NAMBUCCA VALLEY COUNCIL

Remote ICT Access Policy
POLICY No CS 31

Our Vision

Nambucca Valley ~ Living at its best

Our Mission Statement

'The Nambucca Valley Council will value and protect its natural environment, maintain its assets and infrastructure and develop opportunities for its people.'

1.0 Policy Objective

The purpose of this Policy is to define rules and requirements for connecting to Council's network remotely. These rules and requirements are designed to minimise the potential exposure of information held by Council which may result from unauthorised use of Council's resources.

2.0 Related Legislation/Policies

Use of Personal Computers Policy
Use of Internet and Email Policy
CS28 Information Security and Management Policy

3.0 Definitions

"MFA" Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication request.

"Authorised User" is an employee, contractor or vendor who has been approved by Council to remotely access the council network.

"Virtual Desktop" includes a Workstation, Server, Remote Desktop Server or a Virtual Desktop that can be configured

"Sensitive Information" comprises all personal information and all confidential information, the loss of which would, or would be likely to, cause damage or distress to individuals or to the Council.

"Council Controller" is equipment either owned by council or equipment that has council anti-virus software installed and is able to be locked or wiped remotely.

4.1 Policy Content

This policy will define the rules and requirements for connecting to Council's network from a remote location. The rules and requirements are based on industry standards and advice from Cyber Security NSW.

4.2 Scope

This policy applies to all Council employees, contractors, vendors and agents when connecting to the Council network remotely.

4.3 Approval Form

To gain authorisation for remote access each employee, contractor or vendor will be required to complete relevant request forms.

4.4 Secure Connections

Remote access to Council’s network will be over an encrypted VPN connection using unique logins, strong pass-phrases and Multi-factor Authentication (MFA).

Authorised users shall protect their login and passwords and any equipment used for MFA.

All hardware used to connect to Council’s network will be controlled by Council unless approved by the Manager ICT.

Contractors and Vendors may use equipment not controlled by Council but must ensure they are using up-to-date anti-virus software and that all reasonable steps are taken to ensure their equipment if free from viruses and malware and only used by authorised staff. The Manager ICT must approve this equipment and Contractors and Vendors returned signed copies of documentation acknowledging their compliance.

No Council controlled equipment is to be used for personal use and users shall ensure the equipment is not connected to any other network whilst connected via VPN, with the exception of personal networks that are under their complete control or under the complete control of an authorised user or third party.

4.5 Use of Virtual Desktops

No Council systems or data shall be accessed directly from a remote host. All access will be conducted using Remote Desktop Protocol (RDP) to one of the Virtual Desktop types depending on the user’s requirements.

4.6 Industrial Equipment

Remote access to the Scada and PLC’s networks will be restricted and will require approval by the Manager Water and Sewerage.

4.7 Mobile Phones and Tablet Computers

Access to email via mobile phones or tablet computers will not require VPN access.

4.8 Monitoring

Council reserves the right to monitor all internet usage and data access whilst remotely connected to Council’s network. Logon and Logoff times and other information may also be recorded and used to ensure compliance with Council policies.

4.9 Responsibilities

Manager ICT
The Manager ICT is to ensure only authorised users have remote access and appropriate training is provided to those users.

The Manager ICT is also responsible for the development and monitoring of the adherence to the Policy.

5.0 History

New Policy

Department:	**Corporate Services**	**Last Reviewed**	**Resolution Number**
Policy Category	Organisation		
Endorsed By:	AGMCS		
Approval Authority:	General Manager		
Policy Owner:	ICT		
Contact Officer:	Manager ICT		
Document No.	31868/2020		
First Adopted:	14 October 2021		
Resolution No:	413/21		
Review Date:	October 2023		