Bring Your Own Device (BYOD) Policy

Version number	2.2
Last Approved	Jun 19, 2025
Classification	PUBLIC

Overview

The Bring Your Own Device (BYOD) Policy defines terms for access Company systems using non-Company issued devices.

Applicability

The applicability of this statement falls under the purview of the Security Documentation Overview.

Purpose

The purpose of this policy is to outline the Company's standards for accessing Company systems via non-Company assets to ensure the security and privacy of Company systems and data.

Scope

This policy applies to all employees, contractors, and business partners and their devices they may use to connect to the Company’s systems.

Definitions

For the purposes of this policy the following definitions will apply:

- **Bring Your Own Device (BYOD)**: Refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device.
- **Mobile Devices**: phones, tablets, etc.

- **Computer Systems**: Desktop, laptop or any other type of workstation, including virtual machines.

BYOD Policy

- If provided, all employees and contractors must use company-issued devices only.
- Any use of non-Company devices must be pre-approved.
- All devices are subject to our Conditional Access policies, which automatically allow or block access based on the conditions listed on the policy list.
- IT support for authorized non-Company devices is provided on a best effort basis only.

BYOD Authorisation Process

- All BYOD Mobile Devices must be enrolled in the Company's Mobile Device Management (MDM) solution.
- All BYOD Computer Systems must be approved before usage. Such usage may include emergency access, short-term contractor access, etc.
- BYOD Computer Systems will only be approved for short-term usage not to exceed 3 months.
- All requests for the authorisation must be submitted via the IT Service Desk with business justification for the BYOD usage.

BYOD System Requirements

Mobile Devices

- To access the Company's Google Workspace services, the device must be MDM-enrolled and have dedicated mobile Google apps (Gmail, Google Drive, etc.) installed. Mobile Browsers and Non-Google applications are not supported, and access will be blocked.
- Supported mobile operating system versions and/or patches must be installed within 14 days after the release.
- The following mobile operating versions are supported:
  - Apple devices (iOS/iPadOS, etc.): the latest release only
  - Android devices: the last 2 releases

Computer Systems

All approved BYOD Computer systems must be configured to align with the Company's Security Baselines Policy.

All users must access Google Workspace and Microsoft 365 environments via a reverse proxy service, see Netskope - Reverse Proxy Service for more details.

Additional Responsibilities

- **Employees using approved non-Company devices must take all reasonable steps to:**
  - Lock the screen of the workstation before leaving your desk.
  - Ensure that device login credentials are not shared with 3rd party or family members.
  - Comply with Company policies regarding mass storage devices.
  - Delete any Company data stored on the device when no longer required.
  - Prevent synchronizing Company data to personal storage repositories like Personal OneDrive, Personal Google Drive, etc.
  - Notify IT Services immediately if the BYOD device is lost, stolen, or otherwise compromised in any way.

Monitoring and access

- **LTG will not routinely monitor non-Company related aspects of BYOD devices. However, it does reserve the right to:**
  - Prevent access to a particular device from either the wired or wireless networks, or both.
  - Prevent access to all systems or particular systems.
  - Disconnect any device that places the Company's services or network environment at risk.
  - Take all necessary and appropriate steps to retrieve Company information.

- Remember, the option to use your personal devices is a completely voluntary choice and a convenience. We expect that all employees should be able to fulfil their work responsibilities using company-provided devices.

- Company reserves the right to remove Company data from BYOD devices by using secure erasure, also known as remote wiping, if deemed necessary.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the Security Documentation Overview.

Document control

> This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Aleksandr Zaldak	
Author(s)	@Aleksandr Zaldak	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Jun 19, 2025
	@Aleksandr Zaldak - IT Infrastructure Manager	Jun 19, 2025
Review cycle	ANNUAL	
Next review date	Mar 6, 2026	

Version History

Date	Author(s)	Version	Changes
Jun 19, 2025	@Aleksandr Zaldak @angelina.kilmer @Art Machado @Paul Gordon	2.2	Referenced Security Baselines Policy in BYOD System Requirements
Jun 6, 2025	@angelina.kilmer @Aleksandr Zaldak @Art Machado	2.1	Updated definition of BYOD devices; clarified security and privacy measures

	@Paul Gordon		
Mar 7, 2025	@Aleksandr Zaldak @Art Machado	2.0	Annual review
Nov 1, 2024	@angelina.kilmer	1.4	Changed Policy classification from Confidential to Public
Jul 26, 2024	@Aleksandr Zaldak	1.3	Highlighting the fact that employees must use company-issued devices only and that the use of non-mobile or tablet BYOD devices must be pre-approved. Removed reference to old policy.
Dec 4, 2023	@Aleksandr Zaldak	1.2	Annual review/sign off.
Nov 8, 2023	@Aleksandr Zaldak @Art Machado	1.1	Full review of the policy. Language and content has been changed to ensure it meets the requirements of everyone within the scope of the policy.
Mar 1, 2018	@Aleksandr Zaldak	1.0	Original