City of Greater Geraldton

Third Party Data Security Standard

ISMS Policy Principles

Confidentiality – Integrity – Availability – Need-to-know – Least privilege

ICT Strategic Plan Principles

Built in Security and Risk Management

OBJECTIVES

The objective of this standard is to ensure the City of Greater Geraldton's (City) data it owns or is entrusted with is protected when the organisation interacts with 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 and compliance with the Data Security Standard requirements are in addition to any general conditions of contract or service agreement.

Standard Details for Third Parties

Minimum Security Controls

- Maintain and enforce its own security practices, procedures and policies and;
- Ensure these policies are regularly reviewed and updated to align with the City's Data Security Standard Requirements and Good Industry Practice; and
- Ensure that all its personnel are provided with training on the requirements of its information security policy as would be expected of their role
- Ensure that no errors, whether typographical, logical or otherwise, are introduced by its personnel into the City's Data

Where the City's data traverses third party IT Systems:

- Implement and maintain a method to monitor, detect, investigate, and remediate intrusions and incidents of their IT Systems
- 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 malware such as viruses, worms, Trojans or spyware.
- Ensure all software programs used to provide the Services are supported and maintained
- Ensure vendor default passwords and security keys are not used and passwords are not duplicated
- Ensure vendor products provide secure software update mechanisms
- Ensure vendor products have a vulnerability disclosure policy
- Implement multi-factor authentication for all remote access to its IT systems.

- Align with the principals of least privilege and need to know when configuring user or service accounts
- Ensure audit logs which relate to the access or use of City Data are kept for a minimum of twelve (12) months
- Routinely apply patches and/or workarounds as per vendor requirements to address vulnerabilities in its IT Systems
- Implement a vulnerability management program 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 physical security is maintained by means of access control, locks and alarms for any business premises, data centre, server 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
- Perform penetration testing on all 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 third party or a provided service communicates over email:

- Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) in either quarantine or reject mode for any internet domain used by email
- Ensure any service sending email on behalf of the City is secured with DMARC including both DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) mechanisms.

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 expose software versions in protocol headers or error pages
- Prevent administration of the internet facing IT Systems from the internet, unless otherwise agreed by the City *and* provisioned with Multi Factor Authentication
- Comply with Good Industry Practice in the configuration of 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 by the City to the third party

- Validate the potential exposure of City Data or IT Systems to the identified, actual, or potential security vulnerability.
- Take reasonable steps to mitigate the risks associated with the vulnerability within timeframes reasonably commensurate with the risk associated with the vulnerability; and
- If the vulnerability is rated with a CVSS Score of 8 or above, on request from the City, provide a remediation plan demonstrating the steps being taken to mitigate the risk associated with the vulnerability.

PCI Standards Compliance

If the PCI Standards apply to any of the provided Services.

- Comply with the PCI standards
- Maintain a certification to confirm it is compliant with the PCI standards
- Agree in writing they are responsible for the security of the cardholder data they store or process on behalf of the City

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 upon request, relevant audit logs, or access to such logs
- Comply with all reasonable directions of the City in relation to responding to an actual or suspected 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
- Inform the Personnel and subcontractors to abide by the City's Third-party data security standard
- Ensure the Personnel and subcontractors report any suspected incidents or vulnerabilities which could impact City Data
- Notify the City of any changes to employment status such as the termination of employment or subcontractor to ensure access to City Data and IT Systems can be revoked

Right to Audit

- At the cost of the City, allow an appropriate auditor or specialist appointed by the City to assess the controls and protections implemented by the third party to comply with the City's Data Security Requirements. A report associated with the assessment will be provided to both the City and the Contractor.
- Remediate any items of non-compliance with this Data Security Standard as noted in the report within a reasonable, mutually agreed timeframe. Any costs associated with remediation are to be borne by the third party.

Right to Scan

- Where City Data is stored or processed on internet facing IT Systems it is accepted that the City may perform scheduled and automated scans on such Systems for the purpose of validating security controls and protections against security vulnerabilities and misconfigurations.

Return or Destruction of Data at Service Disengagement

- Unless otherwise agreed by the City, the third party agrees to return or destroy all City Data held by the Contractor or subcontractors, in relation to the agreement, within one (1) month of a request by the City.
- The third parties agree to continue to comply with this data security standard to protect any remnant of City Data that cannot be feasibly returned or destroyed such as offline backups.

KEY TERM DEFINITION

- **CVSS** means Common Vulnerability Scoring System (CVSS), which is a free and open industry standard for assessing the severity of information technology system security vulnerabilities and can be found at the following link: https://www.first.org/cvss/.
- **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 entity which has been authorised by the City to provide Services
- **Data Breach** means unauthorised copying, use, disclosure, access, damage or destruction of the City's Data.
- **Data Defect** – means any error, corruption, loss of City Data, or where City Data has become functionally disabled in each case because of anything done or omitted to be done by the third party while providing the Services.
- **Good Industry Practice –** any relevant industry standards either published or defacto relating to the security of information systems including the standards prescribed by but not limited to:
    - Payment Card Industry Data Security Standards;
    - ISO27001;
    - Open Web Application Security Project (OWASP);
    - Or any other standards agreed between the City and the Contractor
- **IT Systems** – means any information technology infrastructure used by a party, that stores, processes, transmits, or accesses City Data (and, in the case of the Contractor, includes any information technology infrastructure used by the Contractor's Personnel or Subcontractors that stores, processes, transmits, or accesses 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 work related to the provision of the Services.
- **Subcontractor** – Any person or company who is not an employee of the Contractor who is required to provide goods or services to the City under the agreement
- **Third Party i**s anybody not an employee of the City or any business not owned by the City of Greater Geraldton

ROLES AND RESPONSIBILITIES

Manager ICT Services

- Oversee this standard and ensure it is being complied with
- Approve variations or amendments to this standard

All Staff

- Ensure this standard is appended to all City contracts where City data is to be accessed, transmitted, stored, processed, or created.

Third Parties

- Apply and comply with this Standard

WORKPLACE INFORMATION

- Council Policy CP4.6 Information Security Management System
- Privacy Act 1988
- Recordkeeping Act

STANDARD ADMINISTRATION

Branch	Officer	Version	Review Cycle	Next Due
ICT Services	Manager ICT Services	1.2	Bi-Annual	October 2024