**Cybersecurity Templates**

**Dat Classification Policy**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **IT Assessment Management Policy** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Type:** | Company Policy | **Policy Code:** | [POL‑ITAM‑001] |
| **Owner:** | [Head of ITAM / CIO] | **Classification:** | [Internal / Confidential] |

Contents

[IT Assessment Management Policy 3](#_Toc207062905)

[1. Purpose 3](#_Toc207062906)

[2. Scope & Boundaries 3](#_Toc207062907)

[3. Definitions (excerpt) 4](#_Toc207062908)

[4. Policy Principles 4](#_Toc207062909)

[5. Governance, Roles & Responsibilities 4](#_Toc207062910)

[6. Asset Categories & Inventory Attributes 5](#_Toc207062911)

[7. Classification & Labelling 5](#_Toc207062912)

[8. Asset Lifecycle Requirements 5](#_Toc207062913)

[9. Discovery & Reconciliation 6](#_Toc207062914)

[10. BYOD & Shadow IT 6](#_Toc207062915)

[11. Risk & Compliance 7](#_Toc207062916)

[12. Audits, KPIs & Reporting 7](#_Toc207062917)

[13. Exceptions 7](#_Toc207062918)

[14. Enforcement 7](#_Toc207062919)

[Annex A — Asset Register (Minimum Fields) 7](#_Toc207062920)

[Annex B — Roles & RACI (Excerpt) 8](#_Toc207062921)

[Annex C — Lifecycle Checklists (Plan → Retire) 8](#_Toc207062922)

[Annex D — Lost/Stolen Response Steps 8](#_Toc207062923)

[Annex E — Secure Disposal (Certificate of Destruction) 8](#_Toc207062924)

[Annex F — Software & SaaS Management (Template Fields) 9](#_Toc207062925)

[Annex G — Annual Stocktake Plan (Outline) 9](#_Toc207062926)

[Annex H — Risk Criteria (Example) 9](#_Toc207062927)

[Annex I — Glossary (Excerpt) 9](#_Toc207062928)

[How to tailor this quickly (step‑by‑step) 9](#_Toc207062929)

[Attributions (inspiration, not copied) 10](#_Toc207062930)

# IT Assessment Management Policy

# 1. Purpose

This policy establishes mandatory requirements for identifying, recording, protecting, maintaining, and disposing of IT assets throughout their lifecycle, supporting business, security, privacy, and compliance objectives.

# 2. Scope & Boundaries

* **In scope:**
  + **Enterprise assets** capable of storing/processing/transmitting data: end‑user devices (desktops, laptops, tablets, smartphones), servers (on-prem/virtual/cloud), network gear (routers, switches, firewalls, WAPs), IoT/OT devices, and **software/SaaS licences** and subscriptions.
  + Information assets and configuration items are recorded in CMDB/asset tools.
* **Out of scope:** Non-computing peripherals (e.g., keyboards/monitors) unless they store data or pose risk; may still be tracked in inventory for logistics.
* **Interfaces:** Finance (capex/opex), Procurement (contracts), Security (controls/monitoring), Legal/Privacy (compliance), HR (joiner/mover/leaver).

# 3. Definitions (excerpt)

* **Asset:** Anything of value to the organisation (hardware, software/SaaS, data sets, virtual/cloud resources).
* **Asset Owner:** Business role accountable for an asset’s classification, protection, and lifecycle decisions.
* **Custodian:** IT role responsible for day-to-day operation and updates in inventory/CMDB.
* **Enterprise Asset Inventory (EAI):** The authoritative register for all in-scope assets.  
  (See Annex I for a fuller glossary.)

# 4. Policy Principles

* **Single Source of Truth:** The EAI/CMDB is authoritative for scope, status, location, ownership, and configuration.
* **Lifecycle Control:** Assets follow a standard lifecycle with documented controls at each stage.
* **Data‑Driven Risk:** Inventory attributes must enable risk assessment (classification, criticality, exposure).
* **Least Privilege & Accountability:** Clear owner/custodian assignment for every asset.
* **Timeliness:** Inventory uis updated within five business days of any change (acquisition, relocation, reassignment, or retirement.
* **Verification:** Stocktakes and control tests occur at least **annually**; high-risk sites/devices **bi‑annually**.
* **Unauthorized Assets:** Detected weekly; removed/quarantined per Incident/Change procedures.

# 5. Governance, Roles & Responsibilities

* **Executive Sponsor:** Ensures resources; approves policy and exceptions.
* **CIO / Head of ITAM (Policy Owner):** Maintains this policy and the EAI process; reports KPIs.
* **Asset Owners (Business):** Classify, approve access, define retention/backup; accept residual risk.
* **Custodians (IT Ops/Cloud/Endpoint/Network):** Tag, onboard/offboard assets; maintain attributes; enforce controls.
* **Software Asset Manager:** Manages licences/subscriptions, compliance, optimisation, and EULAs.
* **Security (CISO/SOC):** Monitors unauthorized assets, integrates discovery tools, logs, and DLP; investigates incidents.
* **Procurement & Legal:** Ensure contracts include security, data location, audit rights, disposal, and exit terms.
* **All Users:** Care for assigned assets, follow AUP, and promptly report loss/theft/damage.

