
# Vendor Management Policy

Version: 2.0

Date of Issue: January 2023

team:grace

# Vendor Management Policy

## Table of Contents

team:grace

# Vendor Management Policy

## 1. Executive Summary

This policy has been produced to set out the approach that will be taken to manage Grace Worldwide vendors in support of the delivery of IT services and products. The scope of the policy covers all IT services and products (hardware or software) provided to the business.

## 2. Context

This policy is part of the Information Security policy hierarchy as shown in the table below.

| Document | Description |
|---|---|
| **Information Security Charter** | Directive on Grace Worldwide's commitment to Information Security |
| **Information Security Policy** | Policy covering Information Security at Grace Worldwide |
| **Information Systems Security Policy** | Policy covering Information Systems and electronic information |

## 3. Applicability

This policy applies to:

- Staff (fulltime, casual, temporary or contractors) and parties that access or use the Grace Worldwide's information assets.
- Joint Ventures.
- Outsourced Service Providers.
- Information systems where Grace Worldwide information is stored electronically either temporarily or long term.
- Information assets such as: data, documents, audio, video, etc. These assets may also include:
    - storage of customer images on Grace Worldwide networks.
    - metadata with location of hard copy records stored within Grace Worldwide applications.
- Information technology (IT) infrastructure owned by Grace Worldwide.
- This policy does not apply to Grace Worldwide information systems that store data that has been classified under the guidelines of the Australian Government Security Classification System as Protected, Confidential, Secret or Top Secret.

### 3.1 Enforcement

This policy will be enforced by technical controls wherever feasible, as indicated in the text.

Otherwise, this policy will be enforced by the Security Governance Team as set out in Grace Worldwide's Information Security Charter.

All members of Grace's workforce have a responsibility to promptly report any known instances of noncompliance to the Security Governance Team or the Chief Information Security Officer

### 3.2 Standard

Refer to Policies Quality, Health, Safety, Environment, FAIM & FIDI Standard Version 3.2, PCI & Security Legislation and Information Sources, for details relating to relevant standards and legislation for each State / Territory, and requirements of International and Australian and New Zealand Standards 9001, 4801, 14001 27001 and PCI, National Heavy Vehicle Accreditation Scheme.

### 3.3 Consequences of Noncompliance

Failure to comply with this policy can result in disciplinary action, up to and including termination of employment.

### 3.4 Language

In the Principles sections of this policy (4 and 5), the keywords "**must," "must not," "should," "should not**" and "**may**" are to be interpreted as follows:

- **"Must**" and "**must not"** mean that compliance with the policy statement is mandatory.
- "**Should"** and **"should not**" mean that compliance with the policy statement is strongly recommended. While these recommendations are not required if technical, operational or business issues make them infeasible, supporting rationale may be requested when audit or compliance review findings cite those responsible for noncompliance.
- **"May**" means that compliance with the policy statement is recommended but optional.

### 3.5 Definitions

**Compliance Risk**: These are risks arising from violations of applicable laws, rules, regulatory mandates, and along with other issues, such as non-compliance of operational, and information security policies, procedures, and processes.

**Reputation Risk**: Risks of negative public perception and opinion, such as unethical business practices, data breaches resulting in loss of sensitive and confidential consumer information.

**Strategic Risk:** These are risks arising from third parties failing to implement business initiatives that align with the overall goals and ideas of Grace Worldwide.

**Region/Country Risk**: Risks arising from the political, economic, and social landscape and other relevant events within a foreign country that can impact the services provided by vendors, ultimately affecting company operations.

**Operational Risk**: Risk arising from a failed system of operational internal controls relating to personal and relevant policies, procedures, processes and practices.

**Financial Risk**: Risks related to the financial condition of the third-party vendors, such as any "going concern" issues, or a vendor under the threat of liquidation in the foreseeable future.

**Information Technology Risk**: Risks from any number of information technology and information governance and security issues, including inadequate resources.

### 3.6 Authority

The CISO is responsible for ensuring that the policy initiative and applicable relevant procedures-are kept current as needed for purpose of compliance with mandated organisational security requirements.

## 4. Principles and Policy Statements

### 4.1 Vendor Planning and Selection Criteria

**Principles**

Planning and selection criteria of vendors prior on boarding.

**Objective**

All vendor contracts should be reviewed to ensure their suitability for Grace Worldwide environment.

**Policy Statements**

- Grace Worldwide should consider vendors that have a strong track record of transparency and maintain security of their systems, services and cyber supply chains prior to onboarding.
- Grace Worldwide should not use high risk vendors that do not conform to relevant regulations and/or relevant cyber security best practice to safeguard confidentiality, availability and integrity of data systems.
- Grace Worldwide must use formalized and written contracts, that dutifully identify roles and responsibilities, obligations, expectations and termination clauses from the relevant parties.
- Grace Worldwide should not accept any contracts that automatically renew without intervention except with the prior written approval of a Grace Worldwide company director.
- Non-disclosure agreements must be signed by relevant parties prior to onboarding any vendor.
- Grace Worldwide vendor contracts must include the right to conduct a vendor review as appropriate to the services being offered.

