Device Loss or Theft SOP

Purpose

To establish a clear and secure protocol for responding to the loss or theft of company-issued electronic devices. This ensures the protection of sensitive data, compliance with applicable regulations, and continuity of operations. This SOP applies to all company-issued devices assigned to employees, contractors, interns, or volunteers.

1. Upon notification, log the incident in the ticketing system. Record device type, assigned user, serial number (if applicable), last known location and time of loss/theft, and circumstances surrounding the incident. If not reported within one hour of discovery, flag for follow-up with supervisor.
2. Assign priority level based on data sensitivity and user role.
3. Immediately disable Microsoft 365 and sessions for the user. Also disable VPN access (if applicable) and other SSO-connected services.
4. If device is enrolled in a device management tool, initiate remote lock or wipe.
5. Review the Microsoft account and device login activity.

* *If no unauthorized access is found*: No password change is necessary.
* *If unauthorized access is detected*: Immediately change the employee’s Microsoft account password. Reset credentials for other connected platforms.

1. Use device management tools to check last known location. Document the location in the incident log.
2. Escalate based on status.

* *If stolen*: File a report with local law enforcement. Request the employee to obtain a police report number and forward it to IT.
* *If lost*: Attempt retrieval if the device is in a known or reachable location. If retrieval fails, treat it as a stolen device and proceed accordingly.

1. If unable to retrieve, flag asset in inventory or device management system as “LOST/STOLEN – DO NOT DEPLOY”. If applicable, issue a replacement device and log the replacement in device management system.
2. Ensure incident record is complete with timeline of actions, tools used, accounts affected, and remediation measures that were taken.
3. Mark ticket for review if negligence is suspected or remote wipe was not possible. If negligence is confirmed, notify HR or supervisor for their review.

Review this SOP annually or after any device-related incident that exposes process gaps.