INTERNAL

INFORMATION SECURITY POLICY FRAMEWORK

Doc. Name:	INFORMATION SECURITY POLICY FRAMEWORK	**Doc. Number:**	OG-POL-ITIS-001		
Version:	v1.4	**Status:**	Released	**Effective Date:**	25-Nov-22

Document Information

Date	Author	Version	Change reference
18-Aug-22	Group Head of Cyber and Information Security	v0.1	Initial draft.
17-Nov-22	Group Head of Cyber and Information Security	v0.2	Revised version – post-review from stakeholders
25-Nov-22	Group Head of Cyber and Information Security	v1.0	Released version
26-May-23	Chief Information Security Officer	v1.1	Updates to section 2.7 and Glossary
26-Sep-23	Chief Information Security Officer	v1.2	Updates to section 2.7.2
26-Jun-24	Chief Security Officer	v1.3	Policy review and updates to section 2.7.2
23-Jun-25	Cyber & Information Security Manager	v1.4	Annual Review

Distribution

Company Name	All Pay Perform entities (“**Company**”)

Properties

Item	Details
Document Title	Information Security Policy Framework
Author	Chief Security Officer
Creation Date	18-Aug-22
Approver	Board of Directors
Approval Date	25-Nov-22

Table of Contents

[Table of Contents – update after opening in Word]

1. Introduction

1.1 Document Definition

This document is a Policy.

For a full description of document types, see Section 1.5 below.

1.2 Mission Statement

Policies, Standards, Procedures, and Guidelines are the primary way in which the Executive Team's direction and expectations are translated into specific, measurable, and testable goals and objectives. They are a critical component of governance at the Company as they provide the structure and rules around which the organisation, and all subsidiary organisations, must operate. The IT-IS Governance Committee (IT-ISGC) has been established to create, maintain, and govern Information Security (IS) Policies, Standards, Procedures, and Guidelines. The IT-ISGC is responsible for communicating these documents to all applicable partners, joint ventures and subsidiaries, as well as distributing them and/or making them accessible to the Company's personnel (including consultants, contractors, and other applicable 3rd party vendors and partners).

1.3 Objective

The objective of the Company Information Security Policy Framework is to provide the foundation for all documentation and operational processes developed to protect information or data assets (used interchangeably from this point forward) owned by, or in the custody of, the Company from:

(a) Unauthorised disclosure – loss of CONFIDENTIALITY

(b) Unauthorised or unintended modification – loss of INTEGRITY

(c) Unintended loss of availability – loss of AVAILABILITY

The Company information security program supports the Executive Team's objectives by providing the guidance and means to protect data assets. The Information Security Program includes maintaining Policies, Standards, and Procedures in areas including (but not limited to), internal and external risk management, threat and vulnerability management, logical and physical security, and mapping of IS responsibilities.

This Policy is based partly on the '*International Organisation for Standardisation and International Electro-Technical Commission (ISO/IEC) 27002 Standard, Information Technology - Security Techniques - Code of Practice for Information Security Controls*'. It is further supported by the Company's Information Security Policy Set.

1.4 Scope

1.4.1 Applicability to Personnel

This Policy applies to all personnel, members of the Board of Directors, and all consultants and contractors of the Company. This Policy also applies to applicable partners and joint ventures of the Company (where/if applicable).

1.4.2 Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

1.4.3 Applicability to Assets

This Policy applies to all information assets globally owned by the Company, or where the Company has custodial responsibilities.

1.5 Document Type Definitions

The primary documents that support this Information Security Policy are Policies, Standards, and Procedures. These are defined below.

For a complete list of all permitted document labels see the *OG-STD-ITIS-001 – IT-IS Document Management Standard*. Only these labels are permitted for document assets.

1.5.1 Policy

A **Policy** is a set of directional statements and requirements aiming to protect corporate values, assets, and intelligence. Policies serve as the foundation for related Standards, Procedures, Processes, and Guidelines and can be seen as a representation of both the corporate culture, and the senior leadership's commitment to the IS program.

