

WS07

Overview
Purpose and scope

Article 1
Ownership models

Article 2
Security and privacy

Article 3
Lifecycle and custody

Article 4
Exceptions, enforcement, and practice

IT GOVERNANCE | ENDPOINT MANAGEMENT | ASSET LIFECYCLE | MOBILE DEVICE POLICY

IT Asset Lifecycle & Device Ownership Policy

POLICY ID	CLASSIFICATION	ACCOUNTABLE	REVIEW CYCLE
POL-EUC-001	Required, audit-ready	IT operations leadership	Annual

I authored the governing policy behind the asset lifecycle program. The policy defines how the company buys, assigns, secures, supports, recovers, and retires every device, and it sets clear rules for three ownership models: corporate standard issue, corporate-owned personally enabled (COPE), and bring your own device (BYOD).

ENVIRONMENT Multistate retail enterprise with ~280 stores, distribution centers, and design studios supporting 3,000+ users.	MY ROLE Authored the asset lifecycle governance model and its BYOD and COPE provisions, aligned them with partner functions, and enforced them through the lifecycle program.
--	---

3 device ownership models with distinct rules	4 policy articles from purchase to disposal	25 day recovery clock with escalation on days 8, 15, and 22	~97% asset recovery under the policy (see WS06)
---	---	---	---

Policy Principles

- P.1** Every device has one owner of record, one assigned user, and one current location.
- P.2** Corporate data stays protected on every device, whoever owns the hardware.
- P.3** Personal privacy on employee-owned devices is defined in writing and respected.
- P.4** Assets return to the company at separation on a fixed clock with financial accountability.
- P.5** Data is destroyed to a recognized standard before any device leaves company control.

Contents

- ARTICLE 1** Ownership Models and Eligibility
- ARTICLE 2** Security Requirements and Privacy Commitments
- ARTICLE 3** Lifecycle, Custody, and Responsibilities
- ARTICLE 4** Exceptions, Enforcement, and Policy in Practice

WS07

Overview

Purpose and scope

Article 1

Ownership models

Article 2

Security and privacy

Article 3

Lifecycle and custody

Article 4

Exceptions, enforcement, and practice

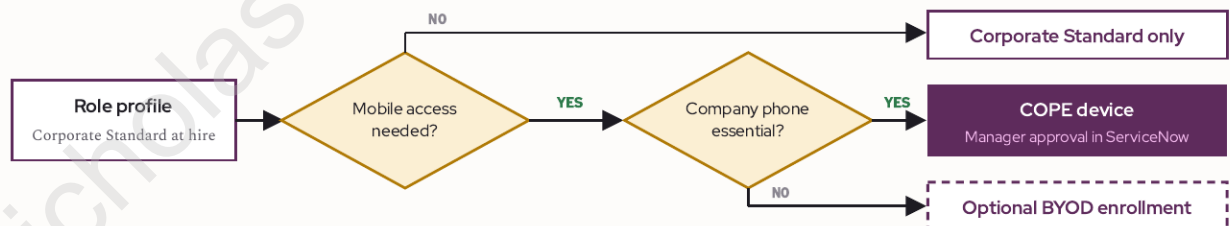
ARTICLE 1**Ownership Models and Eligibility**

Each model balances business need, cost, and control. Role requirements decide the model, and the model decides how IT manages the device.

	Corporate Standard COMPANY-OWNED, BUSINESS USE	COPE COMPANY-OWNED, PERSONAL USE ALLOWED	BYOD EMPLOYEE-OWNED
Typical use	Laptops, desktops, and shared store devices	Phones and tablets for roles that need reliable mobile access	Personal phones used for email, chat, and approved apps
Eligibility	Assigned by role at hire	Role-based, with manager approval	Voluntary, after the user accepts the BYOD terms
Management	Full device management through Intune	Full device management with a personal-use allowance	App protection for corporate apps and data only
Data separation	Corporate data only	Corporate and personal data separated by policy	Corporate data contained inside managed apps
Remote wipe	Full wipe	Full wipe, with notice where practical	Selective wipe of corporate data only
Support	Full IT support and repair	Full IT support and repair	Support for corporate apps and access
At separation	Returned on the recovery clock	Returned on the recovery clock	Corporate data and access removed on the separation date

Model Selection

Every request follows the same decision path, so the role profile decides the outcome before anyone files an exception.

**Eligibility and Approval**

- 1.1** Role profiles define the standard device set for each position, so most requests need no exception.
- 1.2** A COPE device requires a role-based need and manager approval recorded in ServiceNow.
- 1.3** BYOD enrollment requires acceptance of the BYOD terms, including the privacy commitments in Article 2.
- 1.4** Any device outside these models requires an approved exception under Article 4.

WS07

Overview

Purpose and scope

Article 1

Ownership models

Article 2

Security and privacy

Article 3

Lifecycle and custody

Article 4

Exceptions, enforcement, and practice

ARTICLE 2

Security Requirements and Privacy Commitments

Security requirements scale with ownership. The privacy commitments tell employees exactly which information on a personal device remains visible to the company.

