100

ACCESS CONTROL

Strategic Outcome:	Good government		
Date of Adoption:	19 August 2020	Minute Number:	186
Date for Review:	21 August 2024		
Responsible Officer:	Director Corporate Services		
Document Control:	Replaces and revokes the Password Policy adopted 9 October 2019		
Delivery Program Link:	2.1.3.6 Provide information technology and associated support for Council operations		

1. POLICY STATEMENT

Berrigan Shire Council is committed to maintaining a robust and secure Information and Communication Technology (ICT) environment.

A key control measure used by the Council to meet this commitment is access control. Controlling access to the ICT environment minimises the risk of unauthorised use and malicious damage

2. PURPOSE

The purpose of this Policy is to:

- Ensure access to Council information and services is controlled and secure.
- The Council meets all its legislative and other requirements for information security and privacy
- Council operations are not impacted by unplanned ICT loss of service

3. SCOPE

This policy applies to:

- Access control for all items connected to the Council's Information Technology network
- Access control for all Council information and services hosted on the Cloud

4. DEFINITIONS

Access control: Regulation of who or what can view or use resources in a computing environment

Administrator: responsible for the upkeep, configuration, and reliable operation of client computer systems, servers, and data security systems

Authentication: The process of identifying an individual, usually based on a username and password

Authorisation: The process of giving someone permission to do or have something

Cloud: Hosted information and communication services delivered over the internet

Council officials: as defined in the Berrigan Shire Council Code of Conduct

IT Network: A group of computers and other equipment linked by physical or wireless connections.

Logical access the systems used to identify, authenticate and authorise and account for use of the Council's computer information systems.

Multi-factor authentication: a security mechanism that requires an individual to provide two or more credentials in order to authenticate their identity. For the purposes of this policy this will usually be possession of a hardware token or smartphone.

Password: a string of characters used to verify the identity of a user during the authentication process

User name: a name that uniquely identifies someone on a computer system

Virtual Private Network: an encrypted connection over the Internet from a device to a network

5. POLICY IMPLEMENTATION

5.1 Risk management approach

The Council takes a risk management approach to the security of its ICT environment in line with the Council's Risk Management framework. Access control measures put in place by the Council should be based on a risk assessment prepared by Council staff as per the Risk Management framework.

Identified risks and control measures will be included in the Council's corporate Risk Register.

5.2 Physical access

Where possible, the Council will limit physical access to key components of the Council's IT network.

In the first instance, the Council will only allow Council officials and other persons authorized by the Council physical access to Council workspaces.

Secondly, rooms containing key components of the Council's IT system will be kept secure (locked) at all times with access only available to Council officials and contractors as approved by the Director Corporate Services

5.3 Logical access

The Council will maintain a set of procedures for controlling logical access to the Councils computer information systems.

5.3.1 Register

The Council will maintain a register of all access points that require authentication. The register will include at a minimum:

- an assessment of the risk of unauthorised access,
- the complexity requirements for the password, and
- maximum time between password changes

5.3.2 Authorising and removing access

The Council will maintain a set of procedures to ensure logical access to Council's computer information systems is only available to approved Council officials and contractors. This will include procedures for setting and approving, modifying and removing access and authorisation rights for Council employees and Councillors.

The Council's IT Officer, in conjunction with at least one other approved staff member, will review access and authorisation rights for key components every six (6) months. This will include at a minimum:

- the Council's main IT network and email system
- Financial management system, and
- Electronic Document and Records Management System (EDRMS).

Council officials should only have logical access and authorisation for those components of the Council's computer information system reasonably necessary for them to undertake their role with the Council.

5.3.3 Authentication and passwords

All Council officials are to follow routine IT access security requirements.

Council officials must:

- Never share passwords across functions – i.e. use a different password for network access, for the Council's management software and for any cloud functions
- Never share passwords with other users – unless the password is a generic Council username **and** approved by the Director Corporate Services.
- Never re-use the same password twice
- Never write passwords down
- Always log off or lock IT equipment & devices when unattended

5.4 Password requirements

5.4.1 Time

All passwords providing access to Council's ICT network or information must be changed at regular intervals. The Council will maintain procedures setting out these requirements.

Passwords granting administrator rights for the IT network and Council's management software are to be changed no less than annually.

For other services, the length of the interval will be determined by the Director Corporate Services based on an assessment of the risk of unauthorised access.

5.4.2 Complexity

All passwords providing access to Council's ICT network or information must meet minimum complexity requirements. The Council will maintain procedures setting out these requirements.

These will be determined by the Director Corporate Services based on an assessment of the risk of unauthorised access

5.4.3 Multi-factor authentication

Where available multi-factor authentication will be used for access to key services.

Multi-factor authentication **must** be used to access the Council's banking service.

5.5 Remote access

The Council has the capability to provide remote access to its ICT environment for approved Council officials off-site including those working from home or travelling on business.

Remote access is not a right or condition of employment and will only be available with approval

5.5.1 Approval

Approval for remote access to the Council's ICT environment will be granted on an as-needs basis and usually will be for a limited period of time.

Approval for remote access may only be provided in writing by the General Manager or Directors. The IT Officer will maintain a record of Council officials with remote access.

5.5.2 Virtual Private Network (VPN)

Remote access to the Council's IT Network will only be provided via a Virtual Private Network (VPN).

The IT Officer is the only Council official with administrator rights to the VPN

5.5.3 Review

The IT Officer will review the Remote Access register at least once every three (3) months to ensure only approved Council officials have remote access

5.6 Education and Enforcement

Where possible, the Council will use software-based tools to enforce compliance with this policy.

Where this is not possible, the onus is on the Council official to ensure that he/she complies with the requirements of the policy and associated procedures

Initial breaches of this policy will be dealt with via education and training. Further breaches may lead to disciplinary action as per the Local Government (State) Award

6. RELATED LEGISLATION, POLICIES AND STRATEGIES

6.1 Legislation

- *Local Government Act 1993*
- Local Government (State) Award 2020

6.2 Council documents

- Berrigan Shire Council Code of Conduct
- Information and Communication Technology Strategic Plan 2019-2024
- Communication Devices Policy
- Information and Communication Technology Policy
- Risk Management Policy and Framework
- Fraud Control Policy and Framework

6.3 Other resources

- NSW Office of Cybersecurity - password tips