Asset management policy

Introduction

This Asset Management Policy is designed to protect customers' data stored on endpoints, including laptops and mobile devices. It details how Reveal accounts for endpoint information technology assets (e.g. employee computers) and outlines what should be done if assets are lost, destroyed, or otherwise damaged.

Asset Standards

The CTO must review and approve any new type of asset (e.g. a new computer model) that will be used for Reveal's operations.

Currently, approved device manufacturer(s) include [approved device manufacturers]. Devices should be configured such that there's reasonable confidence they will last 36 months.

Configuration Standards

When Reveal purchases the same hardware asset repeatedly, the team should design and implement consistent, secure configuration standards to ensure assets are configured securely and identically. The standards should be based on the team and role of the Reveal employee who will be using the asset.

All devices provided by the company should have included in the baseline configuration:

- Password management software (Dashlane)
- Hard disk encryption (e.g. FileVault) enabled
- Password-protected screensaver that activates automatically after 5 minutes or less.
- Antivirus software
- Personal firewall (e.g. OS X's application firewall) enabled

Variations to the Configuration Standard

Deviations from the standard configuration should be documented and approved by the Reveal CTO. The CTO should only approve deviations for which there's a valid business need. Deviations will be documented in the company's inventory list.

Support of Non-Standard Assets

“Non-standard assets” are those that don’t conform to Reveal’s asset and/or configuration standards. Reveal will try to provide support such that these non-standard assets do not increase the company’s risk profile. If the team cannot provide support, employees will be prohibited from using the non-standard asset. It is the employee's responsibility to ensure that non-standard assets are detected and disconnected from Reveal systems and infrastructure.

Bring Your Own Device (BYOD) Policy

Reveal provides employees with devices that conform to this policy. However, Reveal employees may, from time to time, access company information using their own devices, including mobile devices. All employee-owned devices must conform to Reveal security policies if they’re used to access Reveal data, systems, and/or IT infrastructure.

Asset Procurement Guidelines

Any request for Asset Procurement must be reviewed for compliance with Reveal's Asset Standards by the Reveal CTO. Once the request passes review, the Reveal CTO is responsible for placing orders to procure the requested assets.

Software Licensing Guidelines

Reveal's Vendor Management Policy details the policies for third-party software and services.

Technical Support and Maintenance Practices

The Reveal CTO is responsible for technical support. The CTO handles device maintenance. Support and maintenance requests should conform with all of Reveal’s security policies.

Company maintenance policies are:

- If a device breaks in the first 36 months, the employee will be given a loaner device while the original is repaired
- If an employee leaves the company, his/her device(s) will be wiped and reissued if purchased in the past 18 months; older devices will be added to the loaner pool
- Computers may be replaced when they are 36 months old

The CTO should handle device exceptions that do not meet these policies.

Configuration Management Guidelines

The CTO is responsible for installing critical firmware and software updates on the assets they use exclusively. The [party responsible for installing security updates on communal devices] is responsible for installing firmware and software updates on communal assets (e.g. desktops and/or large monitors).

Asset Inventory Practices

The Reveal CTO is tasked with maintaining a list of all company-owned assets.

Employees must immediately report lost, stolen, or damaged devices to the Reveal CTO, which will then remotely lock down the missing asset as soon as possible.

Asset Disposal Guidelines

Whenever possible, Reveal refurbishes and reissues assets. If an asset will not be reused internally, the Reveal CTO must reformat the hard drive to delete customer data and invalidate access credentials before disposing of it.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Reveal management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The CTO is responsible for ensuring this policy is followed.

Last updated: 2021-06-20