Policies include language such as 'will' / 'will not', or 'must' / 'must not', and should be generic enough to require infrequent change:

> e.g., Access to all the Company systems <u>will</u> include strong authentication.

1.5.2 Standard

A **Standard** is a set of practices and benchmarks employed to comply with the requirements set forth in the Policies. A Standard should always be a derivation of a Policy, as is the second step in the process of an organisation's Policy propagation.

Standards are very specific and detailed and are designed to expand upon the generic Policy statements. For the above example policy statement, the authentication standards would include things like the minimum password length and complexity, when multi-factor authentication is required, approved access methods and protocols and so on. In other words, the standard will define what 'strong authentication' means.

Standards can be seen as the baseline configurations for <u>*how*</u> the policies are to be implemented. From system hardening standards, to vulnerability management schedules, standards can be exceeded, but only with an approved exception can they not be met.

1.5.3 Procedure

A **Procedure** is a set of step-by-step instructions for implementing Policy requirements and executing Standard practices.

As such, Procedures can be seen as personification of ‘corporate knowledge’. If everyone knows what to do and how to do it (especially new employees), then the organisation can only move forward. Everyone is responsible for documenting the repeatable processes relevant to their job role, and for improving on the established procedures where possible.

1.5.4 Guideline

A **Guideline** is a non-mandatory best practice guide designed to help all employees understand some of the more difficult IT concepts. e.g. choosing a strong password.

1.6 Related Documents / References

- OG-CHA-ITIS-001 – IT-IS Governance Steering Committee Charter
- OG-POL-ITIS-004 – Data Classification Policy
- OG-POL-ITIS-006 – IT-IS Risk Management Policy
- OG-STD-ITIS-001 – IT-IS Document Management Standard
- OG-STD-ITIS-002 – Change Management Standard
- OG-PRC-ITIS-001 – IT-IS Document Management Procedure
- OG-PRC-ITIS-003 – IT-IS Policy & Standard Exception Procedure
- OG-OTH-ITIS-001 – IT-IS Master Documents Register

2. Policy Statements

2.1 Protection of Data

It is the Policy of the Company that information in all its forms: written, spoken, recorded electronically, or printed, will be protected from accidental or intentional unauthorised modification, destruction, or disclosure throughout its life cycle in accordance with the data classifications within the *OG-POL-ITIS-004 – Data Classification Policy*. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

2.2 Requirement for Policy Documentation

All supporting Policies, Standards, and Procedures must be documented and must be made available to individuals responsible for their implementation and compliance. All activities identified by the Policies and Procedures must also be documented.

2.3 Regional Variances

Where appropriate, regional variances to this Policy can be permitted to address any local legal and regulatory requirements. All such Policies, Standards, and Procedures are subordinate to, and must be consistent with, this Policy, and must be approved by the Company IT-ISGC.

See Section ‘6. Policy Exception Process’ for more information.

2.4 Compliance with Policy & Standard Provisions

All business processes and information systems implemented after the effective date of these policies are expected to comply with the provisions of all related Policies and Standards. Existing systems are expected to be brought into compliance as soon as practical.

Data Owners will work in conjunction with the Security team to ensure that information systems are managed, maintained, and processed in a manner that supports compliance with all security requirements.

2.5 Policy & Standard Review Period

All documentation must be reviewed at least annually, during significant changes to business goals, or in response to significant changes in the prevailing threat landscape.

In addition to the planned annual review cycle, an ad-hoc review of any Policy, Standard, or Procedure must be initiated **if significant changes occur** to the organisation’s structure, technology environment, regulatory obligations, business objectives, or the external threat landscape. Such trigger-based reviews ensure that documentation remains current and effective at all times, not solely at scheduled intervals.

Alternative Policy and Standard review timings to be determined by the IT-ISGC where applicable.

