



Bring Your Own Device (BYOD) Policy

Document Number: OG-BYOD-POL-004

Version: 1.0

Effective Date: 1 November 2025

Next Scheduled Review: 1 November 2026

Policy Owner: Chief Security & Compliance Officer (CSCO)

Document Review

This policy applies to:

- All employees using personal devices for business purposes
- IT, Security, Finance, Product and Operations teams
- Contractors and consultants who access Orchestrate Global systems using personal devices
- Third-party vendors or partners who access corporate systems, applications, or networks via personal devices

Approvals

Name	Position	Signature	Date
Oleksii Bondarenko	Chief Security & Compliance Officer		1 November 2025
Kevin Kegera	Chief Commercial Officer		1 November 2025
Preston Obadan	Chief Executive Officer		1 November 2025



Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Roles and Responsibilities
5. Eligibility and Enrollment
6. Minimum Security Requirements for Personal Devices
7. Authentication and Access Control
8. Network and CDE (Cardholder Data Environment) Restrictions
9. Acceptable and Unacceptable Use
10. Data Handling and Storage Rules
11. Privacy, Monitoring and User Consent
12. Lost or Stolen Device Procedures
13. Updates, Patch Management and Anti-Malware Requirements
14. Cloud Storage and Backup Restrictions
15. Offboarding and Remote Wipe Procedure
16. Legal and HR Considerations
17. Third-Party and Vendor BYOD Requirements
18. Policy Exceptions
19. Auditing and Continuous Monitoring
20. Revision History

1. Purpose

This policy defines how personal devices may be used to access Orchestrate Global systems, applications, networks or data. The purpose is to ensure that personal devices do not introduce security risks, expose cardholder information or compromise the confidentiality, integrity or availability of corporate data.

2. Scope

This policy applies to any personally owned device used to conduct company business or access Orchestrate Global systems. This includes laptops, smartphones, tablets and wearable devices capable of data synchronization. It applies to all environments, including production, test, staging and remote access setups.

Company-owned devices are not covered by this policy; they are addressed under the Corporate Asset Security Policy.



3. Definitions

Term	Meaning
Bring Your Own Device (BYOD)	The use of personally owned devices for work-related tasks or system access
Cardholder Data Environment (CDE)	Systems that store, process or transmit payment card data
Mobile Device Management (MDM)	Technology used by Orchestrate Global to manage, secure, and remotely wipe devices
Remote Wipe	The authorized removal of company data from a personal device
Full Disk Encryption	Encryption of an entire device storage, typically using AES-256

4. Roles and Responsibilities

Role	Responsibilities
Chief Security & Compliance Officer	Owns this policy, approves exceptions, and oversees enforcement
CTO and IT Security Team	Implements MDM, monitors device compliance, enforces encryption and access control requirements



Human Resources	Ensures BYOD policy acceptance is incorporated into onboarding and employment agreements
Employees and Contractors	Must comply with all requirements, report lost devices, and consent to data security controls
Vendors and Third Parties	Must sign BYOD agreements and follow equivalent or stronger security standards

5. Eligibility and Enrollment

1. Employees and contractors must submit a BYOD Access Request to IT Security.
2. Approval is required from the department manager and CSCO.
3. Devices must be registered with Orchestrate Global's MDM solution prior to accessing any internal application or email.
4. The user must sign the BYOD Consent and Acknowledgment Agreement before access is granted.

6. Minimum Security Requirements

All approved personal devices must meet the following minimum security standards:

- Full disk encryption must be enabled (for example: BitLocker, FileVault or equivalent).
- The device must be protected by a password, PIN, fingerprint or secure biometric authentication.
- Automatic locking must be enabled with a maximum inactivity timeout of 5 minutes.
- An up-to-date anti-malware solution must be installed where supported by the operating system.
- Operating system and security patches must be applied regularly.
- Jailbroken or rooted devices are strictly prohibited.
- Devices must connect only through approved secure networks or VPN configurations.

7. Authentication and Access Control

- Multi-factor authentication is required for access to corporate systems.
- Unique user credentials are mandatory; shared accounts are not permitted.



- Users receive only the minimum level of access required to perform their duties.
- Access to the Cardholder Data Environment from BYOD devices is restricted to approved roles and may be limited to virtual desktop infrastructure or secure remote sessions.

8. Network and Cardholder Data Environment (CDE)

Restrictions

- Personal devices must not directly connect to internal CDE networks.
- Remote access is only permitted through secure VPN or bastion host systems that enforce encryption, access control and monitoring.
- Data may not be copied, downloaded or stored locally from CDE systems unless explicitly authorized and encrypted.

