# Cyber Security Governance Policy

| | |
|---|---|
| Policy Number | A7 |
| Responsible Officer(s) | Chief Executive Officer;<br>Manager People & Governance. |
| Policy Adopted | October 2023 |
| Next Review Date | October 2027 |
| Minutes reference | 2023/10-07 |
| Applicable Legislation | *Privacy Act* (Cth) *1988; Privacy Amendment (Notifiable Date Breaches) Act* (Cth) *2017; Crimes Act* (Cth) *1914; Security of Critical Infrastructure Act* (Cth) *2018; Telecommunications (Interception and Access) Act* (Cth) *1979; Local Government Act* (SA) *1999.* |
| Related Policies | Risk Management Policy; ICT Acceptable Use Policy; Records Management Policy; Emergency Management Policy. |
| Related Procedures | Data Breach Response Plan; Business Continuity Plan. |

## 1. POLICY PRINCIPLE

Wakefield Regional Council's Cyber Security Governance Policy aims to protect its information and communications technology (ICT) systems and electronic information from security threats ('information security'). The policy supports Council and community resilience, and compliance with obligations in relation to information security.

## 2. POLICY OBJECTIVE

- Effectively manage the risks associated with information security threats to Council
- Respond effectively to information security incidents.
- Continuously improve management of information security risks.

Implementation of the policy does not eliminate risks, however it reduces the likelihood and consequences if a risk materialises.

## 3. DEFINITIONS

| | |
|---|---|
| ***Confidentiality*** | The restriction of access to information by authorised persons, entities and processes at authorised times and in an authorised manner. |
| ***Integrity*** | Safeguarding the accuracy and completeness of information and information processing systems. |
| ***Availability*** | Ensuring that authorised users have access to information and associated assets when required. |
| ***Information Security*** | Preservation of confidentiality, integrity and availability of information. |

| | |
|---|---|
| ***Personal Information*** | Information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion. |
| ***Information & Communications Technology (ICT) Assets*** | Any item of value including ICT equipment, services, software, information or data. |

## 4. POLICY DETAIL

This policy applies to all ICT assets to the extent that Council has management responsibility or control of those assets.

### 4.1 Key Stakeholders

Stakeholders in the management of information security include:

- Public and community
- Ratepayers
- Council employees
- Council Members
- Suppliers
- Contractors (accessing ICT system or information)
- Volunteers (accessing ICT systems or information)
- Providers of ICT systems and services to Council
- Other government organisations.

### 4.2 Governance

Key elements of this information security governance policy include:

- Roles and responsibilities
- Culture, awareness and training
- Risk management
- Protection
- Responding to breaches
- Monitoring and reporting
- Insurance

### 4.3 Roles and Responsibilities

- Council approves the Information Security Governance Policy.
- The Risk and Audit Committee provides oversight of management of information security risks.

- The Chief Executive Officer ensures the Information Security Governance Policy is implemented and maintained.
- The Chief Information Security Officer[1] is responsible for implementing and maintaining the information security governance policy across Council.
- The Senior Leadership Team is responsible for defining information security risk appetite and risk tolerance.
- The Senior Leadership Team is responsible for leading information security and information privacy capability development and ensuring compliance with the information security policies and procedures.
- All Council Members, employees, volunteers, and contractors and ICT suppliers must maintain awareness of information security and comply with information security policies and procedures.
- Responsibilities for management of information security risks are assigned, managed and integrated within Council's risk management framework.

### 4.4 Culture, Training and Awareness

- The Senior Leadership Team actively fosters a culture of information security.
- Staff training and awareness initiatives in relation to information security are undertaken regularly and where necessary in response to particular concerns or risks.
- Council is kept informed of risks and issues associated with information security.

### 4.5 Risk Management

Information security risks are managed in accordance with Council's Risk Management Policy. This includes:

- Council defines its risk appetite and risk tolerance in relation to identified information security risks.
- Council maintains records of all ICT assets for which it has management responsibility and/or control.
- An assessment of the importance (i.e. impact if compromised) is undertaken for core ICT asset managed or controlled by Council.
- The confidentiality, integrity and availability requirements for key ICT assets are determined and documented.
- Information security risk assessments are undertaken for key Council ICT assets, and regularly reviewed throughout the life of the system.
- Security and privacy risk assessments include assessments of Council's ICT providers.
- Information security risk management requirements are incorporated into procurement processes and contracts and are actively managed in contracts.
- Council applies the Key Reference Documents at Section 5 where guidelines are required in relation to identifying and managing specific information security risks.
- Information security risks are monitored, and status reported to the Risk and Audit Committee in accordance with Council Risk Management Framework.

