Data Protection Policy

Version: 1.1

Date of Issue: February 2023

team:grace

Data Protection Policy

Table of Contents

team:grace

Data Protection Policy

1. Executive Summary

The purpose of this policy is to provide a uniform system for complying with global data protection laws, efficiently disposing of dated documents and ensuring that Grace Worldwide retains valuable documents. It is also extremely important for every Grace employee to be very familiar with the company's Data Protection Policy. Grace has an obligation to always protect all staff and customer's Personally Identifiable Information (PII). This policy document sets out what is expected of every Grace employee and contractor in the safe processing and security of data.

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.

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.
- **Personally Identifiable Information (PII)** is information about any Grace Worldwide customer, employee or contractor that includes but is not limited to:
    - Passport, visa(s) and immigration documents
    - National identification information eg. Social Security Number
    - Date of birth
    - Driver's license number
    - Medical information
    - Financial information eg. credit card details, Tax File Number (TFN)
    - Employment details
    - Home address, emergency contacts etc
- **Business records** include but are not limited to database entries, letters, emails, memorandum reports, data compilations, financial records, service files, payroll data, employee files and other business-related documents used by Grace Worldwide and its employees and contractors.

4. Principles and Policy Statements

4.1 General Data Privacy and Security

Principle

Grace Worldwide must ensure that all data is stored and accessed in a secure manner.

Objective

To reduce the risk of sensitive data being shared beyond the organisation in an uncontrolled manner including as a result of malicious activity.

Policy statements

- Grace employees and contractors will be issued account(s) for Grace systems based on their role.

- Holders of Grace system accounts must adhere to the principles of the Password Policy and ensure that they never share password details with anyone.
- Users of Grace computer systems must log off or lock their computers when away, even if only for a few minutes.
- Once the need for access is complete (employee termination, project completion), the account(s) must be disabled. No one is permitted to continue using the account of a former employee or contractor.
- All Grace equipment and devices must always be protected and securely kept. Should a Grace computing asset be broken, lost or stolen, it must be reported to IT immediately. This reporting requirement includes the loss of personal smartphones housing Grace data.
- Grace employees and contractors are not allowed to give control or access for any Grace-issued device to any non-Grace employee.
- Grace IDs, badges, keys, vehicles, credit cards, computers, and communication devices must never be given to non-Grace employees for custody or usage.
- Users of Grace computer systems should always save PII on Grace's corporate One Drive. No PII should be stored on portable media.
- All devices containing PII must always be kept secure and not left unattended, even when switched off.
- No Grace employee or contractor is to remove hard copy files containing PII from any office location. Any individual exception to this policy must be supported by written justification and approved by General Manager or Director on a case-by-case basis.
- The only cloud storage service allowed for storing of Grace Worldwide's data is the corporate One Drive. No other cloud storage services can be used.

4.2 Document Security and Storage

Principle

Grace Worldwide must ensure that any physical documents containing confidential or personally identifiable information are handled and stored securely.

Objective

To reduce the risk of sensitive data being shared beyond the organisation in an uncontrolled manner including as a result of malicious activity.

Policy statements

- All hardcopy confidential documents maintained by Grace must be stored in a secured area accessible to only those employees whose job requires them to have access. A desk or workstation is not a secured area.
- A secured area includes a locked drawer, cabinet or room. Access to these areas must be controlled and monitored. The keys must never be left in or near these locked areas or cabinets.
- When not in a secured area, the confidential documents cannot be left unsupervised while physical controls are not in place. When not in a secured area, precautions must be taken to obscure the confidential information from casual view, such as in an opaque file folder or envelope.

- Grace employees and contractors must not have more than three client folders outside of the secure storage at any time. Files removed from the original location for processing shall be stored in locked desk drawers or securely locked cabinets when not actively in use.
- Upon completion of the procedure that caused the file to be moved from its original secured location, all additional papers and documents shall be secured in the file and returned to the original secure location. At the end of the business day, there shall be no files left on desks, chairs, floors or unlocked boxes.
- All desks and cabinets containing PII must be securely locked at the end of the working day. The key to the locks must not be easily accessible. Confidential information must not be taken out of the office or left in an unoccupied vehicle or any other location that third parties may have access to.
- If there is a need to ship hardcopy documents containing confidential or personally identifiable information, care must be taken to ensure that envelopes or courier bags are securely closed with no information viewable. Shipping must include tracking and signature on delivery – no unattended delivery.

4.3 Data Retention

Principle

Grace Worldwide must securely maintain complete and accurate records for the period of their immediate use and to discard them thereafter – unless longer retention is required for historical reference, contractual or legal requirements, or for other purposes as stated in this policy.

Objective

To reduce the risk of sensitive data being shared beyond the organisation in an uncontrolled manner including as a result of malicious activity.

Policy statements

- Business records containing PII must be securely deleted or destroyed once the information is no longer needed for the purpose for which it was collected.
- Secure document and electronic media destruction is handled by Grace Destruction Services.
- Any records for services that did not proceed eg. a lost sale or cancelled service should have PII redacted after 90 days and any files or documents containing PII should be deleted after 120 days.
- Any records for services that have completed eg. a finished and closed relocation should have PII redacted after 180 days from completion date with the exception of international relocations involving import or export of goods which should have PII redacted after 270 days from completion date. Any files or documents containing PII should be deleted after 365 days.
- Redacting data should include purging any relevant log files of any PII.
- Each branch, department or business unit is responsible for adhering to these guidelines and monitoring staff compliance with them on a regular basis. The department manager is responsible for coordinating with IT the disposition of electronic records of former employees.
- Unless relocated under direction of the department manager, files of former Grace employees and contractors should be deleted a maximum of 2 years after termination date.
- Grace Worldwide has a legal duty to retain relevant documents that it knows or should have known are relevant to any legal action. Such documents also include those that could lead to the discovery of admissible evidence. Accordingly, all document destruction is automatically suspended when a lawsuit,

claim or government investigation is pending, threatened or reasonably foreseeable. In such a case, paper document destruction, as well as electronic destruction must cease immediately. In the case of electronic destruction, the IT department is responsible for ensuring that any automatic destruction program is disabled and reviewing all electronic systems that contain documents potentially relevant to the litigation or claim.

5. Related Policies

- Password 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 regulations.

Group Management