IT Asset Management Policy: Computers, Tablets, and Software

1.0 Policy Objective & Scope

The objective of this policy is to establish clear administrative guidelines for the procurement, deployment, tracking, maintenance, and disposal of all company-owned computers, tablets, and software licenses. This policy ensures that IT assets are used efficiently, data is protected in accordance with PIPEDA, and the organization maintains accurate records for audit and compliance purposes.

This policy applies to all employees, contractors, and temporary staff who are issued company-owned computers, tablets, or who use company-licensed software. It also applies to the IT Department, Department Heads, and the Finance team involved in asset procurement and lifecycle management.

2.0 Roles & Responsibilities

- **IT Administrator:** Responsible for maintaining the central asset inventory, assigning assets to users, performing regular audits, and managing software license renewals and compliance.
- **Department Head:** Responsible for approving asset requests for their team members and ensuring that assets are returned upon employee departure or transfer.
- **Finance Manager:** Responsible for approving capital expenditures for asset purchases and ensuring that asset depreciation is recorded correctly.
- End User (Employee/Contractor): Responsible for the physical care and security of assigned assets, reporting loss or damage immediately, and returning assets upon termination or reassignment.
- **HR Manager:** Responsible for notifying IT of employee status changes (hires, transfers, terminations) to trigger asset assignment or retrieval workflows.

3.0 Core Rules & Guidelines

- All company-owned computers and tablets must be inventoried in the SwitchDesk asset management module within 24 hours of receipt.
- Each asset must be assigned a unique asset tag and recorded with make, model, serial number, purchase date, warranty expiry, and assigned user.
- Software licenses must be tracked by license key, version, number of seats, renewal date, and assigned users. Unused licenses must be decommissioned or reassigned within 30 days.
- No employee may install unapproved software on company devices. All software installations must be requested through the IT helpdesk and approved by the IT Administrator.
- Assets must be physically secured when not in use. Laptops and tablets must be locked in a drawer or secured with a cable lock in open workspaces.

- Data on all devices must be encrypted using company-approved full-disk encryption (e.g., BitLocker, FileVault). Any device that stores customer or employee personal information must comply with PIPEDA retention and disposal requirements.

- Asset disposal (sale, donation, or recycling) must follow a secure data wiping process certified by the IT Administrator. A certificate of data destruction must be filed in the asset record.

4.0 Step-by-Step Procedure / Workflow

1. Initiate an asset request by submitting the digital Asset Request Form via the SwitchDesk portal. Include justification, required specifications, and budget code.

2. The Department Head reviews the request and approves or denies it within 48 hours. If approved, the request is forwarded to Finance for budget verification.

3. Finance Manager confirms budget availability and approves the purchase. The IT Administrator then procures the asset through an approved vendor.

4. Upon receipt, the IT Administrator unboxes the asset, applies a tamper-proof asset tag with a unique barcode, and records the asset details in SwitchDesk (make, model, serial number, purchase date, warranty expiry).

5. The IT Administrator configures the device with the standard corporate image, installs required security software (antivirus, encryption, remote management), and applies all critical updates.

6. The IT Administrator assigns the asset to the requesting employee in SwitchDesk, records the assignment date, and sends the employee a notification with the asset tag number and care instructions.

7. The employee acknowledges receipt of the asset by signing the digital Asset Acceptance Form in SwitchDesk, confirming they understand their responsibility for the device.

8. For software licenses, the IT Administrator installs the licensed software on the assigned device and records the license key, version, and seat assignment in the SwitchDesk software license register.

9. On a quarterly basis, the IT Administrator runs a physical inventory audit using the SwitchDesk mobile app to scan asset tags and verify the location and condition of each asset.

10. When an employee leaves the company or transfers departments, HR notifies IT via an automated SwitchDesk workflow. The IT Administrator schedules a return appointment and prepares a data wipe checklist.

11. Upon return, the IT Administrator inspects the asset for damage, performs a secure data wipe using certified software, and updates the asset status in SwitchDesk to 'Available' or 'Disposal Pending'.

12. For disposal, the IT Administrator completes a Data Destruction Certificate, files it in the asset record, and coordinates with the approved e-waste recycler. The asset record is then closed in SwitchDesk.

5.0 Documentation & Compliance

1. All asset records, including purchase receipts, warranty documents, assignment forms, and disposal certificates, must be stored digitally in SwitchDesk for a minimum of seven years after asset disposal.

2. The IT Administrator must generate a monthly asset exception report (missing assets, unassigned devices, expired warranties) and review it with the Department Heads.

3. An annual internal audit of the IT asset inventory must be conducted by the Finance team, comparing physical assets against SwitchDesk records. Discrepancies must be investigated and resolved within 30 days.

4. Software license compliance audits must be performed semi-annually to ensure the organization is not over- or under-licensed. Any non-compliance must be corrected within 15 business days.

5. All data destruction activities must be logged with the method used (e.g., DoD 5220.22-M), the serial number of the device, and the name of the technician. Logs are retained in SwitchDesk for audit purposes.

6. In the event of a security breach involving a lost or stolen device, the IT Administrator must immediately initiate the Incident Response Protocol and notify the Privacy Officer within 24 hours as required by PIPEDA.