- Grace Worldwide will define the criteria for the limits of authority when dealing with the external vendors.
- Grace Worldwide should ensure that all staff involved in vendor onboarding attend awareness training of the appropriate laws and regulations every year.
- Grace Worldwide must ensure security requirements associated with confidentiality, integrity and availability of information entrusted to the vendor are documented in contractual agreements.
- Grace Worldwide must ensure the types of information and its ownership is documented in contractual agreements.
- Grace Worldwide must ensure locations where information will be processed, stored and communicated is documented in contractual agreements.
- Grace Worldwide should ensure information entrusted to a service provider is stored in a portable manner that allows the organisation to perform backups, service migration or service decommissioning without any loss of information.
- Grace Worldwide must ensure systems and information are not accessed by a vendor unless a contractual agreement exist between Grace and the vendor.

## 4.2 Vendor Due Diligence

**Principles**

Due diligence of new and existing vendors.

**Objective**

- All vendors must be aligned with Grace Worldwide strategic goals, as well as safeguard the confidentiality, availability and integrity of data systems in products and service provided
- All vendors must comply with relevant regulatory compliance obligations and relevant audit requirements as per Clause 3.2 Standards.

**Policy Statements**

- Conduct a security review prior to onboarding the Vendor (including check on vendor country origin) to assess vendor capability to comply with regulatory obligations and maintain Grace Worldwide's data availability, confidentiality and integrity.
- Grace IT Compliance will assess the following categories of risk as part of the security review:
    - Compliance Risk
    - Reputation Risk
    - Operational Risk
    - Information Technology Risk
    - Strategic Risk
- Grace Information Management will undertake the following annual assessments as part of the vendor due diligence program:
    - Signed Non-Disclosure Agreement
    - Annual Compliance Questionnaires – High Risk Only
    - Third Party Accreditation Requirements

    - Annual Site Audits – Destruction Vendors Only.
  - Vendors must be able to demonstrate that the product or services provided are consistent with Grace Worldwide cyber security requirements via an agreed mechanism such as Statement of Work.
  - International Partners/Vendors must be compliant with Grace policies including and not limited to the following policies which are published on Grace International Partners Website with Terms and Conditions:
    - The FIDI Professional Cooperation Guidelines
    - The FIDI Anti-Trust Charter
    - The FIDI Anti-Bribery and Anti-Corruption Charter
    - Grace Privacy Policy
    - Grace Information Security Policy
    - Grace Data Breach Response Policy.
- Risk Assessments are undertaken for suppliers in compliant with Grace Policies as per Grace Hazard Identification, Risk Assessment & Control procedure.
- Grace IT Compliance should conduct due diligence on the cyber security posture of vendors before selecting and entering into contracts or relationships.
- Grace Worldwide will develop a set of criteria to assess a vendor based on the classification of risk to the organisation activities.
- Prior to onboarding a third-party vendor, an assessment must be conducted on the vendor's organisational-wide system of internal controls such as:
  - Security Governance
  - Operational Security
  - Asset Management
  - Incident Reporting and Management
  - Personnel Security
  - Information Protection
  - System Acquisition, Development and Maintenance
  - Sub-tier partner security.
  - Business Continuity and Disaster Recovery
  - Physical security
  - Access Control
  - Human Resource Management
- Grace Worldwide will develop a set of criteria to assess a vendor based on the classification of risk to the organisation activities.
- The finance department should review and provide feedback on any applicable financial documentation, such as financial statements on behalf of Grace IT compliance.
- All contracts can only be signed by a Grace representative with the appropriate level of authority as defined in the Limits of Authority Policy.
- Grace Worldwide contracts with third parties must include clauses with vendors to ensure reporting of cyber security incidents or eligible data breaches of Grace Information.

### 4.3 Vendor Management and Monitoring

**Principles**

Vendor Management and Continual Monitoring.

**Objective**

Continually monitor various aspects of the vendor, including reviewing vendor security on a regular basis to ensure that risks are not developing and that service levels are being maintained.

**Policy Statements**

- Grace IT Compliance must conduct reviews periodically depending on the risk rating of the vendor.
- A record must be maintained of all the actions agreed upon with regard to changes in security arrangement resulting from reviews or other events.
- Vendors are required to comply with all applicable Grace Worldwide Information Security policies.
- Any vendors that fail to achieve compliance as agreed must be referred to the Privacy and Governance committee for further action and managed through the Grace Non-Conformance, Corrective and Preventative Action Procedure.

### 4.4 Vendor Termination

**Principles**

Termination of the vendor when a contract expires, the terms of the contract have been satisfied, in response to contract default, or due to changes in business strategy.

**Objective**

Ensure Grace Worldwide systems and data availability, integrity and confidentiality is maintained after contractual arrangements with third parties.

**Policy Statements**

- Data retention and destruction will be managed in accordance with the Information Systems Security Policy.
- Vendors must return any Information Assets in their possession to Grace Worldwide at the end of a contract or in the event of contract termination.
- Grace Worldwide must ensure any access to information systems or data is revoked at the end of the contract in accordance with Information Systems Security Policy.

## 5. Related Policies

- Information Systems Security Policy.
- Data Breach Response Policy.

## 6. Violation Reporting and Escalation

Any person covered by this policy is obligated to report apparent violations of this policy in accordance with the Cyber Security Incident Response policy. If the violation does not appear to be resolved in a timely manner, the person observing the violation must escalate to the CISO.

## 7. Legal or Regulatory Requirements

Grace Worldwide continuously endeavours to comply with the information security requirements and implications of any applicable laws and regulation