DISASTER RECOVERY POLICY

CHANGE HISTORY

Date	Version	Created by	Approved By	Description of change
08/10/2024	1.0	Bharath S	Ashwin Khosla	Basic document outline and submitted for review

Purpose

The purpose of the Disaster Recovery Policy at Veranda Learning is to outline the business plan executed in cases of a natural or manufactured disaster such as a cyclone earthquake strike. The primary objective is to ensure that the management team is prepared and equipped to handle disasters and keep the business operations running.

Scope

Data retention policy applies to following

Personnel

- InfoSec management team
- Senior and operational management
- Executive team

Equipment

- Business Critical information system

Background

Disasters rarely happen, so it is common for management teams to deprioritize or ignore planning for one. However, it is well documented that a written down and a formal plan with specific instructions to follow keeps the nerves out and is highly impactful in times of disaster.

This policy outlines the rules which the management at Veranda Learning has put to ensure that there is always an up-to-date and actionable disaster recovery plan in place. This disaster recovery plan is closely related to the business continuity plan policy.

Policy

Veranda Learning disaster recovery plan is the responsibility of each business unit, and information system. Each group in the company creates, manages, and keeps up-to-date the plan for their systems by working along with the InfoSec Team.

Emergency response Recovery plan

- Veranda Learning has an Emergency Response Plan that documents Who is to be contacted, when, and how? What must immediate actions be taken in the event of certain occurrences?
- The actions listed in this plan are per the business continuity plan and, at the minimum, contains
    - List of most business-critical information systems where the data is stored
    - List of all critical and essential internal and external services in order of priority in which they must be made available
    - Reference to each information system's data backup and restoration policies, ensuring that the right contacts and the steps for recovery are listed.
    - List the equipment, which is required to begin to provide services, list the order in which it is necessary

Succession and Responsibilities plan

- This plan describes the flow of responsibility when normal staff is unavailable to perform their duties.
- This plan also documents who oversees communication between both external and internal stakeholders.
- Internet and intranet provided by Veranda Learning should not be used for illegal or harmful activities such as hacking or the introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

Mapping with Industry Standards

This policy addresses the following risks related to Disaster recovery and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Data Breach	5.29 Information security during disruption 8.14 Redundancy of information processing facilities C 8.1 Operational planning and control
System failure	5.29 Information security during disruption 5.30 ICT readiness for business continuity 8.14 Redundancy of information processing facilities C 8.1 Operational planning and control
Natural Disaster (earthquake)	5.29 Information security during disruption 8.14 Redundancy of information processing facilities C 8.1 Operational planning and control
Man-made hazards (war, terrorism)	5.29 Information security during disruption 8.14 Redundancy of information processing facilities C 8.1 Operational planning and control
Physical Loss or damage	5.29 Information security during disruption 8.14 Redundancy of information processing facilities C 8.1 Operational planning and control

Enforcement

Disaster recovery policy is created and managed by the Infosec team by working with senior management team and operation teams such as support, infrastructure etc.
Each information system is also individually responsible to contribute their own plan for disaster recovery to the Infosec Team.
Infosec team is also responsible to ensure that the plan is tested, and mock exercises are conducted to verify the procedures

Non- Compliance

Violations of the policy may subject employees to disciplinary action, including removal of privilege to the systems, up to and including termination of employment. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable Veranda learning policies.
- Termination of employment.
- Legal action according to applicable laws and contractual agreements.

Validity and Document Management

The owner of this document is the management, who must check and, if necessary, update the document at least once every 12 months.