2.6 Independent Review of the Information Security Program

The IT-ISGC or the Executive Team must initiate an independent review of all relevant aspects of the Company Information Security Program at least annually, during significant changes to business goals, or in response to significant changes in the prevailing threat landscape to ensure the continuing suitability, adequacy and effectiveness of the organisation's approach to managing risk.

The review must:

a. assess opportunities for improvement and the need for changes to the approach to security, including the Policy, Standards and/or control objectives.

b. be carried out by individuals independent of the area under review. These individuals can be internal or 3rd parties but must demonstrate that they have appropriate skills and experience.

c. be recorded and reported to the IT-ISGC and/or the Executive Team as appropriate. These records must be maintained.

d. include recommendations for corrective actions (risk treatment).

2.7 Information Security Roles & Responsibilities

2.7.1 Board of Directors

The Board of Directors are accountable for:

1. Defining the business goals to be supported and enabled by the Information Security Program.

2. Being accountable for the maintenance of the Confidentiality, Integrity, and Availability of Company data and infrastructure assets.

3. Being accountable for all applicable regulatory and statutory compliance requirements.

4. Demonstrating commitment to the continuous improvement, suitability, adequacy, and effectiveness of the Company Information Security Program (ISP).

5. The provision of ongoing ISO 27001 management.

2.7.2 Executive Team

The Executive Team are responsible for:

1. Setting Information Security objectives in-line with business goals, to be reviewed annually or when updated to reflect significant changes to business goals, or the prevailing threat landscape.
2. All Policies related to the maintenance of the Confidentiality, Integrity, and Availability of Company data and infrastructure assets, and the enforcement of them.
3. Maintaining compliance with applicable regulatory and statutory compliance requirements.
4. Support for the IT-ISGC for the ongoing ISO 27001 management.

The Executive Team consists of:

- Chief Executive Officer
- Chief Product & Technology Officer
- Chief Financial Officer
- Chief Compliance Officer
- Chief Security Officer
- Chief Information Officer
- Chief Revenue Officer
- Group General Counsel

2.7.3 IT-IS Governance Committee (IT-ISGC)

The primary functions of the IT-ISGC are:

1. To address “at risk” behaviour or performance counter to the Company Information Security Policy Set.
2. To set and review security strategy and vision to align it with the business.
3. Review key security risks in relation to their progress and risk impact, as reported from Company risk management processes.
4. Maintenance of the Company security risk register.
5. To coordinate the creation and communication of security Policies, Standards and Procedures.
6. To review/approve Document Coordinator’s recommendations on the security Policies, Standards and Procedures.

7. To be functionally responsible for communication of the security Policies to all interested parties (internal and/or external), educate the user community, and make them easily accessible.
8. To review, rule on, and track security change control requests.
9. To review, rule on, and track security Policy exception requests.
10. Arbitration on exceptions disputes to IT-IS Policies and Standards.
11. Management of the *IT-IS Master Documents Register*.
12. To oversee security Change Control.
13. The continuous improvement, suitability, adequacy, and effectiveness of the Company Information Security Management System (ISMS)

The IT-ISGC will consist of, at a minimum, members of the Company's Security, Legal, Technology, Finance, People, Product, Compliance, Operations, Commercial, and Risk teams, with Subject Matter Expertise (SME) support as necessary, and anyone else deemed appropriate by the IT-ISGC Chair. This may include internal or external SMEs to develop specific Policies, Standards, Procedures, Guidelines, or control capability requiring specific subject matter knowledge.

2.7.4 Security Team

General responsibilities include:

1. Management of the Company security risk assessment and risk treatment program(s).
2. Providing security expertise and support for all systems and users.
3. Advising Data Owner and Data Custodian in the security controls appropriate to an asset's Data Classification.
4. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
5. Specifying controls and communicating the control requirements to the Data Owners and users of the information.
6. Educating Data Owners, or other owners of IS relevant assets, with comprehensive information about security controls affecting system users and application systems.
7. Reporting regularly to the IT-ISGC on the status with regards to information security.

