eps

team:grace

Information Systems Security Policy

Reviewed January 2024

Date of Issue: January 2023

Table of Contents

1. Executive Summary

Grace recognises the dependency on information as a valuable asset and the importance of Information System Security to ensure assets are protected and preserved from all types of threats, whether internal or external, deliberate or accidental.

It is the responsibility of corporate management to develop and maintain adequate controls to ensure that the security objectives of the organisation are met. Therefore, the Grace Worldwide Information Systems Security Policy provides the foundation on which the security requirements of the organisation can be based.

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 commitment to Information Security
Information Security Policy	Policy covering Information Security at Grace
Information Systems Security Policy	This document

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.

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 Application Control

Principle

Grace must ensure that only approved, currently vendor supported and licenced software is run on corporate information systems.

Objective

To limit the ability for malicious software to operate within the corporate network and ensure that Grace complies with all licence agreements and copyright laws.

Policy statements

- Application control is to be implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set.
- Application control is to be implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.
- Operating system vendors’ latest recommended block rules are to be implemented to prevent application control bypasses.

- Application control is implemented using cryptographic hash rules, publisher certificate rules or path rules.
- Cryptographic hash rules, publisher certificate rules and path rules used for application control are validated at least annually
- When implementing application control using publisher certificate rules, both publisher names and product names are used.
- When implementing application control using path rules, file system permissions are configured to prevent unauthorised modification of folder and file permissions, folder contents (including adding new files) and individual files that are approved to execute.
- All users (with the exception of privileged users when performing specific administrative activities) cannot disable, bypass or be exempted from application control.
- Application control is configured to generate event logs for failed execution attempts, including information such as the name of the blocked file, the date/time stamp and the username of the user attempting to execute the file.
- All applications must be currently supported by the vendor.
- Application deployment will be subject to the Change Management Policy.
- Authorised applications will be categorised by the primary use of device (workstation, scanning computer, image QA).
- Authorised applications will be packaged for deployment via SCCM

4.2 Application Patching

Principle

Grace must ensure that all computer systems and network hardware are adequately protected against known vulnerabilities.

Objective

To ensure the integrity, confidentiality and availability of corporate information systems.

Policy statements

- Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.
- Security vulnerabilities in applications and drivers assessed as high risk are patched, updated or mitigated within two weeks of the security vulnerability being identified by vendors, independent third parties, system managers or users.
- Security vulnerabilities in applications and drivers assessed as moderate or low risk are patched, updated or mitigated within one month of the security vulnerability being identified by vendors, independent third parties, system managers or users.

- An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place.
- Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.
- Quarterly reviews should be conducted by the Information Technology department to ensure that automated patching solutions are operating correctly.
- Application patching is subject to the Change Management Policy

4.3 Microsoft Office Macro Settings

Principle

Grace must ensure that unauthorised code is not executed within the corporate network

Objective

Reduce security risk by securing or disabling Microsoft Office macros

Policy Statements

- Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros.
- Microsoft Office macros in documents originating from the internet are blocked.
- Microsoft Office macro security settings cannot be changed by users.

4.4 Application Hardening

Principle

Grace must ensure that default settings for applications are changed to ensure that applications are secure and unnecessary functionality is disabled.

Objective

Reduce security risk by ensuring security functions are enabled correctly and unnecessary functionality that might be the subject of future attacks is disabled.

Policy Statements

- Web browsers are configured to block or disable support for Flash content.
- Web browsers are configured to block web advertisements.
- Web browsers are configured to block Java from the internet.
- Microsoft Office is configured to disable support for Flash content.
- Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
- Vendor guidance is implemented to assist in hardening the configuration of Microsoft Office, web browsers and PDF viewers.
- Any unrequired functionality in Microsoft Office, web browsers and PDF viewers is disabled.

- The use of Microsoft Office, web browser and PDF viewer add-ons is restricted to organisation approved add-ons.
- If supported, Microsoft's Attack Surface Reduction rules are implemented.
- Standard users are prevented from bypassing, disabling or modifying security functionality of applications.

4.5 Administrative and Privileged Accounts

Principle

Grace must ensure that administration of systems, both on premise and cloud based, is performed securely.

Objective

Secure system administration allows Grace to be resilient in the face of targeted cyber intrusions by protecting administrator workstations and accounts from compromise, as well as making adversary movement throughout a network more difficult.

Policy Statements

- Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.
- Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.
- Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.
- Privileged users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access.
- The use of privileged accounts, and any activities undertaken with them, are monitored and audited.
- Privileged account names are subject to the same rules as user accounts for uniqueness, Non-reassignment and must be clearly identified as a privileged account.

4.6 Operating System Patching and Hardening

Principle

Grace must ensure that all systems are protected from external threats by applying controls at the operating system level.

Objective

To limit the ability for malicious software to operate within the corporate network.

Policy statements

- Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.

