Gladstone Ports Corporation

Growth, prosperity, community.

Cybersecurity and Information Management Requirements for Suppliers and Vendors

Brief description

This site standard defines GPC's high-level Cybersecurity and Information Management requirements for suppliers and vendors.

Document information	
Current version	#1661613v3
First released	17/11/2020
Last updated	23/12/2024
Review frequency	Every 2 years or as required
Review before	30/11/2026
Audience	All GPC Representatives / Officers / General Manager / Managers / Superintendents / Supervisors / Leaders / Employees / Suppliers / Consultants / Vendors / Sub-contractors

Document accountability	
Role	**Position**
Owner	Chief Financial Officer (CFO)
Custodian	Technology and Cybersecurity Manager

Endorsed by	Chief Financial Officer 07/04/2021

If you require any further information, please contact the Custodian.

The current version of this Specification is available on GPC's Intranet.

Contents

1 Terms and definitions

"ASD/ ACSC" means Australian Signals Directorate/ Australian Cyber Security Centre.

"Confidential Information" means:

(a) all information (in any form) relating to the Principal made available to the Supplier at any time in connection with the Services;

(b) any information that concerns the business, operations, finances, plans, Personnel or customers of the Principal, which is disclosed to or acquired by the supplier (including any information that is derived from such information),

but does not include information which was in the Supplier's possession prior to the date of the engagement, provided that this will not include any information that was provided directly or indirectly by the Principal to the supplier or which is the subject of an obligation of confidence.

"Data breach" means unauthorised access to sensitive or personally identifiable information.

"GPC" means Gladstone Ports Corporation.

"Information Management" means the way by which an organisation plans, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains and disposes of its information; as well as any means through which the organisation ensures that the value of that information is identified and exploited to its fullest extent.

"Information Security" or **"Cybersecurity"** describes the concepts, techniques, measures (technical and administrative) used to protect information assets from deliberate or inadvertent unauthorised acquisition, damage, disclosure, manipulation, modification, loss, or use.

"**NIST Cyber Security Framework**" means the Framework for Improving Critical Infrastructure Cybersecurity published by the US National Institute of Standards and Technology (as amended and updated from time to time).

"**Principal Data**" means all data and information relating to the Principal and its operations, customers, Personnel, suppliers, assets, products, sales and transactions, in whatever form that information may exist, including any data produced, generated or processed in the provision of the Services. It includes any database in which that data or information is contained, any documentation or records related to that data or information, any products (including new data or information) resulting from the use or manipulation of that data or information, any other data and other information entered into, generated by, stored by, or processed by any of the Principal's equipment.

"**Security Incident**" means an incident, event or problem which could result in an actual or potential compromise of the confidentiality, integrity or availability of Principal Data, the Services or the Supplier's own information systems.

"Supplier" means vendors and suppliers and any other worker engaged under the direct management of GPC (for example, contractors, sub-contractors, Consultants, agency resources and volunteers) providing goods, services or materials to GPC under contract or other form of engagement.

"SOC1" or **"SOC2"** means the Service Organization Controls standards.

"ISO/IEC27001:2022" means Information security, cybersecurity and privacy protection — Information security management systems — Requirements and provides guidance for establishing, implementing, maintaining and continually improving an information security management system.

2 Introduction

This site standard defines GPC's high-level Cybersecurity and Information Management requirements for suppliers and vendors. Suppliers are to supply relevant information as per this site Standard.

2.1 Purpose

The purpose of this document is to ensure GPC's information is protected and legislative obligations are met in the delivery of goods or services to GPC.

2.2 Scope

This site standard applies to all GPC employees, vendors and suppliers, visitors and, unless otherwise specified, any other worker engaged under the direct management of GPC (including, contractors, sub-contractors, consultants, agency resources and volunteers). Defined risk management requirements for external entities engaged by GPC are in contractual arrangements and/ or rest with Suppliers to appropriately identify, assess, notify and manage risks related to GPC sites, including site-based activities. This Standard applies regardless of the application of the services or goods to all persons listed as above.

2.3 Objectives

This objective of this site standard is to provide detail to all suppliers and vendors on their requirements to safeguard GPC's information.

3 Principles and Requirements

GPC is a Critical Infrastructure Asset (under Australian legislation), and as such effective Cybersecurity and Information Management is integral to business operations and legislative compliance. Managing information security risks is integrated into GPC's enterprise risk management activities, aligning with the ISMS. GPC is committed to safeguarding its reputation and operational integrity by protecting its information assets through the principles of Confidentiality, Integrity, and Availability (CIA).