2.7.5 Document Coordinator(s)

The Document Coordinator(s) are responsible for working with management, Data Owners, and end users to develop and implement all types of security documentation, and controls. All are subject to the approval of the Security team and must be presented in the format specified in the *OG-STD-ITIS-001 – IT-IS Document Management Standard*.

General responsibilities include the:

1. Functional responsibility for the creation and maintenance of security Policies, Standards and Procedures for submission to the IT-ISGC for approval.
2. Functional responsibility for communication of their individual security Policies to all interested parties (internal and/or external), educate the user community, and make them easily accessible.
3. Approval of documentation storage location, and media type (both soft and hard copy).
4. Management of documents of external origin.

2.7.6 Internal Audit

Internal Audit are responsible for regularly examining systems, people, policies, and processes to verify whether they continuously meet the organisation's approved security requirements and whether the security controls are appropriate. Informal audits can be performed by those operating the system under review or by internal or external auditors.

Internal Audit's responsibilities include, but are not limited to:

1. Ensure that security Policies, Procedures, and Standards are in place and adhered to per the Compliance Measurements specified in each Policy document.
2. Review the effectiveness of internal controls related to the risk treatment plans.
3. Identify risks, estimate the severity of the risk, and develop audit tests to substantiate the impact of the risk to the business assets.
4. Following up on audit findings and recommendations to ensure appropriate resolution.

2.7.7 Data Owners

The Data Owners are generally responsible for the processing and storage of data in a defined domain. Functional responsibility may be delegated to named Data Custodians with the approval of the IT-ISGC.

The Data Owner is responsible for the administration of controls as specified by this Policy. Responsibilities of the Data Owner include:

1. Knowing the data for which s/he is responsible.

2. Assigning Data Classification Level as per *OG-POL-ITIS-004 - Data Classification Policy*.
3. Ensuring appropriate procedures and controls are in effect to protect the confidentiality, integrity, and availability of the data used or created within the unit.
4. Releasing information as authorised by Legal for use and disclosure using procedures that protect the privacy of information.
5. Maintaining operational procedures that support the information security policies and standards as appropriate.
6. Reporting promptly the loss or misuse of Company information.
7. Monitoring and managing the performance of third parties against data quality and security targets and compliance to this policy and supporting standards.
8. Initiating corrective actions when problems are identified.

2.7.8 Line Management

Company Line Management are personnel who supervise other personnel, consultants, and/or contractors. Each Line Manager is responsible for overseeing their team's use of information, including:

1. Reviewing and approving all requests for their team's access authorisations.
2. Initiating security change requests to keep the team's security record and accesses current with their positions and job functions.
3. Promptly informing appropriate parties of team's terminations and transfers, in accordance with termination procedures.
4. Revoking physical access to terminated personnel, i.e., confiscating access passes, changing combination locks, etc.
5. Providing personnel with the opportunity for training needed to properly use Company computer systems.
6. Reporting promptly the loss or misuse of Company information and physical assets (e.g. ID badges, laptops); and
7. Initiating corrective actions when problems are identified.

2.7.9 Users

A User is any person who has been authorised to read, enter, or update Company data. A user of data is expected to:

1. Comply with the Company Acceptable Use Policy.

2. Comply with other Company Information Security Policies and Standards relevant to their job functions (current 'released' versions only).
3. Comply with security controls established by the Data Owner(s).
4. Keep personal authentication devices (e.g. passwords, two-factor authentication devices, etc.) confidential.
5. Report promptly unauthorised access, the loss or misuse of Company data and physical assets (e.g. access passes, laptops).
6. Submit Policy, Standard, and Procedure change requests as necessary.

2.8 Communication of Policies to Relevant Personnel and Interested Parties

The Company must establish and maintain a formal mechanism for communicating all approved Information Security Policies, Standards, Procedures, and Guidelines to relevant personnel and interested parties. The communication process must ensure that all individuals subject to the requirements of this Policy Framework are made aware of their obligations in a timely and verifiable manner.