# 6. Asset Categories & Inventory Attributes

* **Categories:** End‑user devices; servers/virtual machines; network & security appliances; IoT/OT; storage & media; software/SaaS; cloud resources (IaaS/PaaS/SaaS).
* **Minimum attributes** (per record): Unique ID/asset tag; make/model; serial/UUID; owner & custodian; location (physical or logical); status (in‑service, spare, repair, retired); support/warranty; network IDs (hostname, IP, MAC, cloud resource ID); **classification**; **criticality**; **backup/DR**; **encryption**; **supporting contracts/licences**.
* **Software/SaaS:** Vendor, product/version, licence model & count, subscription term, billing owner, data residency, DPA/SLA, auth method (SSO/MFA), export/exit plan.

# 7. Classification & Labelling

* Classify assets based on the sensitivity of data handled (e.g., Public / Internal / Confidential / Restricted).
* Apply labels and handling rules (storage, transmission, disposal) appropriate to classification.
* Tag devices physically where practical; logical/tagging for cloud and virtual assets.

# 8. Asset Lifecycle Requirements

**All assets must follow these stages and controls:**

* **Plan**
  + Validate need, budget, and category; nominate Owner and Custodian; confirm inventory tool and fields.
  + Define required controls (encryption, EDR, MDM/Intune/JAMF, logging, backup).
* **Acquire**
  + Purchase via approved channels; contracts must include security schedules, support, data location, and exit/disposal.
  + Pre-register assets and allocate tags/unique IDs.
* **Receive & Prepare**
  + Record full attributes; baseline image/config; apply patches; enable encryption and EDR/MDM; bind to identity.
  + For SaaS: configure SSO/MFA, roles, logging, retention, and export APIs.
* **Deploy**
  + Assign to user or service; capture handover/acceptance; update location and support group.
  + Document backup/DR (if applicable) and monitoring.
* **Operate & Maintain**
  + Keep attributes current (moves/changes/repairs); apply patches; verify backups; review access quarterly.
  + Detect **unauthorized assets weekly** (network scans/agent/MDM/CMDB reconciliation) and remove/quarantine.
  + Conduct **annual physical audits** and reconcile to inventory; investigate discrepancies.
* **Lost/Stolen (Uncontrolled Disposal)**
  + User must report immediately; SOC revokes access, triggers remote lock/wipe where feasible; create incident record; mark inventory as **lost/stolen**; file police report when required.
* **Retire & Dispose (Controlled Disposal)**
  + Backup/transfer required data; perform secure sanitization (NIST-aligned wipe or crypto‑erase); remove from MDM/identity; revoke certificates; update inventory to **retired**; capture **Certificate of Destruction**.
  + For SaaS: terminate accounts/tenants, export data, confirm deletion by vendor, and close licenses/subscriptions.

# 9. Discovery & Reconciliation

* Use automated discovery (network scans, agents, cloud APIs, MDM, CSPM) to populate and reconcile the EAI.
* Reconcile weekly: **new**, **changed**, or **unauthorized** assets; raise tickets for investigation/cleanup.

# 10. BYOD & Shadow IT

* BYOD is prohibited unless explicitly approved with MDM enrollment and conditional access.
* Unapproved SaaS/IT tools must be onboarded or blocked; data exfiltration controls must monitor exports/sharing.

# 11. Risk & Compliance

* Apply a risk method (likelihood/impact matrix) to assets and environments; record residual risk/acceptance.
* Align with standards/regulatory obligations (e.g., ISO 27001/27002, contracts, privacy laws) and with internal SoA/controls.
* Evidence: retain inventories, audit trails, sanitization certificates, vendor attestations, and stocktake reports as per the retention schedule.

# 12. Audits, KPIs & Reporting

* **KPIs:** Inventory coverage ≥ 99% of connected assets; unauthorized asset closure ≤ 7 days; stocktake variance ≤ 1%; encryption coverage ≥ 99%; licence compliance variance = 0.
* Report quarterly to the Executive Sponsor with trends and corrective actions.

# 13. Exceptions

Time-bound, risk-assessed, compensating controls specified; approvals by Policy Owner and Executive Sponsor; review every 6 months.

# 14. Enforcement

Breaches may result in disciplinary action, up to and including termination, and may also trigger contractual/legal remedies.