- Confidentiality (C): Restrict access to information to authorised personnel only.
- Integrity (I): Maintain accuracy and completeness of information and its processing.
- Availability (A): Ensure authorised users have access to information and resources as needed.

All data must be managed in accordance with at least one of the following cyber security standards and frameworks set out below as best suits your operations:

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
- The Australian Cyber Security Centre's Essential Eight Maturity Model.
- The United States of America's National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity.
- SOC1/2 (Service Organization Controls) standards.
- ISA/IEC 62443 Series of Standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC).

Where an above standard cannot be met by the Supplier, sufficient information security risk assessment and risk treatment processes must be in place to protect GPC's information.

3.1 Information Security

The Supplier must establish, maintain, enforce and continuously improve its security procedures and safeguards against the deliberate or inadvertent unauthorised acquisition, damage, disclosure, manipulation, modification, loss, or use of Principal Data.

The Supplier will provide the Principal at the commencement of the engagement:

(a) Transparency relating to data access and security controls.

(b) Details of the Supplier's cyber security standard/ target framework references.

(c) Where applicable, artefacts which detail the response process for any security breach.

(d) Security reporting which highlights any security incident, breach or potential breach of the Principal's data for which they have access.

(e) Notification of any data breach they incur whilst working for the Principal.

(f) Copies of internal compliance or audit results relating to the Principal's data maintenance.

The Supplier must comply with such security requirements prior to the commencement of the contract, including security requirements relating to access, and use of, any data, information systems or facilities provided by the Principal or another third party.

3.2 Incident Reporting

If the Supplier becomes aware of an Information Security incident, it must:

(a) As soon as reasonably practicable, and in any event no later than 48 hours after the security incident first occurs, notify the Principal about the security incident.

(b) Co-operate with the Principal in any investigation or audit (including by providing relevant access) in respect of the security incident.

(c) Conduct its own investigation of the security incident, implement rectification measures if an actual incident or breach occurred or an incident or breach is likely to occur, or confirm to the Principal that no actual incident or breach occurred or is likely to occur.

3.3 Data Ownership

Unless expressly agreed by the Supplier and the Principal prior to commencement of work:

(a) All Principal data is, or shall be, and shall remain, the sole and exclusive property of the Principal, and deemed Confidential Information of the Principal. Principal data shall not be:

  (i) Accessed, used or copied by Supplier or Supplier Agents other than in connection with providing the services,

  (ii) Disclosed, sold, assigned, leased or otherwise provided to third parties by Supplier or Supplier Agents, or

  (iii) Commercially exploited by or on behalf of Supplier or Supplier Agents.

(b) To the extent permitted by applicable Law, the Supplier hereby irrevocably assigns, transfers and conveys, and shall cause Supplier Agents to assign, transfer and

convey, to Principal without further consideration all of its and their right, title and interest in and to the Principal data.

(c) Upon the Principal's request, the Supplier shall execute and deliver, and shall cause Supplier Agents to execute and deliver, any financing statements or other documents that may be necessary or desirable under any Law to preserve, or enable Principal to enforce, its rights under this agreement with respect to the Principal's data.

3.4 Supplier Acceptance

The Supplier undertakes and warrants that:

(a) It will ensure Principal Data is protected against misuse, interference, loss, unauthorised or unlawful access, use, modification or disclosure or accidental destruction.

(b) Only authorised Supplier's Personnel with a legitimate role in performing the Supplier's obligations under this Contract have access to the Principal Data.

(c) Upon the Principal's request, produce to the Principal or its nominee evidence of the Supplier's compliance with its obligations under clause 3.4 (a).

(d) Without limiting any other clause of this Contract (at the Principal's election) securely destroy or return all Principal Data and Confidential Information of the Principal in the Supplier's possession and control. This includes without limitation, permanently deleting or returning all devices in its possession or control used to store Principal Data or Confidential Information of the Principal, when it is no longer required by the Supplier to perform its obligations under this Contract.

(e) Leading industry standard encryption is applied to all databases that process Principal data, and electronic mail communications between the Principal and the Supplier.

(f) The Supplier's security policies, standards, guidelines, guidance notes and similar documents must address, to at least a standard of experienced and competent suppliers performing services similar to the following:

(i) Acceptable use of technology by the Supplier's Personnel.

