Asset Inventory Management

`2021.1`

You can't protect what you can't see. Therefore, it is imperative for MiCT to maintain an accurate and up-to-date inventory of both its physical and digital assets.

More details on data inventory and data lifecycle management is documented separately in Data Management.

Policy Statements

MiCT policy requires that:

(a) IT and/or Security must maintain an inventory of all critical company assets, both physical and logical.

(b) All assets should have identified owners and be tagged with a risk/data classification.

(c) All physical assets must be labeled with a company property tag.

Controls and Procedures

Physical Asset Inventory

MiCT IT leverages a SaaS-based IT asset management system, JupiterOne, to maintain inventory of all company owned physical computing equipment, including but not limited to:

- servers
- workstations
- laptops
- printers
- networking equipment

Each record includes details of the physical device such as manufacturer, model as well as ownership details and property tag ID.

The movement of computing hardware and electronic media is maintained as part of the records, including media re-use and ownership reassignment.

MiCT IT manager is responsible for ensuring each physical asset is applied with a MiCT property tag, and an up-to-date record is maintained in the IT asset management system.

All company-owned devices are subject to a complete data wipe if deemed necessary, such as in the case of device infection or repurpose. This data wipe will be carried out by the IT manager.

Digital Asset Inventory

MiCT Security team uses an automated system to query across our cloud-based infrastructure, including but is not limited to AWS, to obtain detailed records of all digital assets, including but not limited to:

- Virtual machines
- AWS EC2 instances
- AWS S3 repositories
- AWS Lambda functions
- Security agents
- Source code repositories
- User accounts

The records are stored in a database system maintained by MiCT security team. Records are tagged with owner/project and classification when applicable. All records are kept up to date via automation.

Paper Records

MiCT does not use paper records for any sensitive information. Use of paper for recording and storing sensitive data is against MiCT policies.