



Cyber Security Standard

STD - Standard

Document No.: 0000-A9-STD-60025

Security Classification: Unrestricted

Revision	Issue Reason	Prepared By	Checked By	Approved By
2	Issued for Use	Drew Marshall Principle Cyber Risk	Doug Fairall Manager Technology Infrastructure & Security	Toshi Tanaka General Manager Technology

TABLE OF CONTENTS

ABOUT THIS STANDARD	1
1. BUSINESS RULES	1
1.1. Cyber Security Governance & Management	1
1.2. Cyber Security Risk, Compliance and Assurance	2
1.3. People & Workforce Cyber Security	3
1.4. Asset, System and Information Protection	3
1.5. Identity & Access Control	4
1.6. Physical & Environmental Security	4
1.7. Operations, Vulnerability and Network Security	5
1.8. Secure Change, Projects & Third Parties	5
2. MONITOR, ASSURE AND IMPROVE	6
3. REFERENCE AND COMPLIANCE DOCUMENTS	6
4. ABBREVIATIONS AND DEFINITIONS.....	7
5. RECORD OF AMENDMENT	8

LIST OF TABLES

Table 1: Reference and Compliance Documents.....	6
Table 2: Abbreviations and Definitions	7
Table 3: Record of Amendment	8

About This Standard

Purpose

This Standard defines the business principles and business rules for protecting computer systems from unauthorised access, modification and intentional disruption

This Standard is in place to:

- Maintain the efficiency and safety of business operations that rely on computer systems
- Protect and enhance the Company reputation; and
- Comply with relevant legislation.

In Scope

The scope of application of this Standard is as detailed below and includes (other than those employee groups detailed in “out of scope” below), any individual or entity employed by the Company or INPEX’s Affiliated Companies, including, but not limited to:

- INPEX Australia Pty Ltd (ACN 134 715 254)
- INPEX Browse E&P Pty Ltd (ACN 165 711 017)
- INPEX Oil & Gas Australia Pty Ltd (ACN 155 960 151)
- INPEX DLNGPL Pty Ltd (ACN 104 124 192)
- INPEX Holdings Australia Pty Ltd (ACN 150 217 315)
- INPEX Ichthys Pty Ltd (ACN 150 217 253)
- INPEX Operations Australia Pty Ltd (ACN 150 217 262)
- Ichthys LNG Pty Ltd (ACN 150 217 299)
- INPEX New Energy Business Pty Ltd (ACN 656 098 921)
- INPEX Australia Financial Services Pty Ltd (ACN 672934593)

1. Business Rules

1.1. Cyber Security Governance & Management

1.1.1 Business Principle

To provide management direction and support for Cyber Security in accordance with business requirements and relevant laws and regulations.

Business Rules

- a) Security controls shall be in place to protect the Company from potential disruption caused by Cyber Security events.

-
- b) Roles and responsibilities shall be well defined for managing Cyber Security at all levels within the Company.
 - c) Security incidents shall be detected and responded to in a timely manner.
 - d) Cyber Security incidents shall be managed in accordance with the Company's incident response and crisis management framework, including defined escalation thresholds and executive notification requirements.
 - e) Cyber Security requirements shall be defined and adopted by all system and technological developments.
 - f) All systems and information shall be managed and operated in line with the Cyber Security Standard.
 - g) IT facilities shall be protected from any physical threats based on risk.
 - h) Cyber Security coordination shall ensure that:
 - i) Cyber Security coordination mechanisms shall be established to ensure effective oversight, escalation, and communication of Cyber Security risks and issues.
 - ii) The Company's Cyber Security posture is assessed and made available to senior management at agreed intervals.
 - iii) The Company maintains appropriate contacts with relevant external authorities concerning Cyber Security matters.
-

1.2. Cyber Security Risk, Compliance and Assurance

1.2.1 Business Principle

To ensure that Cyber Security is implemented and operated in accordance with the Company policies and procedures, and legal, statutory, regulatory or contractual obligations; and Cyber Security risks are managed in accordance with the Company's risk appetite and in alignment with the risk management standard.