(ii) Confidentiality.

(iii) Management of Security Incidents.

(iv) Cryptography.

(v) Identity and access management.

(vi) Management direction for information security.

(vii) Transfer of information.

(viii) Security logging and event management.

(ix) Material vulnerability management.

The Principal may, without limiting its rights or limiting the obligations of the Supplier, if it considers that there is a breach by any of the Supplier's personnel, immediately:

(a) Remove the Supplier's Personnel from the facilities of the Principal; and

(b) Deny Supplier access to the information systems of the Principal.

3.5 Business Continuity and Disaster Recovery

To ensure GPC continues to operate the services provided in the agreement, it is essential the Supplier have both a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) in place. The Supplier will confirm that BCP and DRP plans are maintained during the engagement with the Principal to ensure GPC's information remains protected.

4 Software Requirements

This section outlines the key requirements for installing software in GPC's environment to ensure all installations adhere to security, reliability, and compliance standards. Vendors and integrators must follow these guidelines to prevent introducing vulnerabilities or outdated components.

4.1 Pre-Installation Requirements

Before installing software, vendors and integrators must ensure that:

(a) All software components are compatible with the latest versions of the operating system, security tools, and other installed software.

(b) The software version is up to date (to the latest patch release). Outdated or unsupported versions are strictly prohibited.

(c) No software components or dependencies used during the installation are End-of-Support (EOS) or End-of-Life (EOL).

(d) Only required internet access is granted. Confirm and request any necessary firewall rules or internet access needed for the software.

(e) A complete list of all software components (including dependencies) along with their version numbers is submitted for review prior to installation.

4.2 Access Control and Privileges

Following the Principal of Least Privilege (PoLP), vendors and integrators must:

(a) Use the minimal privileges required during installation and ensure administrative or elevated permissions are only used when absolutely necessary.

(b) Not hardcode or store credentials in plain text within scripts or configuration files.

(c) Ensure installation actions, especially privileged operations, are logged for audit purposes.

4.3 Security and System Hardening

To maintain a high level of system hardening, vendors and integrators must:

(a) Conduct a strict component review on all software components, including third-party libraries, to ensure they are free from known vulnerabilities. Software that is approaching End-of-Life (EOL) or End-of-Support (EOS). This applies to all libraries, frameworks, and dependent components. Components with historical vulnerabilities to ensure they are updated or replaced before proceeding with the installation.

(b) Disable deprecated or insecure protocols (e.g., SSLv2, SSLv3, and TLS 1.0/1.1) and weak ciphers (e.g., RC4, DES, 3DES) and use modern encryption standards, (e.g., AES-256) and enforce TLS 1.2 or higher (with a preference for TLS 1.3).

(c) Provide a vulnerability assessment that covers all included components, detailing known risks and their mitigations and ensure all software components and dependencies are patched to address the latest vulnerabilities before installation.

(d) Request exceptions for antivirus or security software in advance (exceptions will only be granted with detailed justification and review).

4.4 Installation Best Practices

Vendors and integrators should:

(a) Install only the necessary components required for the software to function. Avoid adding optional or unused features that could introduce additional security risks.

(b) Not introduce Integrated Development Environments (IDEs) such as Visual Studio, Eclipse, or similar tools on production systems. These tools introduce unnecessary risk and expand the attack surface.

(c) Ensure all sensitive information (e.g., passwords, API keys) is securely stored and encrypted and avoid storing credentials in plain text within configuration files.

(d) Ensure software is installed in secure directories (e.g., C:\Program Files\) unless otherwise agreed upon.

4.5 Post-Installation Security Validation

After installation GPC will conduct a full vulnerability scan using enterprise-grade tools to identify outdated components, insecure configurations, and any potential risks. GPC may also subject the environment to penetration testing, especially on exposed services, encryption, and certificate handling. Vendors and integrators must:

(a) Ensure there are no outdated certificates or weak key lengths (RSA-2048 minimum).

(b) Confirm that legacy or insecure protocols (e.g., SMBv1) are disabled and replaced with modern, secure alternatives.

The vendor will be required to perform and/ or assist in rectification of findings.

4.6 Compliance and Auditing

GPC is required to maintain a level of compliance in line with ISO/IEC 27001:2022 and the ACSC's Essential Eight Maturity Model. Vendors and integrators must ensure that:

(a) The installation complies with GPC's internal security policies and relevant regulatory frameworks (e.g., ISO 27001:2022, ACSC's Essential Eight).

