Signed: Position: Date:

_____ Chairman

_____ Secretary

Contents

1. Overview

Information systems technology is used to conduct the day-to-day operations of Credit Union ("CU"). Physically tangible technology such as computers, laptops, servers and backup tapes are highly visible. However, software systems or applications such as word processing, office productivity tools, anti-virus software, accounting packages and savings & loans systems represent intangible technology that may be less visible. Both tangible and intangible technologies are classified as Information Systems Assets (IS Assets) within the credit union. The principal objective of this policy is maintaining the ongoing adequacy of Information Systems assets in the Credit Union.

The decision to classify a technology component as an IS Asset is based on the value that is gained by doing so. A typical keyboard, for example, is considered to be a generic technology component that is not critical to the operations of the credit union. A faulty keyboard can simply be replaced with another should the need arise, with little or no associated risk. The credit union savings & loans computer server, on the other hand, holds specific software applications and operational data essential for business operations. Loss of a server or another business-critical computer may have significant impact on the credit union. Consequently, servers, computers and software applications are classified as IS Assets in order to recognise their importance in credit union operations, whereas a generic keyboard or mouse are not.

Asset management is the process of receiving, tagging, documenting, managing the usable lifecycle and eventually disposing of equipment. It is critically important to maintain up to date inventory and asset controls to ensure computer equipment locations and status are known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal pursuit, and insurance activities.

"ICT" for the purposes of this document refers to Information and Communications Technology.

2. Purpose, scope and users

The purpose of this policy is to ensure that Credit Union's (CU) IT Assets are managed through an established process. It is also an objective to maintain an accurate physical record of CU's physical computer assets. This document establishes procedures to ensure compliance with regulatory expectations, IT governance recommended practices and to ensure accurate reporting of physical assets and commercially licensed software.

This policy will apply to all computer equipment, software and related assets purchased by CU.

This policy applies to all Credit Union full-time, part-time and contracted employees, vendors and suppliers involved in activities that use or manage technology solutions within CU.

Users of this document are employees, directors and volunteers within CU.

3. Roles and Responsibilities

All staff and volunteers associated with CU share the responsibility for implementing this policy.

3.1 Board of Directors

The Board of Directors of CU have overall responsibility and accountability for all the assets owned and used by CU. They are the approval authority for all I.S. Assets having a High Criticality or where the cost exceeds €1,500.00.

3.2 Audit, Risk and Compliance Committee

The Audit, Risk and Compliance Committee are responsible for making recommendations to the Board of Directors in relation to how I.S. Assets are treated.

3.3 Credit Union CEO

The Credit Union CEO is responsible and accountable to the Board of Directors for the day to day management of all IS Assets owned or used by CU. Under this policy, they have the following key responsibilities.

- They are the approval authority for all IS Assets having a medium or low criticality or where the value does not exceed €1,500.00
- They are responsible for ensuring that all IS Assets are managed in accordance with this policy.
- They are responsible for ensuring that quarterly IS Asset auditing is conducted for all assets having a High Criticality and annual auditing for other assets.
- They are responsible for presenting an annual Information Systems Asset Report to the Board.
- They are responsible for informing the Board of any inconsistencies in relation to assets having a High Criticality.

3.4 IT Oversight Officer

The IT Oversight Officer as designated under the Information Systems Security Policy will have the following responsibilities under this policy:

- They will act as the internal point of contact for IS Asset Management issues.
- They will ensure that the Asset Register is kept up to date for all new and existing IS Assets.
- They will control access to the Asset Register
- They will assign new IS Asset numbers
- They will ensure an asset tag is applied to all hardware based IS Assets prior to being used.
- They will fulfil other IS operational requirements as directed by the CEO.

The IT Oversight Officer will report directly to the Credit Union CEO in relation to IS Asset issues at CU.

3.5 Credit Union Staff and Committee Members

All CU staff and committee members must be made aware of this policy. They need to comply with all the terms of this policy and respect the IS Assets that they use. They also need to comply with instructions issued by the IT Oversight Officer, Credit Union CEO or Board of Directors in relation to IS Assets.

4 Lifecycle Management

With reference to this policy lifecycle management is the process of managing the entire lifecycle of an IT asset from procurement, through installation and commissioning to service and disposal.

Lifecycle management integrates people, data, processes and business systems and provides an information backbone for CU and its extended organisation.