Business Rules

- a) Regulatory requirements applicable to Cyber Security shall be identified and complied with as necessary
 - b) Cyber Risk will be periodically assessed and reported according to the Company Risk Management Standard
 - c) Company appetite for Cyber Risk will be defined by the maximum Target Risk Level of Cyber related risks as documented in the Enterprise Risk Management System.
 - d) Systems shall be periodically reviewed for compliance with the Company Cyber Security standards.
-

- e) All identified risks or deviations from the Company Cyber Security Standards shall be documented and recorded with appropriate treatment plans.
- f) Cyber security risks arising from third-party and supply chain relationships shall be identified, assessed, and managed in accordance with the Company's risk management processes and risk appetite.

1.3. People & Workforce Cyber Security

1.3.1 Business Principle

To protect the Company's interests by ensuring personnel understand and fulfil their Cyber Security responsibilities, during their employment and termination.

Business Rules

- a) The contractual agreements with personnel shall state their and the Company's responsibilities for Cyber Security.
- b) Management shall require all personnel to apply Cyber Security in accordance with the established policies and procedures of the Company.
- c) All personnel shall receive appropriate awareness education and training including regular updates on organisational policies and procedures, as relevant for their job function.
- d) Cyber Security breaches may be subject to disciplinary action in accordance with the Company Disciplinary Standard (0000-AN-STD-60021).

1.4. Asset, System and Information Protection

1.4.1 Business Principle

To identify the Company assets, define and implement the appropriate level of protection based on importance in order to prevent unauthorised disclosure, modification, removal or destruction of systems.

Business Rules

- a) Computer systems shall be identified and appropriately protected. All systems shall be:
 - i) Recorded within an inventory.
 - ii) Classified according to criticality, legal requirements and sensitivity to the Company.
 - iii) Protected in accordance with their classification.
 - iv) Assigned an owner who shall be accountable for assuring their adequate protection.
 - v) Cleansed of sensitive information prior to their disposal.

- b) Protection and resilience controls shall be proportionate to system criticality and business recovery requirements.
- c) Sensitive information shall be protected using appropriate cryptographic controls during storage and transmission, commensurate with its classification.
- d) All personnel shall return all the organisational assets in their possession upon termination of their employment, contract or agreement.

1.5. Identity & Access Control

1.5.1 Business Principle

To ensure applications, systems, services and information processing facilities are only accessed by authorised users who shall safeguard their authentication information.

Business Rules

- a) Users will only be granted access to systems as required to perform their job role
- b) Users will be authenticated commensurate with the risk of the transaction.
- c) A formal user registration and de-registration process shall be used to enable assignment of access rights to users
- d) User access rights will be reviewed at periodic intervals.
- e) The access rights of all users to systems and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
- f) Privileged administrative access to systems shall be provisioned using a separate administrative identity, distinct from the general IT user account.

1.6. Physical & Environmental Security

1.6.1 Business Principle

To protect against loss, damage, theft or compromise of assets and interruption to the Company's operations by preventing unauthorised physical access, damage and interference to the Company's systems and information processing facilities.

Business Rules

- a) Systems shall be protected from threats arising from physical damage and theft.
- b) IT processing facilities shall be hosted in restricted areas accessible only to those personnel with a business requirement to use them

1.7. Operations, Vulnerability and Network Security

1.7.1 Business Principle

To ensure the integrity, availability, and confidentiality of systems and information by protecting operational environments, network communications, and supporting infrastructure.

Business Rules

- a) Suitable technical controls against malicious attack shall be implemented for all Company-managed systems, commensurate with system capability, exposure, and risk.
- b) Systems shall be protected against unauthorised access and modification.
- c) Security-relevant events shall be logged, monitored, and retained in accordance with legal, regulatory, and risk requirements.
- d) Vulnerabilities shall be routinely identified and steps taken to minimise the risk of their exploitation.
- e) Security controls shall be periodically tested for control effectiveness.
- f) Clear accountability and responsibility for the network shall be defined, and key tasks shall be assigned to appropriately qualified personnel
- g) All connections or entry points to the network shall be individually identified, verified, recorded, and approved by the network owner.
- h) Documentation of the Company's network shall be maintained reflecting the architecture at any point in time.
- i) Network integrity shall be protected through appropriate segregation and segmentation.