(b) There is a plan for ongoing patch management of all installed software components. All components must be actively supported and free of known vulnerabilities.

(c) They provide GPC with a Software Bill of Materials (SBOM), listing all components and their respective versions.

(d) Any software components or dependencies that have reached their EOL or EOS are replaced before installation.

4.7 Internal Certificates (Issued by GPC's CA)

To ensure secure communications and maintain compliance with GPC's cybersecurity standards, all certificates used for vendor-installed applications and services must use certificates issued by GPC's Certificate Authority (CA) with the following requirements:

(a) GPC will issue only Fully Qualified Domain Name (FQDN)-based certificates. Wildcard or IP address-based certificates will not be issued, and each service must have its own unique certificate. Certificates must be X.509 certificates using RSA-2048 minimum (or ECC-P-256 where applicable) and SHA-256 or stronger hashing algorithms.

(b) GPC certificates require a valid DNS entry in GPC's internal DNS infrastructure. The vendor must request a hostname resolution and use GPC's naming convention before requesting a certificate. The application or service must be accessible using this DNS name rather than an IP address.

(c) Certificates must be used with TLS 1.2 or TLS 1.3 (TLS 1.3 preferred). Weak ciphers and legacy SSL/TLS protocols (e.g., SSLv3, TLS 1.0, TLS 1.1) must be disabled.

(d) Automatic renewal mechanisms should be used to prevent certificate expiration.

4.8 Additional Security Controls

Vendors and integrators must:

(a) Utilise appropriate certificate and key management principles. Use only valid, non-expired certificates with appropriate key lengths (RSA-2048 or higher). Avoid self-signed certificates unless pre-approved. Ensure certificates are regularly updated and replaced as part of proper certificate lifecycle management.

(b) Use strong authentication. Enforce multi-factor authentication (MFA) for all administrative access to critical systems and ensure all administrative connections are made over secure, encrypted protocols (e.g., SSH, RDP with TLS).

(c) Provide adequate handover and documentation detailing the security controls applied during the installation, including encryption settings, hardening measures, and applied patches. The installation must be handed over to the internal team with a clear understanding of how to maintain and update the system.

5 Roles and Responsibilities

To assist GPC Representatives understanding their responsibilities, key responsibilities and accountabilities summarised below:

Role	Responsibilities
Board/ ELT	To ensure that GPC complies with its obligations by providing strategic direction to ensure GPC's information is protected and legislative obligations are met.
Employees and Suppliers	To ensure that GPC complies with its obligations by adhering to the requirements of this Standard and participating in internal audit and interactions with others to check compliance.
Supply Department in conjunction with Technology team and GPC contract owners	To ensure that GPC complies with its obligations by managing the inclusion of cyber security clauses in contracts, maintaining cyber security expectations in scopes of works, and checking compliance with contract terms and conditions.

6 Appendices

6.1 Appendix 1 – Related documents

(a) Legislation and regulation

Key relevant legislation and regulation, as amended from time to time, includes but is not limited to the following:

Type	Legislation/regulation/guidelines
Federal Acts	*Corporations Act 2001* (Cth) *Security of Critical Infrastructure Act 2018* (Cth) *Australian Privacy Act, 1998* (Cth)
State Acts	*Public Records Act, 2002* (Qld) *Right to Information Act, 2009* (Qld) *Information Privacy Act, 2009* (Qld) *Queensland Government Owned Corporations Act, 1993* (Qld)
Other	*ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection*

(b) Gladstone Ports Corporation documents

The following documents relate to this Specification:

Type	Document number and title
Tier 1: Policy	#1412364 Enterprise Risk and Resilience Policy #1133344 Information Policy
Tier 2: Standard/ Strategy	#829152 Enterprise Risk Management Standard #1973880 Information Management Standard #1190724 GPC Records Management Standard #1904933 Acceptable Use of Technology Standard

6.2 Appendix – Revision history

Revision date	Revision description	Author	Approved by
26/11/2020	Initial Version for Release	Daniel Topham, IS Manager	Rob Hall, Chief Financial Officer
7/1/2021	V2	Daniel Topham, IS Manager	Rob Hall, Chief Financial Officer

Revision date	Revision description	Author	Approved by
23/12/2024	V3	Scott Gimbert, IS Security Administrator	