Requirement	Corporate Standard	COPE	BYOD
Encryption	ENFORCED	ENFORCED	DEVICE-LEVEL EXPECTED
Screen lock and passcode	ENFORCED	ENFORCED	REQUIRED FOR APP ACCESS
Supported operating system	ENFORCED	ENFORCED	REQUIRED FOR APP ACCESS
Compliance check before access	ENFORCED	ENFORCED	APP-LEVEL CHECK
Copy and save limits on corporate data	DEVICE CONTROLS	DEVICE CONTROLS	ENFORCED IN MANAGED APPS
Jailbroken or rooted devices	BLOCKED	BLOCKED	BLOCKED

BYOD Privacy Commitments

VISIBLE TO THE COMPANY

- Device model and operating system version
- Managed corporate apps and their data
- Compliance status needed to grant access

PRIVATE TO THE EMPLOYEE

- Personal email, texts, photos, and files
- Browsing history and personal app activity
- Device location, except after the user reports the device lost

BYOD Enrollment Flow



Reporting and Response

- 2.1 Users report a lost or stolen device to the service desk immediately.
- 2.2 IT removes access and wipes corporate data at the level the ownership model allows.
- 2.3 Devices that fall out of compliance lose access to protected resources until remediated.
- 2.4 Security events involving a device follow the incident management framework in WS01.

WS07

Overview
Purpose and scope

Article 1
Ownership models

Article 2
Security and privacy

Article 3
Lifecycle and custody

Article 4
Exceptions, enforcement, and practice

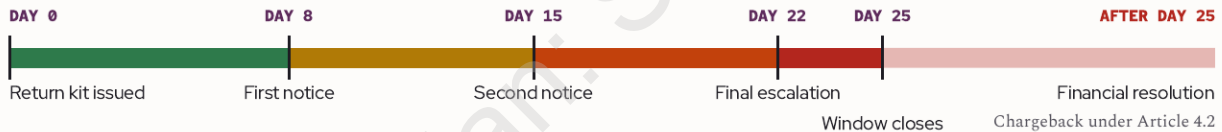
ARTICLE 3

Lifecycle, Custody, and Responsibilities

Custody never lapses. Every handoff from purchase to disposal leaves a record in the asset register and the service request system.

STAGE	POLICY REQUIREMENT
Acquire	Devices come from approved models through approved procurement, and each receipt creates an asset record.
Assign	Assignment links the device to a user, a role, and a location before shipment.
Use and support	Repairs, swaps, and loaners keep the asset record current at every step.
Refresh	Devices are replaced on a defined refresh cycle or when vendor support and security updates end.
Recover	Separation starts a 25-day recovery clock with notices, a final escalation, and financial resolution, as the timeline below shows.
Dispose	Data destruction follows NIST SP 800-88, and each destruction certificate attaches to the asset record. A legal hold pauses disposal.

Recovery Clock



Responsibility Matrix

	EMPLOYEE	MANAGER	IT OPS	HR	FINANCE	SECURITY
Request and approve a device	R	A	C	I	I	I
Procure, configure, and assign	I	I	A/R	I	C	I
Maintain custody and report loss	A/R	I	C	I	I	C
Start the clock at separation	I	C	I	A/R	I	I
Disable access at separation	I	I	A/R	C	I	C
Recover the device on the clock	R	C	A	C	I	I
Apply chargeback for non-return	I	C	C	R	A	I
Destroy data and dispose	I	I	A	I	C	R

R = Responsible, A = Accountable, C = Consulted, I = Informed. Each activity has one accountable function; A/R marks a function that is accountable and responsible.

WS07

Overview

Purpose and scope

Article 1

Ownership models

Article 2

Security and privacy

Article 3

Lifecycle and custody

Article 4

Exceptions, enforcement, and practice

ARTICLE 4

Exceptions, Enforcement, and Policy in Practice

- 4.1** Exceptions require a business reason, compensating controls, an approver, and an expiration date, and each approved exception is recorded in the governance exception register (WS03).
- 4.2** An unreturned device moves to financial resolution through the agreed chargeback process after the recovery window closes.
- 4.3** Policy violations route to the manager and HR under existing conduct procedures.
- 4.4** The policy is reviewed annually and after any significant incident, audit finding, or platform change.

The Policy in Practice

Representative scenarios show how the articles decide real requests.

A store manager wants work email on a personal phone.

BYOD with app protection. Corporate email runs inside a managed app, and personal content stays private (Articles 1 and 2).

A district leader on regular on-call duty needs a dependable phone.

COPE device. The role-based need and manager approval are recorded in ServiceNow (Article 1.2).

An employee leaves, and the COPE phone has not come back.

Recovery clock. Notices go out on days 8 and 15, the final escalation occurs on day 22, and financial resolution begins after day 25 (Articles 3 and 4.2).

A personal phone with corporate apps is reported stolen.

Selective wipe. IT removes the corporate data, and the personal data remains untouched (Article 2.2).

A legacy device must stay in service past its support date.

Exception with an expiration date. Compensating controls and a remediation date go on the register (Article 4.1).

A laptop is due for disposal while under a legal hold.

Disposal paused. The device stays in custody until Legal releases the hold (Article 3).

MANAGEMENT VALUE

The policy turns device ownership into clear, enforceable rules that employees understand and auditors can test. The policy protects corporate data on every device, respects personal privacy on employee-owned phones, and gives the recovery program its authority. The same structure serves a small business issuing its first company phones and an enterprise managing thousands of endpoints.