# Strathbogie Shire Council Information Security Policy

September 2023

Strathbogie
SHIRE COUNCIL

## Contents

# Information Security Policy

| | |
|---|---|
| Document ID: | 11567 |
| Effective Date: | 17 May 2011 |
| Last Review: | November 2019 |
| Current Review: | September 2023 |
| Date Adopted by Council: | 17 October 2023 |
| Next Scheduled Review Date: | September 2025 |
| Responsible Officer: | Manager Digital Innovation and Technology |

# PART 1 POLICY

## 1. PURPOSE

1.1. The Information Security Policy (the Policy) specifies the requirements for the management of information security for  Strathbogie Shire Council.

1.2. For the purpose of this Policy:

- The term "information" covers both information and data.
- Information security refers to the confidentiality, protection, integrity, and availability of Strathbogie Shire Council information, information systems and networks.

1.3. This Policy (and its related documents) is designed to enable Strathbogie Shire Council to:

- Maintain the security, privacy and quality of its information and that of its customers and other stakeholders.
- Manage information risk within appetite, while ensuring that the Strathbogie Shire Council's business objectives are met.
- Meet regulatory requirements and expectations relating to information risks.

1.4. All Business Units (BU) must implement the minimum baseline of controls prescribed in this Policy to manage information risk. Additional controls may be implemented if deemed necessary (e.g. to manage the risk profile of Strathbogie Shire Council, to meet any regulations or contractual arrangements).

1.5 This Policy applies to all personnel (employees, contractors, and Councillors) directly engaged by Strathbogie Shire Council or by a third-party partner providing services to Strathbogie Shire Council

## 2. POLICY STATEMENT

2.1 Strathbogie Shire Council processes, stores and transmits large volumes of personal and confidential information through its information systems to service Strathbogie Shire Council's customers / stakeholders, conduct business activities and inform decision making. This information also forms records that are authoritative evidence of Strathbogie Shire Council's activities. Therefore, managing information risk is essential to Strathbogie Shire Council.

2.2 Strathbogie Shire Council's appetite for management of information risk is to operate effective controls to safeguard the confidentiality, integrity, quality and availability of customer, personnel and business information by continually enhancing information security capability, maintaining a strong position relative to other Victorian Councils which requires allocating sufficient resource capacity and capability to manage and control information security risks, whilst complying with applicable laws, contracts and regulations.

2.3 Strathbogie Shire Council aims to protect the business and the community, including its employees, customers, and councillors by minimising the impact of and learning from information risk.

2.4 Strathbogie Shire Council will implement controls to manage information risk throughout the information lifecycle irrespective of whether information and supporting processes are managed internally or through third party organisations.

## 3. APPLICATION OF THIS POLICY

This policy applies to all information and information assets supporting Information Communication Technology (ICT) and Operational Technology (OT) assets that are owned, managed or operated by Council.

## 4. ACCOUNTABILITY AND RESPONSIBILITIES

### Roles and Responsibilities

4.1 All personnel are responsible for appropriately using the information and information systems provided to them and following defined business processes to protect the security of information.

4.2 Information Management Steering Committee is ultimately responsible for the management of information risk.

4.3 The Executive Leadership Team and Management Group are collectively and individually accountable for meeting the requirements of this policy by:

- Setting direction and leading by example.
- Ensuring that Information risk activities are appropriately resourced and coordinated and include representatives from different parts of the business.
- Developing and maintain processes to ensure that the requirements of this Policy as well as any regulation or contractual requirements specifically applicable to their business are met.
- Ensuring that this Policy and associated procedures are communicated and accessible to all personnel and relevant external parties.
- Ensuring that change initiatives do not weaken Strathbogie Shire Council's information risk profile.

4.4 The Manager Digital Innovation and Technology is responsible for:

- Implementing an Information and Communications Technology (ICT) strategy that is aligned to industry standards (e.g. ISO 27001) where possible.
- Maintaining relationships with relevant external bodies (e.g. Victoria Government Information Security Practice, other councils, law enforcement, industry groups, Municipal Association Victoria, and other State Government Agencies).
- Investigating breaches of this policy and associated procedures

### All Personnel Accountabilities

4.5 Reasonable steps must be taken to protect the confidentiality, integrity and availability of Strathbogie Shire Council information and information system assets.