9. Acceptable and Unacceptable Use

9.1 Acceptable Use

Personal devices may be used for:

- Accessing corporate email, calendars, approved internal applications and collaboration platforms.
- Participating in secure virtual meetings and communications using approved tools.
- Performing job-related functions as authorized by the user's role and access level.

9.2 Unacceptable Use

The following actions are prohibited when using personal devices for business:

- Storing unencrypted Cardholder Data (CHD) or Sensitive Authentication Data (SAD).
- Circumventing security controls, disabling MDM, encryption or malware protection.
- Downloading or using unlicensed software, torrents or applications that compromise security.
- Connecting devices to open, insecure Wi-Fi networks without VPN.
- Sharing devices or credentials with unauthorized individuals, including family members.
- Using personal devices to host, proxy or tunnel unauthorized network connections into corporate systems.

10. Data Handling and Storage Rules



- Cardholder Data and Sensitive Authentication Data must never be stored on a personal device unless explicitly authorized by the CSCO and protected with strong encryption.
- Business emails, files and documents stored on personal devices must be within secure, sandboxed corporate containers managed by the MDM platform.
- Screenshots, local downloads or caching of internal dashboards, logs or payment reports is strictly prohibited unless permitted and encrypted.
- Data retention policies apply equally to personal devices; expired files must be securely deleted.

11. Privacy, Monitoring and User Consent

- Orchestrate Global respects user privacy; however, corporate data on personal devices is subject to monitoring and control.
- Employees must sign the BYOD Consent Form authorizing the company to:
 - Enforce device security settings.
 - Deploy MDM software.
 - Remotely wipe corporate data in case of loss, theft, resignation or contract termination.
- Personal data (e.g., photos, personal messages, private applications) is not accessed, unless legally required.
- Monitoring is limited to corporate applications, connections to company systems, security posture and compliance

12. Lost, Stolen or Compromised Devices

- Users must report lost or stolen devices within 1 hour to IT Security at security@orchestrate.global
- IT will remotely lock or wipe the device's corporate data container.
- A security incident report is generated and investigated in accordance with the Incident Response Plan.
- Replacement devices must undergo the full enrollment process before access is restored.

13. Updates, Patches and Anti-Malware Requirements

- Devices must be regularly updated with the latest operating system versions and security patches.
- If a device is found to be out-of-date or vulnerable, access to corporate resources will be suspended until patched.
- Anti-malware or endpoint protection must be enabled where available; real-time protection and automated scanning must remain active.



- Devices must allow automatic updates for MDM software; disabling or tampering with these services is not allowed.

14. Cloud Storage and Backup Restrictions

- Only approved corporate cloud services (such as company-authorized file storage platforms) may be used to store corporate data.
- Personal cloud services (Google Drive, Dropbox, iCloud, etc.) are prohibited for corporate document storage unless explicitly approved and encrypted.
- Automatic device backups must exclude corporate application data unless encrypted and stored in approved environments.

15. Offboarding and Remote Wipe Procedure

- When an employee or contractor leaves Orchestrate Global, IT Security will remove corporate profiles, email accounts, VPN certificates, encryption keys and data from their personal device using MDM.
- If the device is not reachable, the user must present the device for manual sanitization or provide written confirmation of data removal.
- Access to internal systems, credentials and authentication tokens will be revoked immediately upon termination.
- Failure to comply with offboarding procedures may result in withholding of final payments or legal action.

16. Legal and HR Considerations

- Participation in the BYOD program is voluntary and subject to employee agreement.
- The company is not responsible for personal data loss during remote wipe when performed to protect corporate data.
- Orchestrate Global will not reimburse employees for wear, damage or loss of personal devices.
- Compliance with data protection laws and employment regulations is mandatory in all regions where the company operates.

17. Third-Party and Vendor BYOD Requirements

- Vendors or contractors using personal devices to access Orchestrate Global systems must sign the BYOD Agreement and Vendor Security Addendum.



- Third parties must maintain equivalent or stronger security controls.
- Audits or assessments may be conducted to verify compliance.
- Violations may lead to termination of contracts and reporting to relevant authorities.

18. Policy Exceptions

- Any deviation from this policy requires written approval from the Chief Security & Compliance Officer.
- Exceptions must include justification, risk analysis, compensating controls and expiration date.
- All approved exceptions are logged and reviewed quarterly.

19. Auditing and Continuous Monitoring

- The IT Security team will perform periodic audits of device compliance, including encryption status, patch levels and MDM enrollment.
- Non-compliant devices will be blocked from accessing corporate resources until remediated.
- Quarterly internal audits verify whether this policy is being followed.
- Records of audits, violations and enforcement actions will be retained for no less than 12 months.

20. Revision History

Version	Date	Description	Author
1.0	1 November 2025	Initial policy issuance	CSCO

End of Document