- Security vulnerabilities in operating systems and firmware assessed as high risk are patched, updated or mitigated within two weeks of the security vulnerability being identified by vendors, independent third parties, system managers or users.
- Security vulnerabilities in operating systems and firmware assessed as moderate or low risk are patched, updated or mitigated within one month of the security vulnerability being identified by vendors, independent third parties, system managers or users.
- An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place.
- Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.
- All operating systems should be regularly updated in accordance with the manufacturer's recommendation.
- Default operating system accounts are disabled, renamed or have their passphrase changed.
- Unneeded operating system accounts, software, components, services and functionality are removed or disabled.
- Windows local administrator accounts to be centrally managed (MS LAPS).
- Standard users are prevented from bypassing, disabling or modifying security functionality of operating systems.
- Standard users are prevented from running script execution engines in Microsoft Windows.
- UEFI secure boot functionality must be enabled on all workstations.
- Local hard drives must be encrypted on all end user devices.
- Workstations must be set to automatically lock after 5 mins of inactivity.
- User profiles should be deleted from workstations after 90 days with no login activity.

4.7 Multi-Factor Authentication

Principle

Grace must ensure that all users are authenticated by two or more factors before they can access any system or resource.

Objective

To minimise the risk of unauthorised access to Grace system or data resources

Policy Statements

- Multi-factor authentication is used to authenticate all users of remote access solutions.
- Multi-factor authentication is used to authenticate all privileged users and any other positions of trust.
- Multi-factor authentication is used to authenticate all users when accessing important data repositories.

- Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.
- Multi factor Authentication must be included in the requirements for any new systems that contain PII or other sensitive data.

4.8 Backup and Disaster Recovery

Principle

Grace must ensure the availability of systems and data resources in the event of system failure or catastrophe.

Objective

Minimise the risk of data loss in the advent of a disaster or ransomware attack.

Policy Statements

- Backups of important information, software and configuration settings are performed at least daily.
- Backups are stored offline, or online but in a non-rewritable and non-erasable manner.
- Backups are stored for three months or greater.
- Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.
- Partial restoration of backups is tested on a quarterly or more frequent basis.
- A Disaster Recovery Plan (DRP) must be developed and a Disaster Response Team identified.
- The DRP must identify all critical business systems and the owners.
- The DRP must clearly assign roles and responsibilities to the Disaster Response Team members
- The DRP should be reviewed at least annually or anytime there is a major system upgrade or replacement.
- The DRP should undergo a full test at least annually following a Rehearsal (Table Read) by the Disaster Response Team.

4.9 Identity and Access Management

Principle

Grace must ensure that all users of Grace systems are uniquely identified.

Objective

To ensure that only authorised users can access approved systems and data resources.

Policy Statements

- Uniqueness - each identifier (e.g., user ID) is unique; that is, each identifier is associated with a single person.
- Non-Reassignment - once an identifier is assigned to an individual it is always associated with that person. It is never subsequently reassigned to identify another person or entity.

- Account name will be the individual’s first initial plus their surname e.g. Janice Smith will have the account name jsmith.
- The display name will be set to the individual’s First Name (or nickname if this has been entered) and Surname e.g. Janice Smith (or Jan Smith if the nickname has been entered).
- This information will match exactly what has been entered in the HRIS which is the individual’s legal identity. Any deviation from this must be approved by the Chief Information Security Officer.
- If the account name based on these rules has already been assigned e.g. James Smith already has the account name jsmith, then the first initial of the individual’s middle name or the second letter of their first name is added and the process repeated until a unique account name has been created e.g. James Francis Smith would then become jfsmith or jafsmith.
- The account name also defines the email address e.g. jsmith@grace.com.au or jsmith@grace_removals.co.nz
- The use of generic, group or shared accounts shall be limited to situations of operational necessity and require the approval of the IT Manager or the Chief Information Security Officer.
- Sharing user account details (username and password) is a breach of this policy and must be reported as a Cyber Security Incident according to the corresponding policy.
- Password rules for Grace network accounts are detailed in the Password Policy.
- Access to other Grace systems will either be controlled through the Grace network account (Single Sign-On) or the necessary accounts will be created by IT Service Desk in accordance with the individual’s role.
- Once the new account(s) has been created, the details including temporary password will be provided to the new employee or their manager. The password must be set to expire at first login.
- When an employee leaves the company, the manager creates a termination request in the HRIS. This request is copied to the IT Service Desk so all assigned accounts can be disabled.
- All access to corporate systems and data is governed by the principle of least privilege e.g. access should be limited to resources essential for completion of assigned duties or functions and nothing more.
- All access to corporate systems and data is governed by the principle of segregation of duties. As far as is possible, no one person should be responsible for completing or controlling a task when it involves the potential for fraud, abuse or other harm.
- Authorisation for access to Grace systems is provided by the designated system owner. The list of systems and owners is provided in the Grace Information Security Charter – Table 1. Authorisation based on job role has been pre-approved by the system owners and will be granted when the new account is created.
- Any request for an employee to be granted access beyond what has been pre-approved must be submitted by the employee’s manager and approved by the system owner.

The IT Manager is responsible for auditing the network accounts on a regular basis and disabling accounts that are not being used.

- Audits should be conducted every month.
- Accounts older than one month that have never been logged in should be disabled.
- Accounts that have not been logged in during the previous 60 days should be disabled.

