Personnel Security 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
To ensure that personnel security safeguards are applied to the access and use of information technology resources and data.

Scope
The Veranda Learning Personnel Security and Awareness Training Policy apply to all individuals responsible for hiring, onboarding, offboarding, and training of personnel given access to Veranda Learning Information Resources.

Background
Security personnel is expected to comply with a variety of methods designed to protect the companies they work for. Personnel security policy covers those methods that the organization employs to protect information systems from insider threats and malicious actors.

Policy
General
- For all roles within Veranda Learning, the hiring process should ensure the candidate has the necessary competence to perform the role and can be trusted to take on the role, especially for roles related to the use, management, or protection of information security.
- Information security responsibilities must be communicated to employees during the onboarding process.
- All employees must sign a Confidentiality/Non-Disclosure Agreement before being granted access to any information resource.
- Upon termination of employment, personnel must be reminded of confidentiality and non-disclosure requirements.
- Veranda Learning will provide all employees an anonymous process for reporting violations of information security policies or procedures.

Background Checks
- Background checks are required before employing Veranda Learning employees, regardless of whether a competitive recruitment process is used.
- Background checks may be required for employees who change positions in the company, obtaining more sensitive duties, as determined by Human Resources or the hiring manager.
- Background checks may be required for employees at any time after the employment start date, at the discretion of Human Resources or Executive Management.
- Contractors with access to **confidential information** must have a process for conducting background checks on applicable staff. An agreement must be put in place specifying the responsibilities for conducting background checks if a procedure is not currently being followed or in question.

Training and Awareness
- All new personnel must complete an approved **Security Awareness** training before or within 30 days of being granted access to any Veranda Learning **Information Resources**.
- All personnel, including third parties and contractors, must be provided with relevant information security policies to allow them to protect adequately Veranda Learning **Information Resources**.

- All personnel, including third parties and contractors, must acknowledge they have received and agree to adhere to the Veranda Learning Information Security Policies before they are granted access to Veranda Learning **Information Resources**.
- All personnel must complete the annual security awareness training.

Mapping with Industry Standards

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

Risk	Mapping to ISO 27001:2022
Impersonation	6.1 Screening
Lack of Awareness	6.3 Information security awareness, education and training 5.4 Management responsibilities C 7.3 Awareness
Roles and Responsibilities	6.2 Terms and conditions of employment 5.4 Management responsibilities 5.11 return of assets C 7.1 Resources
Unauthorized access	6.1 Screening 6.5 Responsibilities after termination or change of employment. C 7.1 Resources
Information Leakage	6.4 Disciplinary Process 5.4 Management responsibilities 6.6 Confidentiality or non-disclosure agreements
Theft	6.4 Disciplinary Process 5.4 Management responsibilities 6.6 Confidentiality or non-disclosure agreements
Fraud	6.4 Disciplinary Process 5.4 Management responsibilities 6.6 Confidentiality or non-disclosure agreements
Hiring incompetent workforce	6.1 Screening

Risk	Mapping to ISO 27001:2022
	C 7.2 Competence C 10.1 Continual improvement

Enforcement

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge and civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions, as well as both civil and criminal penalties.

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