Sensitive Relocations
Secure Documents
• Can provide security crates
• Lockable and Trackable Vehicles
• All staff have Police Checks
Fragile Equipment
• Can Pack any fragile and sensitive freight for a safe journey
High Value Items
• Can Provide tailored insurance options to make sure your goods are always safe
• Can supply climate controlled trucks for temperature sensitive items

team:grace

# Information Security Policy

Version: 7.0

Date of Issue: January 2023

## Table of Contents

## Executive Summary

The reputation, business stability, and future growth of Grace are dependent on the way we manage and protect Information and Information Systems that store or access our intellectual property, employee Information, customer Information, and telematics Information we gather from our customers. Grace corporate network may become a target for hackers and other cyber-criminals, or our Information may be potentially vulnerable to other threats to the confidentiality, integrity, or accessibility. We have therefore implemented this Information Security Policy to ensure all employees help protect such Information through the adoption, implementation, and maintenance of adequate and appropriate safeguards and controls.

Each manager shall review this Policy with all Users for whom he or she has direct operational responsibility and with new Users as they are hired. Users may also receive periodic revisions of this policy. Grace reserves the right to change this policy or allow approved exceptions at any

## 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's commitment to Information Security |
| **Information Security Policy** | This document |
| **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). The ISMS forms part of Grace Integrated Management System and is developed in accordance with the following Standards for Information Security:

- ISO/IEC 27001 ISMS Requirements
- ISO/IEC 27002 ISMS Code of Practice
- PCI DSS

An ISMS is a framework and methodology used to manage information security risks. For further information refer to the Integrated Management System Manual.

This policy is guided by legislation, memoranda, circulars and Grace policies which is outlined in Grace Legal & Other Register.

## 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
- Locations where Grace information is stored electronically or hard copy storage, temporarily and/or long term
- Information assets, in any form, such as: paper, electronic, audio, video, etc. These assets may also include:
    - storage of customer images on Grace networks
    - storage of customer hard copy records in Grace facilities
    - metadata with location of hard copy records stored within Grace applications
- Information technology (IT) infrastructure owned by Grace and any IT connecting to, or residing on, Grace IT infrastructure

## Principles and Policy Statements

### Information Security Governance Framework

**Principle**

Grace shall have an Information Security Governance Framework to govern the management of information security within the organisation.

**Policy Statements**

- A Security Governance Team must be in place to ensure a formal security strategy, clear direction and visible management support for security initiatives.
- The Chief Information Security Officer (CISO) shall maintain the ownership of the Information Security policies and procedures. The CISO will be responsible for enforcing the policies and procedures.
- Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly defined.
- A management authorisation process for new information processing facilities must be established.
- Advice on information security provided by in house or specialist advisors must be sought and communicated throughout the organisation.
- Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators must be maintained.
- Independent review of information security in the organisation must be done on a regular basis.

## Outsourcing

**Principle**

Where Grace outsources any aspects of its information processing, the outsourcing arrangements and contracts shall address all information security risks related to such outsourcing.

**Objective**

To ensure that external organisations that provide information processing services comply with the information security policies of Grace.

**Policy Statements**

- The security requirements of any organisation outsourcing the management and control of all or some of Grace's information systems, networks and/or desktop environments must be addressed in a contract agreed between the parties.
- Arrangements involving access to organisational information processing facilities by an organisation handling the outsourcing must be based on a formal contract containing all necessary security requirements. This contract shall include, at a minimum, clauses stating agreement to adhere to
    - all Grace information security policies
    - return all information and assets at the end of the contractual period
    - not copy or disclose information obtained during the contractual period at Grace
    - to seek approval from an appropriate Grace delegate prior to delegating access privileges to any individual not explicitly covered by the outsourcing contract.
- All services delivered by outsourced service provider, shall be monitored for adherence to the agreed information security policies.
- Responsibility for maintaining the contract and relationship with the outsourced service provider shall be allocated to a designated individual.

## Accountability for Assets

**Principle**

Grace shall maintain appropriate control over the security and protection of all its organisational assets.

**Objective**

To secure the information processing environment of Grace, it is essential to have proper control over all assets forming part of this information-processing environment. This includes all data, information, knowledge and intellectual capital.

**Policy statements**

- An inventory of all important assets must be drawn up and maintained.
- Owners must be identified for all major assets and the responsibility for the maintenance of appropriate controls must be assigned.

- A regular inventory of assets must be performed. The minimum detail to be recorded in the asset inventory includes a description of the asset, a unique asset identification number, the designated asset owner, the classification rating of the asset, the location of the assets and date of security classification.

## Personnel Security

**Principle**

Grace must ensure the full confidence in the integrity of qualified people employed in jobs related the organisation's information processing activities.