**Sign‑Off**

**Chief Executive Officer**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date**: \_\_\_\_\_\_\_\_\_  
**CIO / Head of ITAM**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date**: \_\_\_\_\_\_\_\_\_

# Annex A — Asset Register (Minimum Fields)

|  |  |
| --- | --- |
| **Field** | **Example** |
| Asset ID / Tag | ITA‑000123 |
| Category | Laptop / Server / SaaS |
| Make/Model / Serial | Dell 7420 / 1X‑SN‑123 |
| Owner / Custodian | Sales Director / EUC Ops |
| Location | London‑HQ / AWS‑eu‑west‑1 |
| Status | In‑service / Spare / Retired |
| Classification / Criticality | Confidential / High |
| Network IDs | Hostname, IP, MAC |
| Encryption / EDR / MDM | Yes / Yes / JAMF |
| Backup/DR | OneDrive / Snapshots |
| Warranty / Support | Exp. 2027‑01‑31 |
| Licence/Contract | M365 E5 / PO‑12345 |
| Notes/ Evidence | CoD # 2025-009 |

# Annex B — Roles & RACI (Excerpt)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Activity** | **Exec** | **CIO/ITAM** | **Asset Owner** | **Custodian (Ops)** | **Security** | **Proc/Legal** |
| Approve Policy | A | R | C | I | C | C |
| Maintain Inventory | I | R | C | R | C | I |
| Classify Asset | I | C | R | C | C | I |
| Handle Unauthorized Assets | I | C | I | R | R | I |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| (A=Approver, R=Responsible, C=Consulted, I=Informed) |  |  |  |  |  |  |

# Annex C — Lifecycle Checklists (Plan → Retire)

* **Plan:** Need, Owner/Custodian, budget, control set, data flow.
* **Acquire:** Contract clauses (security/exit), asset tag, pre‑registration.
* **Prepare:** Baseline image/config, encryption, EDR/MDM, SSO/MFA.
* **Deploy:** Handover, access granted, location, backup set.
* **Operate:** Patch cadence, access review, reconcile, verify backups.
* **Retire:** Data transfer, wipe/CoD, revoke access, update EAI.

# Annex D — Lost/Stolen Response Steps

User reports immediately → ticket; 2) Lock/wipe; 3) Revoke creds/keys; 4) Update EAI; 5) Incident record & (if needed) police report; 6) Lessons learned.

# Annex E — Secure Disposal (Certificate of Destruction)

Asset ID/Serial, Method (wipe/crypto‑erase/shred), Vendor & Witness, Date/Time, Lot #, Signatures; attach to EAI record.

# Annex F — Software & SaaS Management (Template Fields)

|  |  |
| --- | --- |
| **Field** | **Example** |
| Vendor/Product | Atlassian Confluence Cloud |
| Licence Model/Count | Subscription / 250 |
| Data Residency | EU |
| Auth | SSO + MFA |
| Logs/Retention | 365 days |
| DPA/SLA | Signed 2025‑02‑01 |
| Exit Plan | Export API + 30‑day hold |

# Annex G — Annual Stocktake Plan (Outline)

Scope & sample strategy; bar‑code scan or agent + physical reconcile; variance thresholds; remediation workflow; sign‑off.

# Annex H — Risk Criteria (Example)

Likelihood: Rare → Almost Certain; Impact: Low → Severe; Appetite: No **High** residual risk without CIO approval; triggers for mitigation/escalation.

# Annex I — Glossary (Excerpt)

* **EAI/CMDB, CoD, BYOD, CSPM, EDR, MDM, SSO, MFA, SaaS, IaaS, PaaS.**

# How to tailor this quickly (step‑by‑step)

1. **Fill document control:** owner, approver, effective/review dates.
2. **Confirm scope:** which sites, cloud regions, categories, and which tools hold the EAI.
3. **Adopt categories & fields (Annex A):** add any local fields (cost centre, PO, rack/row/U).
4. **Nominate Owners/Custodians:** publish the RACI (Annex B).
5. **Plug in lifecycle controls:** list your baseline image, encryption standard, EDR/MDM, and wipe method.
6. **Wire up discovery:** define sources (MDM, agent, cloud API) and set the weekly reconcile cadence.
7. **Set KPIs:** choose 3–5 from §12 and add report owners/dates.
8. **Add SaaS:** complete Annex F for your top apps (SSO/MFA, export paths, data residency).
9. **Finalize disposal:** select the wipe standard and add your disposal vendor details to Annex E.
10. **Publish & train:** short guide for requestors, owners, custodians; include lost/stolen playbook (Annex D).

# Attributions (inspiration, not copied)

* Lifecycle & attribute depth, risk-based exclusions, and role clarity reflect best practices from public‑sector AM guidelines and enterprise policies.
* CIS Control 1 alignment and handling of unauthorized assets influenced the discovery/reconciliation cadence.
* Annual audits, classification/tagging, and AUP linkage were inspired by enterprise risk/asset policy models.