Information Security – Software Asset Management Policy

July 26, 2023

1. Purpose

Software asset management is the process of procuring, identifying, tracking, maintaining, and removing software on Company assets. This *Software Asset Management Policy* provides the policies for governing the software asset lifecycle while in use by Belize Telemedia Limited and or its subsidiaries (hereinafter collectively referred to as **"BTL"**). Software assets include both operating systems and software resources. A software inventory must be created and maintained to support the enterprise's mission and to help ensure only authorized software is installed and used. This software inventory must be up-to-date and reflect the current state of software across the enterprise.

2. Scope

This policy applies to all staff employed at BTL who use and or interact with company information utilizing specific applications. All software authorized by the organization will be managed by IT Operations in a Software Asset inventory Tool and vetted by the Information Security Team.

Compliance with this Policy shall form an express condition of employment for any person employed at Belize Telemedia Limited.

3. Responsibility

Responsibility to ensure proper management of authorized Software Assets to be utilized by BTL to reduce risk, resides with the Chief Operation Officer. The Information Security Team, under the direction of COO, is responsible for setting local standards and policies for the acceptable use of these assets throughout its lifecycle, while IT Operations manages operational process of acquisition through to removal.

4. Policy

4.1 Procurement

1. All requests must be sent to COO ServiceDesk for review and approval.
2. Reviews will be conducted by the IT Operations and Information Security and Data Privacy committee. Additional time to get a response on a request may be required depending on the use case and necessary testing.
3. Once approved, and procurement is necessary with an identified budget, only individuals from IT support can initiate purchase with the Procurement Team.
4. IT must maintain a list of approved software and the Procurement Team maintains a list of approved vendors.
5. Software must only be purchased from vendors on the approved software list.

4.2 Installation

1. Any software installed on BTL's assets, alongside other relevant information within the software asset, must be recorded within the software inventory. This must include:
    a. Title of software
    b. Developer or publisher of software
    c. Date of acquisition
    d. Date of installation
    e. Business purpose
    f. App Store(s)
    g. Version(s)
    h. End-of-support (EoS) date, if known
    i. End-of-life (EoL) date, if known
    j. Any relevant licensing information
    k. Decommission date
2. IT Operations must verify the software asset inventory quarterly, or as frequently as needed.
3. Only software and Operating system that have been approved by IT Operations and Information Security and Data Privacy may be installed.
4. Only cloud services that have been approved by IT Operations and Information Security and Data Privacy may be used within the Belize Telemedia.
5. Managed mobile devices may only obtain software from IT Operations approved sources.

4.3 Usage

In general, refer to the **Belize Telemedia's *Acceptable Use Policy*.**

4.4 Discovery

1. IT Operations must review all software installed on BTL assets on a monthly basis.
    a. All software installed on company assets must be reported to IT operations on a regular basis.
    b. Newly discovered software must be checked against the list of approved software in the software catalog managed by IT Operations.
2. Identified software not included within this inventory must be investigated as the software may be unauthorized.

a. Assets containing unauthorized software must be removed from the network unless temporary access is granted by IT Operations with Information Security and Data Privacy first being consulted.

b. The presence of unauthorized software must be thoroughly investigated.

c. All newly discovered (authorized) software must be added to the software inventory.

d. Unauthorized software must be removed from use on BTL assets or receive a documented exception.

Update and Upgrade

All updates and upgrades must be approved by IT Operations prior to installation. IT Operations may configure a device for automatic updates, or directing users to do so, constitutes implied approval.

4.5 Removal

1. Software to be decommissioned must be removed from all BTL assets.
2. Assets containing retired software must be protected with additional defensive mitigations, by consulting with the Information Security and Data Privacy team, for guidance on implementation of mitigations such as removal from the network or isolation.
3. IT Operations must make a copy of the user data as needed.
4. IT Operations must ensure that any retired software does not store data in other servers or cloud infrastructure not owned by the BTL.

5. Policy Compliance

5.1 Compliance Measurement

The Information Security & Data Privacy team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits.

5.2Exceptions

Any exception to the policy must be approved by the COO based on the recommendation of the Information Security & Data Privacy Manager. Requests for exception must be made in writing and must contain:

- The reason for the request,
- Risk to the enterprise of not following the written policy,
- Specific mitigations that will not be implemented,

- Technical and other difficulties, and
- Date of review.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, and including termination of employment.

6 Revision History

Date of Change	Responsible	Summary of Change
June 12, 2023	Irving Griffith	Development of SAM policy.
July 26, 2023	Irving Griffith	Modification to Exception policy statement

7 Approvals

______________________________ ______________________

Chief Operations Officer Chief Finance Officer

______________________________ ______________________

Chief Human Resource Officer Chief Executive Officer

____

Chief Commercial Officer

Approved Date: _______________