**Objective**

To ensure the suitability of all employees working on the organisation's information systems to reduce the risks of human error, theft, fraud or misuse of facilities.

**Policy statements**

- Relevant information security roles and responsibilities must be documented in job definitions where appropriate.
- Employees working in the information processing environment must be screened at the time of application and promotion.
- All employees and third parties such as contractors, consultants, business partners and outsourced staff must sign a confidentiality agreement as part of their initial terms and conditions of employment.
- Aspects related to information security must be addressed in an employee's terms and conditions of employment and for third parties, with a formal contract with Grace.
- Security training must be provided to newly hired employees.

## User training

**Principle**

All employees and users using Grace's information systems will receive training to ensure that they are aware of potential information security threats.

**Objective**

To ensure that users are aware of information security threats and are equipped to support organisational security policies and supporting functional policies in the course of their normal work.

**Policy statements**

- All employees of the organisation and, where relevant, third party users, must receive appropriate training and regular updates in organisational policies and procedures.
- Employees must have regular security training.
- All employees must be appropriately trained on the use of Grace systems that they will be authorised to use.

## Physical and Environmental Security

**Principle**

Grace’s critical and sensitive business information processing facilities shall be housed in secure areas.

**Objective**

To ensure that a defined security perimeter, with appropriate security barriers and entry controls exist in all areas housing information processing facilities to prevent unauthorised access, interference and damage to business premises and information.

**Policy statements**

- Physical security perimeters must exist for all areas housing information processing facilities or identified as having special security requirements
- Appropriate entry controls must be installed for secure areas to ensure that only authorised personnel are allowed access.
- Delivery and loading areas must be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.
- Access to machine rooms must be restricted to only those people who are permitted to use the machines
- Access to all secure areas must be monitored for unauthorised access attempts
- Visitors to secure areas and areas housing information processing facilities must sign-in at a manned reception area prior to being allowed access to facilities.
- Visitors to secure areas must be escorted at all times and must wear some form of identification.
- Access privileges to restricted areas shall be reviewed regularly.

## Equipment Security

**Principle**

Information processing equipment should be physically protected from security threats and environmental hazards.

**Objective**

To prevent loss, damage or compromise of assets and interruption to business activities.

**Policy statements**

- Equipment must be sited and protected to reduce risks from environmental hazards and opportunities for unauthorised access.
- Equipment must be protected from power failures and electrical anomalies.
- Standards shall be developed detailing the minimum environmental controls required for facilities housing information and information processing systems.
- Power and telecommunications cabling carrying data or information services must be protected from interception or damage.

- Equipment must be maintained in accordance with manufacturer's instructions and/or documented procedures to ensure its continued availability and integrity.
- Any information processing equipment situated outside Grace’s secure perimeters, must be secured in a way equivalent to on-site equipment.
- Information must be erased from equipment prior to disposal or re use.
- No employee must be allowed to remove property from company premises unless they have obtained authority to do so from an approving manager.

## Information Processing Facilities

**Principle**

Information and information processing facilities must be protected to maintain confidentiality, integrity and availability of information.

**Objective**

To prevent compromise or theft of information and information processing facilities.

**Policy statements**

- A clear desk and a clear screen policy must be implemented in order to reduce the risks of unauthorised access, loss of, and damage to information.
- All users must ensure that information is not left unattended on their desks and are responsible for securing information when they leave their desks.
- Removal of any equipment, information or information facilities that belong to Grace from the premises must be strictly monitored and controlled.

## Compliance

**Principle**

The design, operation, use and management of information systems shall comply with legal, statutory, regulatory and contractual security requirements.

**Objective**

To avoid breaches of criminal and civil law, statutory, regulatory or contractual obligations.

**Policy statements**

- All relevant statutory, regulatory and contractual requirements must be explicitly defined and documented for each information system.
- Appropriate procedures must be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights and on the use of proprietary software products.
- Only authorized software and licensed products shall be installed on Grace systems.
- Controls must be applied to protect personal information in accordance with relevant legislation.

- Management must authorise the use of information processing facilities and controls must be applied to prevent the misuse of such facilities.

### Audit and Review

**Principle**

All information processing activities must be audited on a regular basis to ensure compliance with Information Security policies.

**Objective**

To ensure compliance of systems with organisational security policies and supporting functional policies and procedures.

**Policy statements**

- Managers must ensure that all information processing functional policies and procedures within their area of responsibility are carried out correctly and all areas within the organisation must be subject to regular review to ensure compliance with security policies and functional policies.
- Information systems must be regularly checked for compliance with information security policies and procedures.
- Audits of operational systems must be planned and agreed such as to minimise the risk of disruptions to business processes.
- Access to system audit tools must be protected to prevent possible misuse or compromise

## Violation Reporting and Escalation

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

## Legal or Regulatory Requirements

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

**Group Management**