IT Security Policy

1 Document Information

Version Date *(Draft or Council Meeting date)*	30 April 2019]
Author	Nathan Stubberfield, System Administrator
Owner *(Relevant director)*	Director of Finance and Corporate Services
Status – *Draft, Approved, Adopted by Council, Superseded or Withdrawn*	Adopted by Council
Next Review Date	Within 12 months of Council being elected
Minute number *(once adopted by Council)*	19/04/14

2 Summary

The IT Security Policy sets the requirements to ensure Cabonne Council's Information and anything that stores, or accesses Cabonne Council Information is secure.

3 Approvals

Title	Date Approved	Signature

4 History

Unless otherwise indicated, printed or downloaded versions of this document are uncontrolled. Before using this document check it is the latest version by referring to Council's Policy Register at www.cabonne.nsw.gov.au.

Minute No.	Summary of Changes	New Version Date
19/04/14	**Endorsed by Council**	**30 April 2019**

5 Reason

5.1 To ensure any asset that stores or accesses Cabonne Council information including but not limited to computer systems, PCs, mobile devices and telephones is secure.

5.2 To minimise the impact of incidents on the Council's image, reputation, business operations and profitability.

5.3 To ensure compliance with regulatory requirements

5.4 To protect information so as to minimise the risk of financial and other loss to the Council

5.5 To establish the accountability for employee actions in regard to protecting, disclosing, accessing, destroying and modifying Cabonne Council information.

5.6 To support the strategic endeavours of Cabonne Council by being safe, secure and reliable.

6 Scope

6.1 This policy is applicable to the whole of Cabonne Council, its employees, Councillors, contractors, consultants, and any other party given access to Council information technology assets or confidential information.

6.2 This policy applies to all information technology and physical assets that are owned or leased by Cabonne Council or in Council's custody and control, and to Cabonne Council's confidential information.

7 Associated Legislation

Government Information (Public Access) Act 2009

Information Privacy Act 2000

NSW State Records Act 1998

Privacy and Personal Information Protection Act 1998

Public Records Act 1973

Workplace Surveillance Act 2005

8 Responsibilities

8.1 Policy Owner

The policy owner is responsible for overseeing the implementation, adherence to and review of this Policy.

8.2 System and Information Owners

System and Information owners are responsible for managing the risk associated with their relevant systems and information and ensuring compliance with policies, standards, procedures and guidelines. They are also responsible for reporting non-compliances and associated actions to the System Administrator

8.3 Others

All Council permanent and temporary employees, contracted staff, consultants and other workers are responsible for ensuring personal compliance with this policy and related standards and procedures.

9 Related Documents

Document Name	Document Location

10 Policy Statement

10.1 The Policy

10.1.1 This Security Policy and access to the Security Standards must be available to, understood, formally accepted and adhered to by all Council staff.

10.1.2 All Cabonne Council staff have a responsibility to protect Council and to minimise the risk that might result from inappropriate use of such information.

10.1.3 Security standards and procedures must be developed and reviewed annually to ensure they continue to support the objectives of this policy.

10.1.4 All information technology and physical assets must be secured in accordance with the relevant information security standards and procedures.

10.1.5 Council assets are to be made available to authorised people only, according to least privilege, and must only be used in accordance with the relevant security standards and procedures. Access must be approved by Managers and/or System Owners.

10.1.6 All Council information rated confidential or internal use only must be protected against intentional or unintentional access or disclosure.

10.1.7 All Council information and systems must be protected and maintained to ensure that integrity is assured.

10.1.8 All Cabonne Council information and systems must be protected and maintained to ensure that availability is assured.

10.1.9 All access to Council information and systems must be auditable to ensure accountability and non-repudiation of actions.

10.1.10 Defence in depth must be applied to the design, development and deployment of all Council systems to ensure a balanced security approach.

10.1.11 The design, development, deployment, and maintenance of systems must be done in consultation with the System Administrator and in accordance with the security standards and procedures.

10.1.12 All Council systems and services must comply with relevant national and international standards identified by the System Administrator.

10.1.13 Security incident management response procedures must be implemented.

10.1.14 Information security risks and exemptions must be included in the risk management framework and reviewed at least annually.

10.1.15 Management will carry out an annual review of the policy to ensure ongoing compliance with legal and industry requirements.

10.2 Exemptions

10.2.1 The policy owner is responsible for approving and monitoring all exemptions to the policy.

10.2.2 Exemptions to this policy must be expressly authorised in writing by the policy owner who will ensure that the channel, system or information owner understands, acknowledges and accepts the risk associated with the exemption – and will notify the System Administrator.

10.3 Discipline

10.3.1 Where a breach of this security policy is identified, whether accidental or intentional, individual users, system and information owners are required to notify their supervisor and the System Administrator immediately, the System Administrator will then notify the Human Resources Coordinator if appropriate.

10.3.2 Any breach of this policy by staff will be handled within the Cabonne Council policy and framework for human resources.