Policy number	Policy 331
Policy title	Information Systems Security
Strategic outcomes supported	CL04 - Appropriate information management that is easily accessible, accurate and reliable.

POLICY OBJECTIVE:

To set a multi-pronged approach in place to protect the data and systems of the Town. This includes robust practices to provide for business continuity in the event of a disaster.

The Town of Victoria Park (the Town) has a strategic priority to implement an Information Security Management System (ISMS). An ISMS consists of a suite of policies, procedures, guidelines and relevant resources to manage all information assets.

The strategic objectives are drawn from the Western Australian Whole of Government Digital Security Policy, published in June 2017.

POLICY SCOPE:

The scope of the policy is the management of digital and physical information security and access in the context in which information is created and managed.

DEFINITIONS:

Nil.

POLICY STATEMENT:

IS Security Strategic Plan

1. The Town has implemented the IS Security Strategic Plan which includes the adherence to the Australian Signals Directorate's (ASD) Essential Eight as part of its security tool kit and then plans to implement ISO 27001 (Information technology -- Security techniques -- Information security management systems – Requirements) in the future.

2. The ASD Essential Eight is one of many tools to enable the Town to enable cyber resilience focusing on two areas:
   a. Preventing malware from running in the environment; and
   b. Limiting the extent of security incidents, and being able to recover data.

Cyber Security

3. The CEO will ensure the following security objectives for the Town are maintained:
    a. Develop and continuously improve security management practices
    b. Empower our staff, partners, and communities to be strong links in our overall security chain through collaboration and enablement
    c. Enable innovation while effectively identifying and managing cyber risks

Digital security

4. The CEO will ensure the application and management of controls are in place to ensure that the right information is available when ever required by staff with the appropriate access permission and the confidentiality and integrity of information is secured.

Information Privacy

5. In accordance with the Information Privacy Principles of the *Privacy Act 1988* (Cth) the Town has developed a Privacy Statement. The Town adheres to the provisions of the *Freedom of Information Act 1992* (WA).

Information access

6. Staff, contractors and consultants may, subject to appropriate permissions and authority, have access to the Town's records to fulfil their duties and obligations.

7. The CEO will ensure measures are in place to ensure the security of its records, both hard copy and electronic, and authorised access to them. Reference to Security and Access have been documented in the Town's Record Keeping Plan.

Public access documents

8. The CEO will ensure that regular identification of Councils documents for public access purposes is followed to increase greater communication with the community, this may have a positive effect by reducing Freedom of Information applications submitted to the Town.

Security of physical documents

9. The management of physical records has been outlined in the Town's Record Keeping Plan.

Third Party Information Access Permissions

10. The CEO will ensure that access to Corporate Information / Networks / Business System will be refined to ensure all appropriate security measures are in place.

11. The term 'third party' refers to various forms of external hire of labour and specialists such as contractors, consultants, Trainees, Work experience students and various specialists such as IS support and other vendors etc.

12. When providing access to the network/business systems the CEO will consider the following:
    a. Signing a confidentiality agreement restricting the use and dispersal of confidential information
    b. Documented permissions standards appropriate to fulfil duties and obligations as per contract/terms of reference.
    c. Procedures to identify what type of third party should gain access the type and how much access to systems should a third party gain to perform their duties as required.
        i. Contractor – location and reporting level, develop appropriate criteria if applicable
        ii. Consultant – location and reporting level, develop appropriate criteria if applicable
        iii. Trainees
        iv. Work experience students
        v. IS - Software vendors and support etc.
        vi. Include – mobile devices such as laptop, tablets, and other mobile devices – thumb drives etc.
        vii. Induction training
        viii. Comply with all aspects of relevant policies – e.g. IS policy – which includes conditions of use for mobile devices, standards, guides, references, practices and procedures.

RELATED DOCUMENTS:

- ICT Strategic Plan
- Information and Communications Technology Asset Management Plan (as part of the Integrated planning and reporting framework)
- Information Statement

Policy manager	Manager – Corporate Services
Approval authority	Council
Next Evaluation Date	

REVISION HISTORY

Version	Approved, Amended, Rescinded	Date	Authority	Resolution Number	Key Changes/Notes
1	Approved		Council		

.