MOBILE DEVICE 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

This policy defines connecting to **Veranda Learning** networks from any mobile device. These standards prevent unauthorized access to mobile devices both within and outside the organization's premises. The objective of this policy is to ensure the security of teleworking and the use of mobile devices.

Scope

This policy applies to all mobile devices, whether owned by Veranda Learning or by employees that have access to Veranda Learning information Assets (i.e., networks, data, and systems).

Applications used by employees on their own personal devices that store or access corporate data/information, such as cloud storage applications, are also subject to this policy.

Mobile devices are defined to include desktop systems in a telework environment. Mobile devices include, but are not limited to:

- Laptop computers.
- Palmtop computers.
- Tablet computers.
- Smartphones.
- Personal Digital Assistants (PDAs).
- FireWire devices.
- Universal Serial Bus (USB) devices.
- Flash drives.
- Modems.
- Handheld wireless devices.
- Wireless networking cards.
- Wireless hotspots.
- Portable music players; and
- Any other existing or future mobile computing or storage device is defined as Personal Electronic Device (mobile device)

Background

Security must be central to an organization's workforce mobility strategy in order to protect corporate data, maintain compliance, mitigate risk and ensure mobile security across all devices. With data flowing across public networks, to and from devices that are easily lost or stolen, protecting data becomes a paramount concern and the primary driving force for implementing Mobile Device Management policy.

Policy

Mobile Device Management

Employees are expected to comply with Company policies regarding protecting the employer's confidential and proprietary information when using personal devices.

- Establishes usage restrictions and implementation guidance for organization-controlled mobile devices.
- Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational systems.
- Monitors for unauthorized connections of mobile devices to organizational systems.

- Enforces requirements for the connection of mobile devices to organizational systems.
- Disables system functionality that provides the capability for automatic execution of code on mobile devices without user direction.
- Issues specially configured mobile devices to individuals traveling to locations that the organization deems significant risk.
- Applies inspection measures to mobile devices returning from locations that the organization deems to be of significant risk before the device is connected to the organization's network.

Business Requirements

- A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
- The organization centrally manages mobile devices.
- The organization provides the capability to remotely purge information from mobile devices.
- The organization restricts the connection of personally owned, mobile devices to organizational systems. (*Reference:* Employee-owned Device Policy BYOD)

Technical Requirements

- Devices must use the following Operating Systems: Android 10 or later, iOS 10 or later.
- Devices must store all user-saved passwords in an encrypted password store.
- Devices must be configured with a secure password that complies with Veranda Learning's password policy. This password must not be the same as any other credentials used within the organization.
- Only devices managed by IT will be allowed to connect directly to the internal corporate network.
- These devices will be subject to valid compliance rules on security features such as encryption, password, key lock. These policies will be enforced by the IT department using Mobile Device Management software.

User Requirements

- Users may only load corporate data essential to their role onto their mobile device(s).
- Users must immediately report all lost or stolen devices to Company's IT.
- If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident in alignment with Veranda Learning's incident handling process.
- Devices must be kept up to date with the manufacturer or network-provided patches. At a minimum, patches should be checked weekly and applied at least once a month.
- Users must not load pirated software or illegal content onto their devices.
- Devices must be encrypted in line with Veranda Learning's compliance standards.
- Applications must only be installed from official platform-owner-approved sources.
- Users must ensure that backup is performed periodically, and sufficient network bandwidth is available to perform a backup.
- Users to notify Company's IT immediately if they notice error messages from Anti-Virus products.

The above requirements will be checked regularly and should a. Should noncompliant that result, it in the loss of access to email, a device lock, or in particularly device wipe in particularly severe cases that may result in a full or partial wipe of the device, or other interaction by IT.

- A device is jailbroken/rooted.

- A device contains an application known to contain a security vulnerability (if not removed within a given time frame after informing the user)
- A device is lost or stolen.
- A user has exceeded the maximum number of failed passwords attempts.

Exceptions

There are company-owned internal devices used only for testing (i.e., mobile applications). The standards above do not apply to those devices since none have data plans, do not access or store any PII, and never leave the company network.

Mapping with Industry Standards

This policy addresses the following risks related to Mobile Device Policy and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Malware	8.1 User endpoint devices 6.7 Remote Working
Loss of CIA (Confidentiality, Integrity and Availability)	8.1 User endpoint devices 6.7 Remote Working 5.3 Segregation of duties
Non-adherence to laws and regulations	8.1 User endpoint devices 6.7 Remote Working 5.3 Segregation of duties 5.10 Acceptable use of information and other associated assets
Unauthorized access	8.1 User endpoint devices 6.7 Remote Working 5.3 Segregation of duties
Information Leakage	8.1 User endpoint devices 6.7 Remote Working 5.3 Segregation of duties 5.10 Acceptable use of information and other associated assets
Theft	8.1 User endpoint devices 6.7 Remote Working 5.3 Segregation of duties

Risk	Mapping to ISO 27001:2022
Fraud	8.1 User endpoint devices 6.7 Remote Working 5.3 Segregation of duties
Copyright	8.1 User endpoint devices 6.7 Remote Working

Enforcement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

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.