



## Third

### OBJECTIVES

The objective of this standard is to ensure the City of Greater Geraldton's (City) data it owns with is protected when it is stored, processed, transmitted or is supplied Services by third parties.

### STANDARD STATEMENT

To the extent that authorised third parties (contractors, their personnel, and subcontractors) in the 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 remains in addition to any general conditions of contract or service agreement.

#### Standard Details for Third Parties

##### Minimum Security Controls

- 
- Standard 5 and Requirements and Good Industry Practice
- Ensure that all its policy as would be expected of their role
- its information security into the City's Data

##### When the City Data traverses this party:

- Implement and maintain a method to monitor, 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 Systems for Trojans or spyware.
- Ensure all remote access to its IT systems is protected with a secure connection
- 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 audit logs when configuring IT services 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
- Ensure all data is protected by a secure process to protect data by the Service Provider or a specialist data storage 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
- Support and maintain all services that its IT Systems and at the request of the City, provide executive reporting on security incidents
- 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 facing IT Systems to be restricted to the City and agreed by the City and provisioned with Multi Factor Authentication
- Comply with Good Industry Practice security settings in relation to the Service 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 reasonable steps to mitigate the risk associated with the vulnerability with critical services reasonably commensurate with the risk associated with the vulnerability, and the risk associated
-



- ~~Assist the City's internal or external incident investigations by providing access to relevant audit logs, user access logs and~~

### Security Breaches and Incident Investigation Support

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

- ~~Contact the City.~~
- ~~Assist the City's internal or external incident investigations by providing access to relevant audit logs, user access logs and~~
- ~~Data Breach~~

### Third Party Personnel

~~When third parties have personnel who have access to City Data or IT Systems:~~

- They perform background checks on these personnel
- ~~And submit the results to the City's internal information for Third party data security standard~~
- ~~Ensure the Personnel and subcontractors report any suspected incidents to a compliance officer who will then report to the City.~~
- ~~Notify the City of any changes to employment status of the personnel who have access to City Data and IT Systems can be revoked.~~

### ~~Right to Audit:~~

- ~~For IT systems of the City owned or operated by a contractor, the contractor will provide the City with access and 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 and act as a third party data security noted in the report with remediation are to be borne by the third party.~~

### Right to Scan

- ~~When a contractor is providing IT services to the City and is providing IT Systems it is assented that the City may perform scheduled and automated scans on such Systems for the purpose of validating security controls and protections implemented by the third party~~

### Return or Destruction of Data Service Disengagement:

- ~~When a contractor is providing IT services to the City and is providing IT Systems it is assented that the City may perform scheduled and automated scans on such Systems for the purpose of validating security controls and protections implemented by the third party~~
- ~~The third party agrees to return or destroy all City Data held by the contractor on or before the date of the request (1) month of a request by the City.~~
- ~~The third parties computer operations to be deleted with all information privately held and not to be any remnant of City Data that cannot be offered back to the City return or destroyed such as~~



## KEY TERM DEFINITION

- **CVSS** means Common Vulnerability Scoring System (CVSS) which is a free and open industry standard for measuring the severity of information security vulnerabilities. You can find more information on the CVSS website at <http://www.firstmonks.com>
- **City** means the City of Greater Geraldton
- **City Data** means information which is provided to the third party (including its subcontractors) for the purpose of providing or utilising the services
- **Contractor's Information Security Policy** is the Contractor's own Information Security Policy or Information Security Management System used to comply with this Data Security Standard
- **Contractor** is a third-party contractor who has been authorised by the City to provide Services
- **Data Breach** means unauthorised access, use, disclosure, access, damage or destruction of the City's Data.
- **Data Defect** – means a data security breach of City Data, or where City Data has been accessed by a third party while providing the Services.
- **Payment Card Industry Data Security Standard** means the Payment Card Industry Data Security Standard, which includes:
  - Payment Card Industry Security Standards; Payment Card Industry
  - ISO27001;
  - Any other standard agreed between the City and the Contractor
- **IT Systems** means any information technology infrastructure used by a party, that stores, processes, or uses any City Data, or is used by the Contractor's Personnel or Technology Infrastructure Subcontractors that stores, processes, or uses any City Data
- **Internet Facing IT Systems** – IT Systems that are accessible via a publicly accessible internet IP address
- **Services** – the service (s) provided to the City under an agreement and includes any incidental activities or ancillary services provided in relation to the Services.
- **Subcontractor** means any party who is not an employee of the Contractor who is required to provide services or assistance to the Contractor in providing Services to the City
- **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

- **Ownership** – ensure the standard is being complied with
- **Approve** variations or amendments to this standard

### All Staff

- **Compliance** – ensure that all data supplied to the City is protected in accordance with this standard, stored, processed, or created.

### Third Parties

- **Compliance** – ensure compliance with this Standard

## WORKPLACE INFORMATION

- **Council Policy CB46 Information Security Management System**
- **Privacy Act 1988**
- **Personal Information Protection Act**



## STANDARD ADMINISTRATION

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