POLICY:-	
Policy Title:	Digital Information Security Policy
File Reference:	F13/77-07
Date Policy was adopted by Council initially:	18 December 2014
Resolution Number:	401/14
Other Review Dates:	N/A
Resolution Number:	N/A
Current Policy adopted by Council:	16 August 2018
Resolution Number:	242/18
Next Policy Review Date:	2020

PROCEDURES/GUIDELINES:-	
Date procedure/guideline was developed:	N/A
Procedure/guideline reference number:	N/A

RESPONSIBILITY:-	
Policy developed by:	Director of Finance and Administration
Committee/s (if any) consulted in the development of this Policy:	N/A
Responsibility for implementation:	General Manager
Responsibility for review of Policy:	Director of Finance and Administration

1. BACKGROUND

It is best practice that Council adopts a formal policy supporting the consistent and systematic collection, classification, labelling and handling of information and digital information systems.

2. SCOPE

This policy establishes the digital information security requirements that take into account a minimum set of controls for the electronic / digital forms of information held by the Council. This policy does not specifically cover the security of hardcopy or non electronic information; however the objectives of this policy apply equally to information in any format.

This policy applies to all employees, contractors, and Councillors of Upper Lachlan Shire Council.

3. OBJECTIVE

This policy is designed to ensure that digital information and information systems security objectives are achieved by Council. These objectives include:-

- Confidentiality – to uphold authorised restrictions on access to and disclosure of digital information, this includes all types of information including personal information.

- Integrity – to protect information against unauthorised distribution, alteration or destruction, and ensure information is lawfully used.

- Availability – to provide authorised users with timely and reliable access to information.

- Compliance – to comply with all applicable legislation, regulations, policies and contractual obligations requiring information to be available and safeguarded (security controls in place).

- Assurance – to provide assurance to the community, rate payers and the general public that information held by Council is appropriately protected and handled.

4. PRINCIPLES

1. To meet operational business needs, accountability requirements and community expectations;
2. Internal documents should be easily accessed and they must be structured to ensure that they capture the information required and are presented in a manner that makes the information easy to interpret;
3. Active risk management and risk mitigation; and
4. To facilitate the minimum data requirements for information required.

5. POLICY STATEMENT

Council's responsible officer for digital information security, information systems security, individual user access rights, and implementation of this policy is the Director of Finance and Administration.

Information must be appropriately recorded and archived in accordance with Council's records management requirements and in accordance with the NSW State Records Act 1998 and associated standards.

Council will, within its budgetary constraints, endeavour to ensure complete, concise, and systematic digital information is maintained and stored appropriately in an Electronic Document Management System. Council at present uses HPE Content Manager (TRIM EDM).

Council utilises Civica's Authority finance database for the capture, storage and financial management and reporting tool to meet Australian Accounting Standard and Local Government Code of Accounting and Financial Reporting guideline requirements.

The unauthorised modification, deletion, or disclosure of information from Council digital information technology systems is expressly forbidden and disciplinary action will be taken by Council against any individual who does not comply with this policy.

6. CORPORATE INFORMATION SECURITY

Security is a vital element of information technology provisions; including equipment and privacy of information. All reasonable measures will be taken to preserve privacy. The Council will comply with data protection provisions in the Privacy and Personal Information Protection Act 1998 (PPIPA) and comply with the Government Information (Public Access) Act 2009 (GIPA).

All non-public information will be protected by an authorisation (password) system and users will be advised on the best practices for data management and security.

All equipment will be identifiable in case of theft and appropriate measures will be taken to prevent theft of equipment.

Appropriate measures will continue to be implemented to protect Council information and systems from external electronic attack (hacking), for instance by the use of up-to-date firewall technology and endpoint protection from viruses, malware, cyber security threats, and similar hazards.

Backup copies of all information stored on centrally managed file servers will be made daily and will be carefully stored. The primary purpose of such backups is to make it possible to recover critical systems, software and corporate data.

Controls are implemented to protect Council’s information and IT assets from external threats originating through remote access technology. Council provides a secure dual factor authentication method for remote users.

