INFORMATION CLASSIFICATION 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

1. PURPOSE, SCOPE AND USERS

The purpose of this document is to ensure that information is protected at an appropriate level.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all types of information, regardless of the form – paper or electronic documents, applications and databases, people's knowledge, etc.

Users of this document are all employees of Veranda Learning.

2. POLICY STATEMENTS

2.1 Steps And Responsibilities

Steps and responsibilities for information management are the following:

Step name	Responsibility
Entering the information asset in the Inventory of Assets	Management
Classification of information	Asset owner
Information labelling	Asset owner
Information handling	Persons with access rights in accordance with this Policy

If classified information is received from outside the organization, IT Management is responsible for its classification in accordance with the rules prescribed in this Policy, and this person becomes the owner of such an information asset.

2.2 Classification Of Information

2.2.1 Classification criteria

The level of confidentiality is determined based on the following criteria:

- Value of information – based on impacts assessed during risk assessment
- Sensitivity and criticality of information – based on the highest risk calculated for each information item during risk assessment
- Contractual obligations

2.2.2 Confidentiality Levels

All information must be classified into confidentiality levels.

Confidentiality level	Classification criteria	Access restriction
Public	Making the information public cannot harm the organization in any way	Information is available to the public
Internal use	Unauthorized access to information may cause minor damage and/or inconvenience to the organization	Information is available to all employees and selected third parties

Restricted	Unauthorized access to information may considerably damage the business and/or the organization's reputation	Information is available only to a specific group of employees and authorized third parties
Confidential	Unauthorized access to information may cause catastrophic (irreparable) damage to business and/or to the organization's reputation	Information is available only to individuals in the organization

The basic rule is to use the lowest confidentiality level ensuring an appropriate level of protection, in order to avoid unnecessary protection costs.

2.3 Information Labelling

Confidentiality levels are labelled in the following way:

- paper documents – the confidentiality level is indicated in the top right corner of each document page; it is also indicated on the front of the cover or envelope carrying such a document as well as on the filing folder in which the document is stored
- electronic documents – the confidentiality level is indicated in the top right corner of each document page
- information systems – the confidentiality level in applications and databases must be indicated on the system access screen, as well as in the top right corner of each consecutive screen displaying confidential information
- electronic mail – the confidentiality level is indicated in the subject or first line of the e-mail body
- electronic storage media (disks, memory cards, etc.) – the confidentiality level must be indicated on the top surface of such a medium
- information transmitted orally – the confidentiality level of confidential information to be transmitted in face-to-face communication, by telephone or some other means of communication, must be communicated prior to the information itself

2.4 Handling Classified Information

All persons accessing classified information must follow the rules listed in the following table. IT Manager must initiate disciplinary action each time the rules are breached or if the information is communicated to unauthorized persons. Each incident related to handling classified information must be reported in accordance with the Incident Management Procedure.

The method for secure erasure and destruction of media is prescribed in the document Veranda Learning Technologies Operating Procedures for Information and Communication Technology.

	Internal*	Restricted*	Confidential*
Paper documents	• only authorized persons may have access • if sent outside the organization, the document must be sent as registered mail • documents may only be kept in rooms without public access	• the document must be stored in a locked cabinet • documents may be transferred within and outside the organization only in a closed envelope • if sent outside the organization, the	• the document must be stored in a safe • the document may be transferred within and outside the organization only by a trustworthy person in a closed and sealed envelope • faxing the document is not allowed

	• documents must be frequently removed from printers or fax machines	document must be mailed with a return receipt service • documents must immediately be removed from printers or fax machines • only the document owner may copy the document • only the document owner may destroy the document	• the document may be printed out only if the authorized person is standing next to the printer
Electronic documents	• only authorized persons may have access • when files are exchanged via services such as FTP, instant messaging, etc., they must be password protected • access to the information system where the document is stored must be protected by a strong password • the screen on which the document is displayed must be automatically locked after 15 minutes of inactivity	• only persons with authorization for this document may access the part of the information system where this document is stored • when files are exchanged via services such as FTP, instant messaging, etc., they must be encrypted • only the document owner may erase the document	• the document must be stored in encrypted form • the document may be stored only on servers which are controlled by the organization • the document must not be exchanged via services such as FTP, instant messaging, etc.
Information systems	• only authorized persons may have access • access to the information system must be protected by a strong password • the screen must be automatically locked after 15 minutes of inactivity • the information system may only be located in rooms with controlled physical access	• users must log out of the information system if they have temporarily or permanently left the workplace • data must be erased only with an algorithm which ensures secure deletion	• access to the information system must be controlled through an authentication process using smart cards or biometric readers • the information system may only be installed on servers controlled by the organization • the information system may only be located in rooms with controlled physical access and identity control of

			people accessing the room
Electronic mail	• only authorized persons may have access • the sender must carefully check the recipient • all rules stated under "Information systems" apply	• e-mail must be encrypted if sent outside the organization	• all e-mails must be encrypted
Electronic storage media	• only authorized persons may have access • media or files must be password protected • if sent outside the organization, the medium must be sent as registered mail • the medium may only be kept in rooms with controlled physical access	• media and files must be encrypted • media must be stored in a locked cabinet • if sent outside the organization, the medium must be mailed with a return receipt service • only the medium owner may erase or destroy the medium	• media must be stored in a safe • media may be transferred within and outside the organization only by a trustworthy person in a closed and sealed envelope
Information transmitted orally	• unauthorized persons must not be present in the room when the information is communicated	• the room must be sound proof • the conversation must not be recorded	• no transcript of the conversation may be kept

*Controls are implemented cumulatively, meaning that controls for any confidentiality level imply the implementation of controls defined for lower confidentiality levels – if stricter controls are prescribed for a higher confidentiality level, then only such controls are implemented.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Number of incidents related to unauthorized access to information
- Number of information assets classified with an inappropriate confidentiality level

3. Mapping with Industry Standards

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

Risk	Mapping to ISO 27001:2022
Loss of CIA (confidentiality, Integrity and Availability)	5.10 Acceptable Use of Information and Other Associated Assets 5.12 Classification of Information 7.9 Security of Assets Off-premises 7.10 Storage Media
Non-adherence to laws and regulations	5.12 Classification of Information

Risk	Mapping to ISO 27001:2022
Unauthorized access	5.12 Classification of Information 7.9 Security of Assets Off-premises 7.10 Storage Media
Information Leakage	5.12 Classification of Information 7.9 Security of Assets Off-premises 7.10 Storage Media
Theft	5.12 Classification of Information 7.9 Security of Assets Off-premises 7.10 Storage Media
Fraud	5.12 Classification of Information 7.9 Security of Assets Off-premises 7.10 Storage Media

4. 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.

5. VALIDITY AND DOCUMENT MANAGEMENT

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