[1] Australian Cyber Security Centre, Information Security Manual in the context of a Regional Council.

- Independent specialists are engaged as required to advise on information security risk management.
- At a minimum an annual review of information security risks is undertaken and status of risks reported to the Risk and Audit Committee.
- Information security risks, controls and treatments are managed and fully integrated within Council's risk management programs.
- The ongoing effectiveness of control measures for information security risks is monitored, reviewed and reported.
- Risks that fall outside tolerance are escalated to the Risk and Audit Committee.

### 4.6 Protection

Council implements the following baseline measures to protect and mitigate against information security breaches:

- Progressive implementation of the information security mitigations in accordance with the requirements of the Australian Cyber Security Centre Essential 8 Maturity Model at a level of maturity based on assessment of risks (for Microsoft Windows based systems). As a guide Level 2 Maturity will generally be targeted.
- Implementation of appropriate systems to monitor, detect, alert and respond to information security attacks including email attacks.
- Information security procedures aligned with the guidelines provided within the Australian Cyber Security Centre, Information Security Manual, 10 March 2022 and subsequent revisions as applicable to Council risk context.
- Inclusion of information security requirements and enhancements within the ICT Strategic Plan and budgets.
- Inclusion of information security requirements in all relevant procurement contracts.
- Regular reporting of progress with the implementation of information security control measures to the Audit and Risk Committee.
- Monitoring of information security measures in place with suppliers of ICT services.
- Monitoring of Australian Cyber Security Centre alerts and advisories, initiating timely action as required to address issues raised.

### 4.7 Responding to Breaches

Council establishes and regularly tests the following plans in relation to information security breaches (or suspected breaches):

- Data Breach Response Plan
- Emergency Management Plan (for critical ICT systems)
- Business Continuity Plans (inclusion of ICT systems)
- Response plans are enacted by Council as appropriate.

Reporting of information security breaches to relevant authorities and impacted parties within stipulated timeframes is undertaken. Privacy breaches are reported in accordance with the Data Breach Response Plan.

### 4.8 Monitoring and Reporting

Council monitors the effectiveness of the Information Security Governance Policy and reports performance to the Audit and Risk Committee annually.

This policy shall be reviewed in the case of:

- Significant changes to the information security risk context
- An information security incident occurring associated with a High or Extreme Risk.

Cyber security incidents, and suspected incidents, associated with risks classified as High or Extreme shall be reported to the Audit and Risk Committee.

### 4.9 Exemptions

Exemptions from this policy must be approved by the Chief Executive Officer.

### 4.10 Insurance

Council maintains cyber security insurance through Local Government Risk Services.

### 4.11 Information Privacy Breaches

Information privacy breaches (including those resulting from an information security breach) are managed in accordance with this policy and Council's Data Breach Response Plan.

## 5. REFERENCES

Council aligns its information security policy with the following as applicable to the Council context:

- Australian Cyber Security Centre, Information Security Manual, 10 March 2022 and subsequent revisions.

Other standards relevant to this policy include:

- AS/NZS 5050:2010 Business Continuity – Managing Disruption Related Risk.
- AS ISO 31000:2018 Risk Management Standard.
- ISO/IEC27001:2013 Information Security Management.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

Council aligns its information security risk mitigation strategies with the following:

- Australian Cyber Security Centre, Strategies to Mitigate Cyber Security Incidents, February 2017 and subsequent revisions.
- Australian Cyber Security Centre, Essential Eight Maturity Model, November 2022 and subsequent revisions (Microsoft Windows internet connected systems only).

## 6. REVIEW

This Policy shall be reviewed every 48 months, or more frequently if required by legislation or Council.

**Document history:**

| Version | Adopted | Description of Change |
|---|---|---|
| 1.0 | October 2023 | New Policy |