The communication mechanism must include the following elements:

1. All new and updated Policies, Standards, and Procedures must be communicated to relevant personnel within 30 calendar days of approval or revision.
2. Communication channels must include, at a minimum: publication on the Company intranet or designated document management system, direct notification via email or equivalent electronic communication to all affected personnel, and inclusion in onboarding materials for new starters.
3. External interested parties (including contractors, consultants, partners, and applicable third-party vendors) must be notified of relevant Policy requirements through contractual provisions and/or direct communication as appropriate.
4. The Document Coordinator(s) and the IT-ISGC are jointly responsible for ensuring that the communication process is executed and that records of distribution are maintained.
5. Communication records must be retained in accordance with the Company's document retention requirements and must be available for audit purposes.

2.9 Acknowledgement of Policies by Relevant Personnel and Interested Parties

All relevant personnel and interested parties must formally acknowledge receipt and understanding of applicable Information Security Policies, Standards, and Procedures.

This acknowledgement requirement ensures that the Company can demonstrate awareness and acceptance of obligations across the organisation.

The acknowledgement process must meet the following requirements:

6. All personnel (including employees, Board members, consultants, and contractors) must provide documented confirmation of receipt and understanding of applicable Policies upon initial onboarding and following each material update or annual review cycle.

7. Acknowledgement must be captured through a verifiable mechanism such as an electronic signature, a dedicated acknowledgement form within the Company's learning management system, or equivalent documented confirmation.

8. External interested parties must acknowledge relevant Policy requirements as part of contractual agreements or through a separate written acknowledgement, as determined appropriate by the IT-ISGC.

9. Line Management are responsible for ensuring that all members of their teams complete the required acknowledgements within the specified timeframe.

10. The Security Team must maintain a register of acknowledgements and report on compliance rates to the IT-ISGC on at least a quarterly basis. Non-compliance with the acknowledgement requirement must be escalated in accordance with the enforcement provisions of this Policy.

2.10 Documentation Development

Where documentation does not already exist, the IT-ISGC may assemble a group of subject matter experts or other necessary resources to review and comment on the feasibility of specific Policies and Standards. Each document will be presented in a prescribed format, described in the 'Policy Format, Naming Convention, & Required Language' section below, and in the *OG-STD-ITIS-001 – IT-IS Document Management Standard*.

Each Policy and Standard document will undergo a detailed preliminary review and approval from the appropriate SMEs and relevant Document Coordinator(s). Once the preliminary review and approval is completed, a final sign-off will be provided by the IT-ISGC.

When a document is approved, the Document Coordinator will oversee the communication and training initiative(s) with relevant areas and publish them for Company personnel.

2.11 Policy Format, Naming Convention, & Required Language

A standard template will be used in the creation of all Information Security Policies, and for the related Standards, Procedures and Guidelines.

The primary mandatory attributes are detailed in the *OG-STD-ITIS-001 – IT-IS Document Management Standard*.

Creation of IS documentation will follow the procedure defined in the *OG-PRC-ITIS-001 – IT-IS Document Management Procedure*.

2.12 Policy Exceptions

In the event that a business area or department is unable to comply with an approved Policy or Standard, an exception may be requested and submitted to the Document Coordinator for initial review and onward presentation with recommendations to the IT-ISGC and other interested parties.

An exception also allows for non-compliance with a Policy or Standard for either approved time, or indefinitely. This may be caused by technical limitations within an application or system or may be a result of a fundamental change to a business process or be in-line with specific business goals. In the case of an exception, a member of the Executive Team must formally accept the risk and retain accountability for non-compliance.

The process for requesting an exception is detailed in the *OG-PRC-ITIS-003 – IT-IS Policy & Standard Exception Procedure*.