4.10 Malware and Anti-Virus

Principle

Grace must ensure that all information systems are protected against viruses as well as spyware, trojans, ransomware and other malware.

Objective

To maintain the integrity, confidentiality and availability of corporate information assets.

Policy statements

- All computers and servers that connect to the Grace corporate network must be protected by anti-virus and anti-malware software.
- Information systems owned by Grace must be protected by the approved corporate standard anti-virus and anti-malware solution.
- Anti-virus and anti-malware software must be installed and configured in accordance with the manufacturer’s standards for hardening and update schedules.
- Anti-virus and anti-malware software must be configured to quarantine suspicious files and internet sites immediately on detection and notify the Service Delivery team.
- The Service Delivery team will respond to every alert and if quarantine is not successful or if the incident is identified as high risk they will physical quarantine the system by disconnecting it from the network and arranging its return to IT for remediation.
- All email will pass through the corporate email security solution.
- Content and attachments will be blocked according to security best practices as recommended by email security vendor.

4.11 Network Security, Data Transmission and Encryption

Principle

Grace must ensure that information systems are secured by implementing controls around the confidentiality, integrity and availability of information.

Objective

To maintain the security of organisational information assets.

Policy statements

- With the exception of the guest wireless network, only Grace assets are to be connected to the corporate network.
- Where possible, network access is to be limited to specific devices.

- Network connections between sites will be encrypted.
- Traffic prioritisation will be used to ensure the availability of services.
- Remote access to the corporate network will only be provided to authorised users based on their role. Remote access is not granted by default.
- All customer data transmitted outside the Grace network must be secured by IPSec, SFTP or SSL
- Customer data transfers are from Grace hosted systems unless authorised by the IT Security Manager.
- Physical media may be used for data transfers if secured by encryption or a separate physical locking mechanism.

4.12 Vulnerability Management

Principle

Grace must ensure that all externally facing systems are maintained to limit exposure to known vulnerabilities.

Objective

To ensure the integrity, confidentiality and availability of information systems containing corporate and customer data.

Policy statements

- Grace Information Technology will conduct a vulnerability assessment each quarter and penetration test each year in conjunction with an accredited supplier.
- The assessment and test will cover all externally facing systems.
- The results will be reviewed by the Security Governance Team.
- All vulnerabilities rated Critical must be addressed within 3 business days.
- All vulnerabilities rated High must be addressed within 10 business days.
- All other vulnerabilities will be prioritised by the Security Governance Team and scheduled by Information Technology.
- Any vulnerabilities rated Critical or High that cannot be remediated, eg. waiting for vendor to provide solution, must be referred to the Group Manager - Compliance and Risk for action.

4.13 Internet Content Filtering

Principle

Grace must ensure that all reasonable actions are taken to block internet content that is malicious, disruptive, degrades network performance significantly or is inappropriate in a corporate environment.

Objective

To ensure that systems that have been optimised for the benefit of corporate activity are not impacted by inappropriate or malicious content.

Policy statements

- Internet content filtering will be enabled on all workstations wherever they are located.
- Access restrictions, including categories and/or time specific, are determined by the company directors.
- Any exception to the block list must be approved by a company director.
- Logging must be enabled for all user accounts.
- The ability to access content on the Internet does not imply permission to access that content. All users of Grace Worldwide computer systems must also abide by the terms of the Internet Usage policy.

4.14 Security of External Entities Access

Principle

Grace must ensure that information systems are secured in all cases where systems are accessed by third parties.

Objective

To maintain the security of organisational information processing facilities and information assets accessed by third parties.

Policy statements

- The risks associated with access to Grace information system by third parties must be assessed and appropriate security controls implemented. These will normally include the following.
  - Named user accounts will be created clearly identifying that the account has special privileges.
  - No email or Internet access unless it is integral to the service being provided.
  - Source address for external access will be limited to specific third party where possible.
  - The principle of least privilege will apply for access to all services.
  - File transfers will not be permitted. A separate, managed file transfer solution must be established if required.
- All risks resulting from third party access must be reassessed on a periodic basis, or whenever such risks change.
- Arrangements involving third party access to Grace's information systems must be based on a formal contract that must contain all necessary security requirements accompanied with appropriate responsibility and confidentiality undertaking. 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 contract.

- Access to 3rd Party systems is not permitted from the Grace environment unless specifically requested and approved by the IT Manager or CISO.

4.15 Media Destruction

Principle

Grace must ensure that devices storing corporate or client data are destroyed at the end of their useful life in such a way that the information is rendered unrecoverable.

Objective

Remove the possibility that data can be leaked outside the organisation's control.

Policy Statements

- All physical media (including backup tapes), hard drives or devices with non-volatile internal memory such as smartphones and tablets must be securely destroyed by shredding to a size less than or equal to 3mm.
- Confirmation of the destruction must be obtained and retained with the destruction request.

5. Related Policies

- IT Change Management Policy
- Technology Acceptable Use Policy
- Password Policy
- Information Asset Management 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 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.

7. Legal or Regulatory Requirements

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

Leon Hulme
Managing Director