Policy

95 INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Version: 01

File Reference No:	17.048.1
Strategic Outcome:	Good government
Date of Adoption:	19/09/2018
Date for Review:	21/09/2022
Responsible Officer:	Director Corporate Services

1. POLICY STATEMENT

Berrigan Shire Council needs to have an information technology framework that assists Council to carry out its duties to the public. The Information and Communication Technology (ICT) services need to be secure, functional, flexible and robust to meet the digital changes in local government.

2. PURPOSE

This policy provides direction to Councillors and Council staff on the operation and facilitation of Council ICT infrastructure and services.

3. SCOPE

This policy applies to all Councillors, Council staff, third party vendors and Council's ICT department and functions.

4. OBJECTIVE

This policy was developed to assist the Council with the following Delivery Plan Action:

> *2.1.3.6 Provide information technology and associated support for Council operations*

5. DEFINITIONS

Anti-virus - Software designed to detect and destroy computer viruses.

Backup - A copy of a file or other item of data made in case the original is lost or damaged.

BYOD (Bring Your Own Device) - The practice of allowing the employees of an organisation to use their own computers, smartphones, or other devices for work purposes.

Cloud service – A cloud service is any service made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers.

Cryptographic key – A cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.

Data - The quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

Hardware - The machines, wiring, and other physical components of a computer or other electronic system.

Mail filter - Email filtering is the processing of email to organize it according to specified criteria.

Mobile device - A portable computing device such as a smartphone or tablet computer

Software - The programs and other operating information used by a computer.

SSL Certificate - SSL Certificates are small data files that digitally bind a cryptographic key to an organisation's details.

Replication - The action of copying or reproducing something.

Virus - A piece of code, which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

VPN (Virtual Private Network) - A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.

Wi-Fi - A facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

6. POLICY IMPLEMENTATION

6.1 Security

Council takes steps to ensure that its network and data is kept secure and its data integrity is maintained.

Access to Council server infrastructure and equipment is restricted in the server room and access will only be permitted by the General Manager, Directors and the IT Officer.

Council has in place an appropriate anti-virus and mail filtering systems.

Council blocks all ports other than those that are required for Council services to run. Council reviews the firewall access, remote access, logs and ports on an annual basis.

Council will provide remote access and Virtual Private Network (VPN) access where a business case is demonstrated. The IT Officer regularly reviews and revokes remote access where it is no longer required.

SSL certificates are purchased and renewed to ensure Councils website and public facing access points are secure.

Where Council makes use of cloud services it will ensure that those services are secure, have backups, are access controlled and if services cease Council has a way to maintain data integrity.

6.2 User Permissions

User permissions can only be set or altered by the IT Officer on request from General Manager, Directors or the Finance Manager. Council have developed a procedure to ensure new council staff are given appropriate permissions and access levels (software, email, domain, Wi-Fi, network drives) to undertake their role and that permissions are removed as appropriate if they change roles or leave Council.

Council keep a register of user permissions and access levels for all Council officials and third parties. This is reviewed on a three monthly basis or as required.

6.3 Devices & Hardware

Procurement of devices and hardware i.e. PCs, mobile phones, tablets, printers and other peripherals to be purchased through Council's IT Officer. A business case is be demonstrated before procurement of new equipment (as opposed to replacements).

Procurement is done in line with the Council's procurement policy and framework.

Council keeps a register of all devices and hardware issued to Councillors and Council staff. Council officials are responsible for safe keeping and appropriate use of this equipment.

Bring Your Own Device (BYOD) may be permitted with permission from the Director of Corporate Services and is assessed on a case-by-case basis.

Data Usage can be monitored to ensure no misappropriate use occurs. Directors and Managers are notified of any anomalies with data usage.

6.4 Software

Procurement of software is obtained with permission of directors and advice from IT officer. A business case is to be undertaken before purchase of a new software product.

Procurement is done in line with the Council's procurement policy and framework.

Installation is undertaken by IT officer or by a third party with permission and access from the IT officer. Individuals are not permitted to purchase or install their own software.

All software installed by council is appropriately licensed and renewed. A register is kept by the IT officer of all software being used by Council. No unlicensed software is installed.

6.5 Backup, Replication and Recovery

6.5.1 Backup and replication

Council has a backup and disaster recovery procedure in place. This consists of replication and frequent backups of the virtual server environment. Council runs incremental backups every workday on the hour between 8AM and 6PM and a full backup on Sunday. Backup logs are emailed to IT Officer for every backup and replication instance.

Daily backups are taken and transferred off-site on a daily basis. An End of Financial Year backup is taken and provided to the Finance Manager for safe keeping.

Councils Virtual Server environment are replicated two times every day.

Council has backups of its website. Monthly backups are taken and tested every three months or as required.

6.5.2 Disaster Recovery

Council tests backup data integrity every three months or as required. Virtual Server replication is tested on a daily basis.

6.6 Use and misuse

6.6.1 Information protection

The Council ensures that information stored on its Information Technology and Communications systems is stored, accessed and used in line with its legislative obligations and its Privacy Management Plan.

6.6.2 Private use

Council officials are expected to use Council's Information and Communications Technology resources in line with both the letter and the spirit of the Council's Code of Conduct and other appropriate Council policies relating to private use.

7. RELATED LEGISLATION, POLICIES AND STRATEGIES

7.1 External Legislation Policies and Strategies

- *Local Government Act 1993*
- *Workplace Surveillance Act* 2005
- *Privacy and Personal Information Protection Act 1998*
- Audit Office of NSW – Detecting and Responding to Cyber Security Incidents

7.2 Internal Policies

- Code of Conduct
- Privacy Management Plan
- Procurement & Disposal Policy

Policy

- Payment of Expenses & The Provision of Facilities for Mayors & Councillors Policy
- Public Internet Usage Policy
- Risk Management Policy & Framework
- Expenses and Facilities Guidelines for Staff
- Communication Devices Policy
- Social Media Policy
- Fraud Control Policy