7. PERSONNEL INFORMATION SECURITY

Every individual who has access to and uses Council held information, information systems, computers or mobile device equipment will be made aware of this policy. All Council staff, contractors, and Councillors are responsible for maintaining information security.

The responsibility of individual users includes, but is not limited to, the following:-

- Complying with all Council policies, procedures, guidelines, contracts, and relevant statutory and regulatory legislation requirements;

- Ensuring information is only used for the purpose it was collected;

- Maintaining confidentiality of all user passwords;

- User passwords login are reset by an IT system control and users are required to update their password after 60 days;

- Council computers must be switched off when not in use, to prevent unauthorised access to the Council network;

- Maintaining a clear desk and clear computer screen so confidential and commercial in-confidence information is secured. Council computers and ipads shall enforce a password protected screensaver after 15 minutes in-activity to ensure the device is not utilised by another party;

- User access rights of file server directories and Civica’s Authority module permissions will be regularly reviewed by the Information Systems Coordinator to ensure that any unnecessary privileges will be removed and any unauthorised use of privileges will be detected and addressed;

- Maintaining the safe storage and physical security of Council owned information technology equipment, information assets, and mobile electronic devices;

- All loss or damage of Council information and systems including computers, laptops, tablets and mobile phones must to be promptly reported to Council’s Information Technology Staff; and

- Report all security incidents, events, weaknesses, and security threats that are designed to compromise Council information systems integrity promptly to the Information Systems Coordinator to allow timely corrective action to be taken.

8. INFORMATION CLASSIFICATION

All digital information shall be classified to ensure it receives an appropriate level of protection. In classifying information, regard is given to obligations imposed by relevant legislation and regulations, in particular the State Records Act 1998, Privacy and Personal Information Protection Act 1998, and the Government Information (Public Access) Act 2009.

Council's HPE Content Manager (TRIM EDM) has an appointed Administrator and has developed an Administrator User Manual and General User Manual. The Administrator User Manual has detailed notes in relation to the following information classification processes:-

1. Access Controls
2. Caveats
3. Location Security Caveats
4. Information Classification Security Caveats
5. Record Security Caveats
6. Adding New Classification Levels
7. Document Security
8. Data Retention Schedules
9. Data Disposal Reports

9. HANDLING AND PROCESSING OF INFORMATION

Controls must be in place to prevent unauthorised disclosure, modification, removal and destruction of digital information.

There is user authentication, access logs, and active audit event history on all HPE Content Manager (TRIM EDM) file containers and user email accounts. Staff training is undertaken periodically to assist users meet their obligations with regards to the safe handling and processing of information.

Information Access and Network Access may be revoked at any time by the Director of Finance and Administration if there is a reasonable suspicion that the continued provision of access to information assets and systems is not in the overall interests of Upper Lachlan Shire Council.

10. RELATED POLICIES

- Information Technology Strategic Plan 2015-2018.
- Records Management Policy and Procedures.
- Council's Code of Conduct.
- TRIM EDM Administrator User Manual.
- TRIM EDM General User Manual.
- Business Continuity and Disaster Recovery Plan.
- Complaints Management Policy.
- Gathering Information Policy.
- Internet and Email Usage Policy.
- iPad Policy.
- Social Media Policy.
- Electronic Security System Policy.

- Delegations of Authority Policy.
- Privacy and Personal Information Management Plan.
- Fraud and Corruption Prevention Policy.

11. OTHER RELEVANT LEGISLATIVE PROVISIONS

- Local Government Act 1993;
- Local Government (General) Regulation 2005;
- Local Government (State) Award 2017;
- State Records Act 1998;
- Electronic Transaction Act 1999;
- Privacy and Personal Information Protection Act 1998;
- Independent Commission against Corruption Act 1988;
- Government Information (Public Access) Act 2009; and
- Work Health and Safety Act 2011.

12. VARIATION TO POLICY

That Council reserves the right to vary the terms and conditions of this policy.