Gladstone Ports Corporation

Growth, prosperity, community.

Cybersecurity and Information Management for Suppliers and Vendors Site Standard / Specification

Brief description

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

Document information	
Current version	#1661613v1
First released	17/11/2020
Last updated	17/11/2020
Review frequency	Every 2 years or as required
Review before	17/11/2022
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
Custodian	IS Manager

Endorsed by	Chief Financial Officer [DD]/[MM]/[YY]

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

Contents

1 Terms and definitions

In this Site standard / Specification:

"ASD" means Australian Signals Directorate.

"ASD8" means the Australian Signals Directorate Essential Eight standards.

"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.

"GPC" means Gladstone Ports Corporation.

"**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.

"ISO27000" or **"ISO27000:2013)** means the family of standards released by the ISO/IEC group for cybersecurity management.

2 Introduction

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

2.1 Purpose

The purpose of this Specification is to support vendors and suppliers, as they ensure GPC's obligations in legislative compliance for Cybersecurity management through the delivery of goods or services to GPC.

2.2 Scope

This Specification applies to all GPC Employees, vendors and suppliers, visitors and, unless otherwise specified, any other worker engaged under the direct management of GPC (for example, contractors, sub-contractors, Consultants, agency resources and volunteers). Where relevant, 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 specification applies regardless of the application of the services or goods to all persons listed as above.

2.3 Objectives

This Specification aims to:

(a) Provide detail to all Employees, vendors and suppliers, visitors and, unless otherwise specified, any other worker engaged under the direct management of GPC (for example, contractors, sub-contractors, Consultants, agency resources and volunteers), on their requirements for management of cybersecurity and information.

3 Principles and requirements

Effective Data and Information Security for GPC is critical for operations. GPC is considered a Critical Infrastructure Asset for Australia (under legislation), and as such is integral to our business.

All data must be managed in accordance with at least one of the ISO27000 family of Standards (ISO27002:2013), NIST Cyber Security Framework (National Institute of Standards and Technology), ASD8 (Australian Signals Directorate Essential Eight) and/or SOC1/2 (Service Organization Controls) standards, which govern Cybersecurity and Information Management in response to Confidentiality, Integrity and Access requirements for data control.

3.1 Cyber and Data Security

The Supplier must establish, maintain, enforce and continuously improve its safety and security procedures and safeguards against the unauthorised use, disclosure, destruction, loss or alteration of Principal Data and the Principals other Confidential Information.

The Supplier will provide at the commencement of the engagement:

(a) Transparency relating to data access and security controls

(b) Artefacts including Policies, Standards and Guidelines, which details the suppliers Security Model/Target Framework references.

(c) Where applicable, artefacts including Policies, Standards or Guidelines, which detail the response process for any data/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 to the Principal 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 of the Principal communicated to the Supplier from time to time, including security requirements relating to access to, and use of, any data, information systems or facilities provided by the Principal or another third party.

If the Supplier becomes aware of a Security Incident, it must:

(i) immediately, and in any event no later than 24 hours after the Security Incident first occurs, notify the Principal in writing, and give the Principal full details, about the Security Incident;

(ii) co-operate with the Principal in any investigation or audit (including by providing access to the Supplier's premises, the Supplier's Personnel, processes and systems) in respect of the Security Incident; and

(iii) Conduct its own investigation of the Security Incident, and:

(A) Implement rectification measures if an actual incident or breach occurred or an incident or breach is likely to occur; or

(B) Confirm to the Principal that no actual incident or breach occurred or is likely to occur.

3.2 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. Without Principal's approval (in its sole discretion):

i Supplier shall not access, copy or use any information of Principal other than Principal data, and

ii Principal data shall not be;

a) Used or copied by Supplier or Supplier Agents other than in connection with providing the services,

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

c) Commercially exploited by or on behalf of Supplier or Supplier Agents.

iii 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.

iv 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.

The Supplier undertakes and warrants that:

(a) It will:

(i) Ensure that, at all times:

(A) 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; and

(ii) Upon the Principal's request, produce to the Principal or its nominee evidence of the Supplier's compliance with its obligations under clause 1.3(a) (i);

(b) Without limiting any other clause of this Contract, it will (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; and

(c) Ensure all electronic mail communications between the Principal and the Supplier are appropriately secure by leading industry standard encryption. The encryption algorithm and methodology must be reviewed annually and any changes be approved by the Principal.

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 Services, at least the following:

(a) Acceptable use of technology by the Supplier's Personnel;

(b) Confidentiality;

(c) Management of Security Incidents;

(d) Cryptography;

(e) Identity and access management;

(f) Management direction for information security;

(g) Transfer of information;

(h) Security logging and event management; and

(i) 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 of this clause 3 by any of the Supplier's Personnel, immediately:

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

(b) Deny any access by the Supplier's Personnel to the information systems of the Principal.

3.3 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 for the duration of working with GPC. The supplier will detail and supply BCP and DRP artefacts at the commencement of this engagement.

4 Roles and Responsibilities

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

Role	Responsibilities
Board /EMT	To ensure that GPC complies with its obligations by: Strategy review and development of cyber security requirements to ensure legislation and legal obligations are met
Managers and Superintendents	To ensure that GPC complies with its obligations by: Communicating and consulting with stakeholders to ensure specification is understood and complied with
Employees and Suppliers	To ensure that GPC complies with its obligations by: Ongoing monitoring and implementation of the specification to manage risks Identify and implement opportunities to ensure GPC is meeting the specifications identified. Participating in internal audit and interactions with others to check compliance
Supply Department in conjunction with ICT Department and GPC contract owners	To ensure that GPC complies with its obligations by:

Role	Responsibilities
	Managing the inclusion of Cyber security clauses in standard contract templates Maintaining Cyber security expectations in scopes of works Managing executed contracts and checking compliance with contract terms and conditions

Monitoring conformance to this Specification through external and internal audit processes.

Adjustments to clauses will occur from time to time, to ensure GPC remains protected. The vendor/supplier is required to review this document at least annually, where an agreement spans beyond a 12-month period, and respond to any changes as directed.

Please contact the IS Manager for any additional information, raise a new idea or program, or otherwise have any concerns with conformance to this Specification.

5 Appendices

5.1 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) *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	*AS/NZ ISO27000 family of IT Security Frameworks,* *Queensland Government Information Security Policy (IS18),* *Queensland Government Information Security Classification Framework (QGISCF)*

(b) Gladstone Ports Corporation documents

The following documents relate to this Specification:

Type	Document number and title
Tier 1: Policy	#1564208 *Technology, Security and Information Policy* # 924357 *GPC Risk Management Policy*
Tier 2: Standard/ Strategy	#1074448 *GPC Information Systems Security Management Standard (ISMS)* #1190724 *GPC Records Management Standard*

5.2 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