2.13 Operational Procedures

At a minimum, the following operational procedures must be developed, documented, and distributed to relevant Company personnel and contractors:

- The installation and configuration of information systems (platform and application)
- Processing and handling of data assets both automated and manual
- Performing and protecting back-ups
- Change control management
- Vulnerability management & patching
- Instructions for handling errors or other exceptional conditions
- Collection of audit-trail and system log information
- Monitoring procedures for Company assets
- Monitoring and review procedures for third party providers

2.14 Change Management

Any changes to the organisation, business processes, information processing facilities or systems that affect information security must be controlled.

Change requests will include all information as detailed in the *OG-STD-ITIS-002 - Change Management Standard* and follow the relevant change request procedure(s).

All affected documentation must be updated because of any changes to Company systems or processes.

2.15 Capacity Management

A capacity management plan must be documented for critical information systems.

The plan should include:

- System tuning and monitoring parameters
- Detective controls to alert on threats to production systems
- Projections of future capacity requirements

2.16 Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of Company's assets.

Where this is not possible, detailed mitigating controls must be prepared and approved as a Policy Exception by the Company Security team.

Where practical, the initiation of an event should be separate from the authorisation.

The possibility of collusion must be considered in the design and implementation of information security controls.

2.17 Information Security in Project Management

Information security must be built into the Company project management method to ensure that information security risks are identified and addressed as part of a project. This applies to projects of any sort.

The following requirements will be integral to all project plans:

- Information security objectives are included
- An information security risk assessment is conducted
- Information security is part of all phases
- Information security implications should be reviewed regularly in all projects
- Responsibilities for information security should be defined and allocated to specific roles defined in the project management method

2.18 Background Checks

Background verification checks will be conducted on all candidates for employment and shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirement(s), the data classification to be accessed, and the perceived risks.

2.19 Delegation of Information Security Responsibility

Any individual with information security responsibilities may delegate to others, but the overarching accountability must reside with the original individual.

Where data with a classification of RESTRICTED may be at risk, permission to delegate must be received from the Data Owner.

3. Policy Compliance & Enforcement

3.1 Compliance Measures

Compliance with this Policy Framework is enforced through the validation of Compliance Measures relevant to each individual Policy and Standard derived from it.

3.2 Enforcement

This Policy applies to all personnel, members of the Board of Directors, and all consultants and contractors of the Company. Violations of this Policy may result in disciplinary action, up to and including termination of employment and / or legal action.

3.3 Policy Update & Approval

This Policy is established as a Group-wide policy and is subject to an annual review.

An earlier review of this Policy may be needed to reflect new laws, regulations and/or newly emerging risks, as applicable.

This Policy is subject to the approval of the Board.

4. Glossary / Acronyms

4.1 Glossary / Acronyms Table

Term	Definition
Company	All entities of Orbital Group collectively
Board of Directors	Each and any Board of Directors of the Company entities
Information System Assets	Information, regardless of classification, stored, processed, owned, or transmitted by the Company that has tangible and intangible value to the organisation, owned markets and joint ventures, or that must be secured under applicable legal requirements. This includes information in all forms (physical, electronic, intellectual, and sound) as well as the physical media and or systems upon or within which the information is stored, processed, or transmitted.
Information Security Policy Set	The Information Security Policy Set is composed of those documents and publications that have been approved, and which detail requirements for information security globally.
IT-ISGC	Information Technology / Information Security Governance Committee
IT-IS	Information Technology / Information Security
Accountability	Cannot be delegated and represents the highest form of responsibility. For example, the CEO can delegate responsibility for IT security, but will always be held ultimately responsible.
Responsibility	Assigned to those responsible for getting things done, and usually assigned to department head level, or an overarching committee or steering group. Cannot be delegated.
Functional Responsibility	Those responsible for performing the actual functions. For example, a department leader can be responsible for creating and distributing relevant policies but can delegate the drafting to a Document Coordinator.
Production Systems	Any Company Data Asset that directly supports the generation of revenue or transmit, process or store data.