021	GM & ICT Consultant	

Principle 5 - Communications and operations management

Principle	Action	Date	By Who	Completed
a network security guideline is developed and documented in line with the ASCS to guide network administrators in achieving the appropriate level of network security.	Review actions under Federal Governments - acsc.gov.au/publications/Information_Security_Manual_2017_Controls.pdf	ongoing	GM & ICT Consultant	
adequate controls are defined and	That attacks are reported to ELT and the Internal and External	ongoing	GM & ICT Consultant	Ongoing

implemented for the prevention, detection, removal and reporting of attacks of malicious code on all ICT assets.	Auditors as to attack type, impact and controls implemented			
comprehensive systems maintenance processes and procedures including operator and audit/ fault logs, information backup procedures and archiving must be implemented.		ongoing	GM & ICT Consultant	ongoing
operational change control procedures are implemented to ensure that changes to information processing facilities or systems are appropriately approved and managed.	That a report is submitted to ELT prior to any changes to control procedures or ICT processing for approval.	Ongoing	GM & ICT Consultant	ongoing
methods for exchanging information within Council and with third parties are compliant with legislative requirements.	That a written process is prepared to exchange information of a sensitive nature with third parties. Note: this does not apply to publicly available information based on Councils web site, social media articles or information being supplied under council policies.	December 2021	GM & ICT Consultant	
processes are developed and implemented to periodically review and test firewall rules and associated network architectures to ensure the expected level of network perimeter security is maintained.	That an external consultant is used to test councils fire wall procedures annually. E.g. White Hack	Annually or as required when a breach is detected.	GM & ICT Consultant	

Principle 6 - Access management

Principle	Action	Date	By Who	Completed
authentication requirements, including on-line transactions and services, are assessed	That Councils Internal and external Auditors review annually and check the on-line transaction processing and security.	ongoing	GM & ICT Consultant	Ongoing

policies and/or procedures for user registration, authentication management, access rights and privileges are defined, documented and implemented for all ICT assets.	1. Social media policy developed 2. User acknowledgement form and access privileges recorded on form to be signed by employee.	1.August 2021 2. September 2021	GM GM & ICT Consultant	
control measures are implemented to detect and regularly log, monitor and review information systems and network access and use, including all significant security relevant events.	Event log to be printed weekly and reported breaches to be reported to ELT for action.	ongoing	GM & ICT Consultant	ongoing

Principle 7 - System acquisition, development and maintenance

Principle	Action	Date	By Who	Completed
security requirements are addressed in the specifications, analysis and/or design phases and internal and/or external audit are consulted when implementing new or significant changes to financial or critical business information systems.	That Council include security requirements in the replacement of all ICT programs and assets purchased to protect the organisations IT network.	As required	GM & ICT Consultant	ongoing
processes (including data validity checks, audit trails and activity logging) are established in applications to ensure development and support processes do not compromise the security of applications, systems or infrastructure.	That suppliers are advised of Councils requirements to protect all ICT assets and networks both internal and external and that as per Principle 1 that a signed statement is provided to Council acknowledging this requirement.	ongoing	GM & ICT Consultant	ongoing
authentication processes	That an authentication process for	November 2021	GM & ICT Consultant	ongoing
are consistent.	all new and externally sourced data is undertaken and the event log is retained.			
processes are developed and implemented to manage software vulnerability risk for all IT security infrastructures.	1. Written back up procedures and tests are undertaken to determine if procedures are being applied. 2. A review of the procedure by Councils Internal Auditor is	October 2021	GM & ICT Consultant	ongoing

Principle 8 - Incident management

Principle	Action	Date	By Who	Completed
ensure information security incident management procedures are established to ensure appropriate responses in the event of information security incidents, breaches or system failures.	That Council Contingency plan is updated to include procedures for IT recovery.	September 2021	GM & ICT Consultant	
ensure all information security incidents are reported and escalated (where applicable) through appropriate management channels and/or authorities (ELT).	Report all incidents to ELT and to the external auditors.	ongoing	GM & ICT Consultant	ongoing
establish and maintain an information security incident and response register and record all incidents.	Develop a standalone (NonElectronic) register.	September 2021	GM & ICT Consultant	
ensure that information security incidents caused by employees are investigated and where it is found that a deliberate information security violation or breach has occurred, that formal disciplinary processes are applied.	Develop as a staff procedure a disciplinary process to be signed off by staff as part of the staff commencement and change of authority procedure.	September 2021	GM	

Principle 9 - Business continuity management

Principle	Action	Date	By Who	Completed
establish an information and ICT asset disaster recovery register to assess and classify systems to determine their criticality.	Include the recovery process in Councils contingency plan	October 2021	GM & ICT Consultant	
establish plans and processes to assess the risk and impact of the loss of information and ICT assets on Council business in the event of a disaster or security failure.	Contingency plan developed. Update ICT process in plan	October 2021	GM & ICT Consultant	
develop methods for reducing known risks to Council information and ICT assets.	Develop a procedure to limit access by staff to restricted ICT controls eg password changes or authorisation codes.	October 2021	GM & ICT Consultant	
ensure business continuity and information and ICT asset disaster recovery plans are maintained and tested to ensure systems and information are available and consistent with Council business and service level requirements.	1. Undertake an annual test of fire walls and run a mock test of ICT failure to ensure key staff are aware of contingency procedures. 2. Record event and improvement outcomes.	December 2021	GM & ICT Consultant	ongoing

Principle 10 - Compliance management

Principle	Action	Date	By Who	Completed
ensure that all reasonable steps are taken to monitor, review and audit Council information security compliance	Require Councils internal auditor to review and assess ICT performance and records annually and report any concerns to the Internal Audit group for action.	annually	GM & ICT Consultant	Ongoing
all Council information security policies, processes and requirements including contracts with third parties, are reviewed for legislative compliance on a regular basis and the	Require Councils internal auditor to review and assess ICT performance and records annually and report any concerns to the Internal Audit Group and ELT for action.	Annually	GM & ICT Consultant	Ongoing
review results reported to appropriate Council management (ELT).				