Company IT Device Usage Policy (End-Users) Version 1.0

	Name	Position	Signature	Date
Prepared by:	**Sackthavy LASICHAN**	**Application Specialist**		04/10/2024
Reviewed by:	**Norman Cunanan**	**IT Manager**		04/10/2024
Approved by:	**Sihamano BANNAVONG**	**Chief Executive Officer**		04/10/2024

I. Policy outline

This policy serves as a guideline for the use of IT devices (computers, laptops, tablets, phones, and related accessories) assigned to staff within our group for company business purposes. It aims to ensure that all company-issued devices are used responsibly, securely, and in compliance with IT protocols to protect company data and systems.

For damage protection, policy **KST-IT-DMP-001** will apply.

II. Scope

This policy applies to all staff in the KST Group who have been assigned company IT devices for business purposes. Before receiving any device from the IT department for work-related use, staff members are required to read, understand, and acknowledge this policy. The goal is to ensure that employees are aware of their responsibilities in using these devices securely and in accordance with company guidelines.

1. General Usage:

- IT devices are provided to staff solely for company business purposes.
- Internet usage on the devices must comply with the company's acceptable use policy.
- Employees are not permitted to install, uninstall, or modify any software or applications without prior approval from the IT department.
- All installation requests must be submitted via the company's IT support system.
- All data on company devices, including emails and documents, is the property of the company.
- Employees must not attempt to bypass or disable security settings or software installed by IT.
- Only company-approved applications are permitted; unauthorized applications will be removed during routine checks.
- Issues, malfunctions, or suspected security breaches must be reported to IT immediately.

2. Regular IT Reviews:

- IT will conduct Inventory of all devices every 6 months to ensure compliance with security protocols.
- These reviews will include a check of applications, system settings, and security patches.
- Employees are required to submit their devices for inspection upon request; non-compliance may lead to suspension of privileges.
- Unauthorized software or data discovered during reviews will be removed, and the employee may face disciplinary action.
- IT will document all inspections for audit and accountability purposes.

III. Additional Provisions

1. IT device Assignment and Return:

- Employees will be assigned IT devices based on job requirements and must return the devices upon termination of employment or reassignment unless otherwise directed by IT.
- IT will maintain an inventory log for tracking all issued IT devices.

2. Personal Use:

- Minimal personal use of devices is permitted provided it does not interfere with work responsibilities or security requirements. All personal use must comply with the company's acceptable use policy.

3. Reporting Lost or Stolen Devices:

- Employees must report any lost or stolen device to the IT department immediately. IT will then initiate security protocols to safeguard company data.

4. Updates and Maintenance:

- Employees are responsible for ensuring their devices are updated as per the schedule provided by IT. IT will assist with updates that require administrative privileges.

5. Training:

- Employees must attend mandatory training sessions on device security and best practices as scheduled by the IT department.
- Employees are required to read the cybersecurity awareness updates sent monthly through the Company Communication Platforms, such as Email, WhatsApp Group, Line Apps, and any other company communication platforms. This ensures that employees stay informed about the latest security threats and safe practices.

6. Sanctions for Non-Compliance:

- Non-compliance with this policy may result in disciplinary action, including suspension of device privileges, up to termination of employment.

7. Review and Update of Policy:

- This policy will be reviewed annually or as needed by the IT department to ensure it remains up-to-date with technological and regulatory changes.

IV. Policy Effective

This policy will become effective after being signed by the relevant individuals. Users must adhere to these guidelines to ensure efficiency and professionalism. This policy supersedes any previous device usage policies and will remain in effect until a newer version is approved. Non-compliance may result in suspension of device privileges or further disciplinary actions.