### Management Accountabilities

4.6 Information risks must be identified, assessed and monitored and reported, accepted and / or acted upon in accordance with the Strathbogie Shire Council Risk Management Policy and associated Framework.

4.7 Personnel must be suitable for the roles for which they are being considered and be aware of their responsibilities for ensuring security and quality of Strathbogie Shire Council information.

4.8 Information and systems must be classified and handled in accordance with the level of confidentiality of the information.

4.9 Access to information must be restricted to those parties with a business "need to know" through appropriate authentication mechanisms, with no individual able to perform all roles or functions within an end-to-end process.

4.7 Information and systems must be protected from unauthorised physical access, damage, theft or compromise of assets.

4.8 Managing information risk must be an integral consideration while developing, acquiring, enhancing and decommissioning information processes and systems.

**Manager Digital Innovation and Technology Accountabilities**

4.9 Cryptographic Keys and certificates used to protect information must be managed and secured throughout their lifecycle.

4.10 Changes to production systems must be appropriately approved, tested and implemented, with information and information systems protected through separation of production and non-production environments.

4.11 Systems availability must be protected through management of configuration, capacity, events, incidents and problems, supported by resilience and recovery controls.

4.12 Ongoing and emerging information security threats and vulnerabilities must be identified, assessed and responded to in a timely manner.

4.13 Key security–related events must be logged and monitored.

4.14 Backups of information and information systems must be taken, stored securely and periodically tested.

4.15 The security of Strathbogie Shire Council's Network must be protected.

## 5. POLICY EXEMPTIONS

5.1 Policy exemptions are required where the business is unable to comply with the mandatory requirements of this Policy and its related Standard Operating Procedures, and immediate action cannot be taken to achieve compliance. In this context, mandatory requirements are the 'must' and 'must not' statements.

5.2 Policy exemption requests must be submitted to the Policy Owner for review and will be forwarded to the Chief Executive Officer for approval at their discretion.

5.3 In case of a conflict or inconsistency between this Policy and the laws and regulations of Victoria/Australia, those laws and regulations take precedence to the extent of the conflict or inconsistency, unless this Policy places a higher requirement, especially if compliance with this Policy would result in a breach of the local legislation or regulation. The Policy Owner must be informed if any such conflict or inconsistency exists.

## 6. POLICY BREACHES

6.1 Breaches of this Policy and related Standard Operating Procedures (i.e. non-compliance that is not managed via the formal exemption process) must be managed in accordance with the Strathbogie Shire Council Staff Code of Conduct CEO Directive.

6.2 All instances of breaches of this Policy must be communicated immediately to Manager Digital Innovation and Technology. Any **material** or **systemic** breach of this Policy must be communicated to the Manager Digital Innovation and Technology and appropriate remediation measures agreed and implemented.

## 7. DEFINITIONS

| Term | Meaning |
|---|---|
| Information | covers both information and data |
| Information security | refers to the confidentiality, protection, integrity, and availability of Strathbogie Shire Council information, information systems and networks. |
| Council | means the Strathbogie Shire Council |

## 8. RELATED POLICIES AND LEGISLATION

The following Council, State, regional and national plans and policies are relevant to this policy under each subtitle.

- *Copyright Act 1968*
- *Fair Work Act 2009 (Commonwealth) – Human Resources policies*
- *Freedom of Information Act 1982*
- *Local Government Act 2020*
- *Victorian Equal Opportunity Act 1995 (or Australian Human Rights Commission Act 1986)*
- *Privacy and Data Protection Act 2014* (Vic)
- *Public Records Act 1973* (Vic)
- *Spam Act 2003*
- *Electronic Transactions Act 2001*
- ISO 27001:2015 aligned

### 2. Related Documents

- Staff Code of Conduct CEO Directive
- Councillor Code of Conduct
- Information Security Procedures
- Media Policy
- Social Media Policy
- Records Management CEO Directive
- Transfer of Council Records to Places of Deposit Policy
- Fraud and Corruption Policy
- Privacy and Data Protection Policy
- Mayor and Councillor Correspondence CEO Directive
- ICT Change Management Policy
- ICT Change Management Framework
- Risk Management Policy
- Enterprise Risk Management Framework
- Employment contracts and associated records

## 9. POLICY REVIEW

Council may review this policy at any time and at least two years from the date of adoption.

Minor amendments to the policy may be authorised by the CEO at any time where such changes do not alter the substance of the policy (e.g. a change to the name of a related document, or a change in legislation).