1.8. Secure Change, Projects & Third Parties

1.8.1 Business Principle

To ensure that cyber security requirements are integrated into the design, development, acquisition, implementation, operation, and maintenance of systems and services, and that cyber security risks arising from third-party relationships are managed in accordance with the Company's risk appetite, and business requirements

Business Rules

- a) Cyber Security related requirements should be included in the requirements for new systems or enhancements to existing systems.
- b) Cyber Security risks associated with cloud, hosted, and managed services shall be identified and managed in accordance with defined shared responsibility models.

- c) Selection of appropriate security controls shall be integrated in the design phase of system development.
- d) New or modified systems shall be validated against agreed Cyber Security requirements prior to their deployment.
- e) Testing of Cyber Security functionality shall be carried out during development and prior to systems moving into production.
- f) Cyber Security requirements to address supply chain risks shall be established, prioritised, and integrated into contracts and other agreements with suppliers and other relevant third parties.
- g) Cyber risks posed by suppliers, their products and services, and other third parties shall be understood, recorded, assessed, responded to, and monitored

2. Monitor, Assure and Improve

Compliance with this Standard shall be monitored in accordance with the Company Assurance Standard (0000-A0-STD-60031). Changes made to this Standard shall be subject to Company management of change processes. Relevant Technical Authority(s) and Subject Matter Expert(s) must be consulted and involved in revisions to this Standard.

The Owner of this document can be found [here](#).

3. Reference and Compliance Documents

The documents listed below are relevant to the execution of this Standard.

Reference documents (R) are documents referred to in the course of completing this Standard.

Compliance documents (C) include all standards, regulatory governance, contracts, business rules or policies applicable to this Standard.

Table 1: Reference and Compliance Documents

Document Name	R	C	Document Number
Policies			
Standards			
Sensitive Information Standard		C	0000-A9-STD-60008
Disciplinary Standard		C	0000-AN-STD-60021

Other Documents (e.g. External Documents, Specifications)			

4. Abbreviations and Definitions

Table 2: Abbreviations and Definitions

Abbreviation / Term	Definition
Cyber Security	Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
The Company / INPEX	Any operation or business under the control of INPEX Executive Management in Australia, whether located in Australia or another location (as a branch office), is deemed to be the company.
Systems	Critical and non-critical information technology systems that support the Company's business objectives.
Personnel	Includes Employees, Contractors, Expatriates, Inpatriates, Consultants and Secondees, and for the purposes of this document, Directors, Officers, Agents and Representatives of INPEX and Ichthys LNG and other individuals, effectively controlled by or under operational control of INPEX or Ichthys LNG Pty Ltd or that act on their behalf (either directly or indirectly).

5. Record of Amendment

Table 3: Record of Amendment

Revision	Section	Amendment
0	All	Supersedes 0000-A9-STD-60009 Information Security Standard
1	All	Revised scope to include both IT and ICSS General update to include high level rules.
2	All	Transferred content into the updated BMS Standard template. Combined sections to ensure maximum of 8 business rule sections. Added rules for: 1. Privileged user accounts 2. Supply Chain Cyber risk

NOTICE

All information contained within this document has been classified by INPEX as [Unrestricted](#) and must only be used in accordance with that classification. Any use contrary to this document's classification may expose the recipient and subsequent user(s) to legal action. If you are unsure of restrictions on use imposed by the classification of this document you must refer to 0000-A9-STD-60008, Sensitive Information Protection Standard or seek clarification from INPEX.

Uncontrolled when printed.

Document Endorsement and Approvals

This page has been automatically generated and appended to this document by the INPEX Australia Controlled Document Management System (CDS). This page contains key events related to this document that are listed in the tables below and the information is unable to be manually edited.

Document Identification

Document Number	Revision	Security Classification	Date
0000-A9-STD-60025	2	Unrestricted	16/03/26 08:00

Document Revision History

Revision	Date and Time	Issue Reason

Delegation of Authority

From Name	To Name	Date and Time	Action

Name	Title

Electronic Endorsement and Approval

Electronic approval of this document complies with the issued INPEX Electronic Approval Standard (0000-A9-STD-60011) and records evidence that the applicable person has either endorsed and/or approved the content contained within this document. The reviewers of this document are recorded in the CDS.

Name	Title	Date and Time	Action
Toshiki Tanaka	General Manager Techn	16/03/26 17:57	Approver