Information Security Charter

Reviewed January 2024

Date of Issue: January 2023

team:grace

Information Security Charter

Table of Contents

team:grace

Information Security Charter

1. Business Need for Information Security

Grace holds significant assets in the form of information, some of which would lose substantial value if disclosed improperly, destroyed or otherwise misused. Unauthorized changes to information content could also damage Grace's ability to conduct its business operations, and even actions that prevent authorized access to information could do the company significant harm. Grace's Information Security Charter addresses the mission-critical need to secure these assets, including written and oral information transmitted and stored in telecommunications devices, documents, applications, systems, databases and networks. There is also a need to ensure that all vendors to Grace Worldwide maintain an acceptable information security posture and commit to ensuring the confidentiality, security and availability of Grace's information assets.

2. Context

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

DOCUMENT	DESCRIPTION
Information Security Charter	This document
Information Security Policy	Policy covering Information Security at Grace Worldwide
Information Systems Security Policy	Policy covering Information Systems and electronic information

This Policy supports Grace's directive that all agencies appropriately protect information by establishing an Information Security Management System (ISMS). This Policy was developed in accordance with the following Standards for Information Security:

- ISO
- FIDI

3. Applicability

This policy applies to:

- Staff (fulltime, casual, temporary or contractors) and parties that access or use the Grace's information assets.
- Joint Ventures.
- Outsourced Service Providers.
- Information systems where Grace 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 networks.
    - metadata with location of hard copy records stored within Grace application.

- Information technology (IT) infrastructure owned by Grace.

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 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 Consequences of Noncompliance

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

3.3 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.

4. Principles and Policy Statements

4.1 Roles and Responsibilities for Information Security

- **Employees**: All Grace employees — including temporary, part-time and contract workers — and all other people authorized to perform work on company premises or otherwise granted access to company information or systems are responsible for ensuring that company information assets are used appropriately at all times. Specifically, they must ensure, to the best of their abilities, that information assets and systems are used only in support of the company's business operations, that information is not improperly disclosed, modified or endangered, and that access to company information resources is not made available to any unauthorized person.
- **Chief Information Security Officer (CISO):** The CISO is responsible for ensuring that appropriate security controls exist throughout the company and that companywide security awareness is increased. This specifically includes determining methods of implementing and enforcing security policies, advising information and system owners on security-related issues and ensuring that appropriate audits are conducted.
- **Security Governance Team:** The security governance team is a multidisciplinary group that includes representatives from the Finance, Compliance and Risk and Information Technology departments and is led by the CISO. The team is responsible for coordination, monitoring and communication of information security related matters throughout Grace Worldwide.

- **Information owners:** Information owners are the individuals responsible for leading business departments or headquarters functions, and are responsible for the security (that is, the integrity, availability and confidentiality) of the information they control. Information owners are also responsible for the classification of information in accordance with the Information Systems Security Policy.
- **System owners:** Any employee with administration responsibility for a computer system or involvement in selecting or purchasing computer hardware or application software is responsible for ensuring that this policy can be effectively implemented for that system or application.
- **Vendor relationship managers:** Any employee with responsibility for managing a relationship with an external vendor that has access to Grace information assets must ensure that the vendor has implemented appropriate security controls in accordance with the Vendor Management Policy.

4.2 Delegations

Table 1 – Delegations

Role	Grace Representative	Responsibility
Chief Information Security Officer (CISO)	IT Manager/ Finance Director (combined role)	• Establish the corporate security program and governance framework. • Develop security budget projections and resource allocations as required. • Ensuring compliance with national policy, standards, regulations and legislation. • Facilitating communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives.
Privacy Officer	Finance Director / National Quality Manager (combined role)	• Ensure security measures comply with privacy legislation • Providing strategic level guidance for the Grace security program
Information Technology Security Manager (ITSM)	IT Manager	• Managing the implementation of security measures • Monitoring information security for systems and responding to any cyber security incidents • Identifying and incorporating appropriate security measures in the development of ICT projects and the information security program • Helping system owners to understand and respond to reported audit failures • Delivering information security awareness and training programs to personnel

Information Security Advisor – Governance	Group Manager – Compliance and Risk (NQM)	• Responsible for the management and maintenance of the Grace Integrated Management System. • Management of Information Security risks and ensure appropriate mitigation to minimize the risks. • Assist the CISO to ensure compliance with national policy, standards, regulations and legislation.
Security Governance Team	General Manager Finance Director IT Manager Group Manager – Compliance and Risk Branch Manager	• The security governance team is a multidisciplinary group that includes representatives from the Finance, Compliance and Risk and Information Technology departments and is led by the CISO. The team is responsible for coordination, monitoring and communication of information security related matters throughout Grace.
System Owners	See Table 2	• Any employee with administration responsibility for a computer system or involvement in selecting or purchasing computer hardware or application software is responsible for ensuring that all Information Security policies can be effectively implemented for that system or application. The system owner is responsible for the secure operation of their system and needs to ensure it is accredited. If modifications are undertaken to a system the system owner will need to ensure that the changes are undertaken and documented in an appropriate manner, and that any necessary reaccreditation activities are completed

System Owners

Interact – All Branch Managers and Grace NZ Coordinators (with access and responsibilities to the Interact system and Grace shared drives (NZ)

5. Related Policies

- Information Security Policy
- Information Systems Security Policy

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 and NQM (National Quality Manager).

7. Legal or Regulatory Requirements

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

Leon Hulme
CEO