Bring Your Own Device (BYOD) Policy

Version number	1.4
Last Approved	Dec 4, 2023
Classification	PUBLIC

Overview

The Bring Your Own Device (BYOD) Policy defines who can access LTG systems using non-LTG devices, their responsibilities in doing so, and LTG monitoring and access to the device.

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 use of assets not owned by The Company so that they are used and managed securely, consistently, and appropriately in order to ensure privacy and protection of Company and customer data.

Scope

This policy applies to all employees, contractors, and business partners and their devices they may use to connect to the LTG network, including, but not limited to:

- Mobile phones
- Tablets
- Desktop and laptop computers
- Portable storage and removable storage devices

BYOD Policy

Implementation

1. If provided, all employees must use company-issued devices only.
2. The use of non-mobile or tablet BYOD devices must be pre-approved.
3. All BYOD systems are subject to our Google Context-Aware-Access Policy, which automatically allows or blocks access based on the conditions listed on the policy list.

4. Google Chrome is the only supported Internet Browser for access. Firefox, Edge, Opera, and Private browsing are not supported, and access will be automatically blocked.
5. IT support for BYOD devices is provided on a best efforts' basis only. Device owners must comply with the controls detailed in this document.

Responsibilities

4. **Employees using BYOD must take all reasonable steps to:**
    a. Prevent theft and loss of company data
    b. Keep information confidential where appropriate
    c. Maintain the integrity of data and information
    d. Take responsibility for any software they download onto their device
    e. Ensure that software on personally owned devices is appropriately licenced

5. **Employees using BYOD must:**
    a. Configure and align device configuration to meet minimum security baselines as per Security Baselines policy.
    b. Do not “jailbreak” or “root” your mobile device, as it removes the manufacturer’s protection against malware.
    c. Enroll their BYOD devices in LTG Mobile Device Management, which mandates using dedicated Google apps like the Gmail app, Google Calendar app and Google Drive app to access your work email, calendars, Google files, etc. All other desktop or mobile clients will not be supported and will be blocked from access.
    d. Be aware of any Data Protection issues and ensure personal data is handled appropriately.
    e. Not hold any information that is classified as **CONFIDENTIAL** or of commercial value on personally owned devices. Instead, they should use their device to make use of the many services that the LTG offers over the internet. See Data Classification and Handling Policy for more information.
    f. Non-public LTG information may not be stored on local disc drives or unapproved cloud storage services (for example personal Google Drive, personal Dropbox, etc.)
    g. Non-public company information should not be stored longer than necessary and should be deleted as soon as possible once it is no longer required. This includes information contained within emails.
    h. Ensure that no LTG information is left on any personal device indefinitely. When disposing, selling or transferring ownership of a personal device, any LTG information must be irreversibly purged in accordance with the Data Destruction Policy.
    i. Report the loss of any device containing LTG data (including email) to the IT Help Desk within 24 hours.
    j. Report any security breach immediately to the Security Service Desk in accordance with the Incident Reporting Policy.

Monitoring and access

4. **LTG will not routinely monitor personal devices. However, it does reserve the right to:**
    a. Prevent access to a particular device from either the wired or wireless networks, or both
    b. Prevent access to all systems or particular systems.
    c. LTG reserves the right to disconnect any device that places LTG services or network environment at risk
    d. Take all necessary and appropriate steps to retrieve information owned by the LTG

5. 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.

6. LTG reserves the right to remove LTG data from BYOD devices by using secure erasure, also known as remote wiping, if deemed necessary. The company will do its best to limit the scope and need for erasure, but it’s not always possible or practical, which means that secure erasure may affect all data on the BYOD devices.

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	Dec 4, 2023
	@Aleksandr Zaldak - IT Infrastructure Manager	Dec 4, 2023
Review cycle	ANNUAL	
Next review date	Dec 3, 2024	

Version History

Date	Author(s)	Version	Changes
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