Third

OBJECTIVES

The objective of this standard is to ensure the City of Greater Geraldton's (City) data it owns with is supported by adequate security controls when or is supplied Services by third parties.

STANDARD STATEMENT

To the extent that authorised third parties (contractors, their personnel, and subcontractors) transmit, process, store, create or access City data and IT systems there exists an obligation to protect City data and systems from unauthorised access, copying, reproduction, transfer, dissemination, destruction, deletion, corruption or alteration by any person or organisation.

This standard applies to all such authorised third parties with the Data Security Standard and is in addition to any general conditions of contract or service agreement.

Standard Details for Third Parties

Minimum Security Controls

-
- Standard and Requirements and Good Industry Practice
- Ensure that all its its information security policy as would be expected of their role
- into the City's Data

Where City data traverses third party :

- Implement and maintain a method to r, detect, investigate, and remediate intrusions and incidents of their
- Ensure that City Data is encrypted to protect it from unauthorised use or disclosure while in transit, in storage or at rest.
- Scan its IT Trojans or spyware.
-
- Ensure vendor default passwords and security keys are not used
- Implement multi-factor authentication for remote access to its IT systems.
- Align with the principals of least privilege and role based access when configuring user access and accounts.

- which relate to the access or use of City Data are kept for a minimum of twelve (12) months
- in its IT Systems
- Implement vulnerability management processes that includes performing routine vulnerability scans on its IT Systems and if requested by the City, provide executive reporting on relevant findings
- Develop and maintain an ability to detect and respond to security threats
- Develop and maintain change management processes to control any changes that relate to its IT Systems used to provide the Services
- [illegible] processing data resides on or back-up system used to provide the Services
- Provision and maintain appropriate firewalls, anti-malware and intrusion detection software to protect all its IT Systems
- Regularly undertake [illegible] its IT Systems and at the request of the City, provide executive reporting on relevant findings
- Ensure all City Data is kept within Australia unless otherwise approved by the City

Where the Services provide internet facing IT Systems traversed by City Data the following must be configured:

- Strong cryptographic protection for data in transit such as HTTPS using TLS 1.2 or better
- Not
- Prevent administration of the internet f[illegible] agreed by the City *and* provisioned with Multi-Factor Authentication
- Comply with Good Industry Practice security settings in relation to the Service's being exposed to the Internet

Secure Development

- Where there is a requirement to develop code to provide the Services it must comply with Secure by Design Principles such as OWASP or other Good Industry Practices

Vulnerability Management

If an actual or potential security vulnerability which may cause a Data Defect or Data Breach, is publicly known, identified by the third party, or notified to the City to the third party

- Validate the potential exposure of City actual, or potential security vulnerability.
- Take [illegible] reasonably commensurate with the risk associated with the vulnerability, with the risk assoc
-

-

Security Breaches and Incident Investigation Support

In the event of an incident or potential Data Breach that impacts City Data

- Contact the City
- A
  logs
-
  Data Breach

Third Party Personnel

Where third parties have personnel who have access to City Data or IT Systems

- They perform background checks on these personnel
-
-
- Notify the City of any changes to employment statu
  Data and IT Systems can be revoked

Right to Audit

-
  controls and protections implemented by the third party
  Requirements. A report associated with the assessment will be provided to both the City and the Contractor.
- Remediate any items of non-compliance noted in the report
  with remediation are to be borne by the third party.

Right to Scan

- i facing IT Systems it is asserted that the City may perform scheduled and automated scans on such Systems for the purpose of validating security

Return or Destruction of Data upon Service Disengagement

- third party agrees to return or destroy all City Data held by
  one (1) month of a request by the City.
- The third parties
  remnant of City Data that cannot be

KEY TERM DEFINITION

- **CVSS** means Common Vulnerability Scoring System (CVSS) which is a free and open industry [illegible] [illegible]
- **City** [illegible]
- **City Data** means information which is provided to the third party (including its subcontractors) for the purpose of providing or utilising [illegible]
- **Contractor's Information Security Policy** is [illegible] own Information Security Policy or [illegible] Data Security Standard
- **Contractor** is a third-party [illegible]
- **Data Breach** [illegible] City's Data.
- **Data Defect** – [illegible] third party while providing the Services.
- [illegible]
    - [illegible]
    - ISO27001;
    - [illegible]
    - [illegible]
- **IT Systems** [illegible] means any information technology infrastructure used by a party, that stores, processes, [illegible] Subcontractors that stores, [illegible]
- **Internet Facing IT Systems** – IT Systems that are accessible via a publicly accessible internet IP [illegible]
- **Services** – [illegible] (s) provided to the City under an agreement and includes any incidental activities or [illegible] Services.
- **Subcontractor** [illegible] who is not an employee of the Contractor who is required [illegible]
- **Third Party** is anybody not an employee of the City or any business not owned by the City of Greater Geraldton

ROLES AND RESPONSIBILITIES

Manager [illegible]

- [illegible] standard and ensure it is being complied with
- Approve variations or amendments to this standard.

All Staff

- [illegible] stored, processed, or created.

Third Parties

- [illegible]

WORKPLACE INFORMATION

- Council Policy CP4.6 Information Security Management System
- Privacy Act 1988
- [illegible]

STANDARD ADMINISTRATION

Branch	Officer	Version		
Cybersecurity	Manager ERP and Cybersecurity	2.0	Bi-Annual	2026