5 Policy Statements

5.1 Asset Value

- Assets which cost less than €200 (two hundred euro) will not be tracked, including computer components such as smaller peripheral devices, video cards, or keyboards, or mice.
- Assets, which store data regardless of cost, must be tracked either as part of a computing device, as a part of network attached storage or as a standalone data repository.
- Such assets include:
    - Network Attached Storage (NAS), Storage Area Network (SAN), USB keys or other computer data storage
    - Temporary storage drives
    - Tape or optical media with data stored on them including system backup data

5.2 Asset Types

- The following minimal asset classes are subject to tracking, lifecycle management and asset tagging:
- Hardware
    - Desktop workstations
    - Laptop mobile computers
    - Tablet devices
    - Printers, copiers, cash counting devices, and multifunction print devices
    - Handheld devices
    - Organisation issued mobile telephones
    - Scanners
    - Servers
    - Network appliances (e.g. firewalls, routers, switches, Uninterruptible Power Supplies (UPS), endpoint network hardware, and storage)
    - PBX and Voice over Internet Protocol (VOIP) Telephony Systems and Components
    - CCTV systems
    - Internet Protocol (IP) Enabled Video and Security Devices
    - Storage devices

- Software:
    - Core Line of Business Application [Progress]
    - Legacy Systems
    - Server Operating Systems
    - Virtualisation Software
    - Back Up and Replication software
    - Accounts software
    - Payroll software
    - Email platform
    - Office Productivity tool [MS Office]
    - Risk and Compliance Software
    - Endpoint Security software
    - Managed Services platform [IT Support]

5.3 Asset Identification

- To manage IS Assets, each one will be assigned a unique identifier.
- Hardware based IS Assets will be identified with the prefix HW, followed by a unique four-digit number that increases in single increments each time a hardware based IS Asset number is assigned.
- The following illustrates the hardware based IS Asset numbering convention:

  HW-0001

  HW – Designates it is a physical piece of IT equipment as per IT Asset Register
  0001 – Denotes the number of that piece for recording purposes in IT Asset Register

- Hardware based IS Assets will be marked with a non-removable asset tag for identification purposes.
- The asset tag will be attached in a highly visible location on the IS Asset and clearly displays the unique IS Asset number.
- The following illustrates the software based IS Asset identifying convention, labels are not applied due to impracticality. Software Assets are named based on a logical description:
  - Progress Banking
  - Windows Server 2022
  - Windows Server 2019

5.4 IT Asset Register

- An IT asset-tracking register will be maintained to track assets.
- This will be held in a secure location within the credit union.
- An additional copy will be kept in the disaster recovery location off premises
- Data backups will include the asset register.
- Critical attributes of the managed asset will be documented and updated over the lifetime of the asset.
- At a minimum these will be:
  - Asset ID: Unique identifier
  - Current Status: Live / Withdrawn from service
  - Asset Type: Hardware (HW) or Software (SW)
  - Asset Criticality: High/Medium/Low
  - Type of Asset: Desktop computer, server, router, software system, etc.
  - IP Address IP Address of the asset on the network if applicable
  - Serial Number/Service Tag: Serial number or the manufacturer service tag
  - Equipment: Details of what the asset is
  - Asset/Device as PC Name: Windows/Linux name of the PC
  - Asset/Device as per Managed Service Report: Given name of the asset under management by Managed Service Solution if applicable
  - O/S: Operating System if applicable
  - Location: Location of the asset with the branch
    - Branch: Name of branch the asset resides in
    - Person Responsible: The person who has responsibility for the asset if applicable
    - Supplier: Name of supplier who provided the asset
    - Purchase date: Date asset was purchased (where available)
    - Replacement date: Date asset is anticipated to be replaced or will reach end of life

- Notes: Anything else relevant to the asset

- A maintenance / problem log should be created for all IS Assets that have a High or Medium Criticality. This will include the following details;
  - IS Asset number
  - Date reported
  - Name of the person who reported the problem
  - Nature of the problem
  - Date resolved
  - Detailed description of how the problem was resolved
  - Name of the person or company who resolved the problem

5.5 Hardware Replacement

Hardware (i.e. desktop, monitors etc.) is on a strict replacement cycle.

- Application Server: 5 years
- Windows Server: 5 years
- Desktop: 5 years
- Monitor: 5 years
- Printer: 5 years

Unless otherwise noted Life of hardware constitutes: Until hardware no longer performs to necessary industry standards or whether associated operating systems are obsolete and it more commercially sensible to replace both the operating system AND the associated hardware.

Hardware may be upgraded before the replacement date due via:

- CEO Request
- Hardware Malfunction

Specifically in relation to assets identified as being of High Criticality the Credit Union ensures that it has;

- An adequate back-up and restore to new machine process; and/or
- A duplicate asset; and/or
- An agreed replacement with an external supplier.

5.6 Acquisition and Commissioning

- All new assets covered under the scope above must be sourced via an CU approved supplier [see register of providers and CU Outsourcing Policy].
- CU policy and procurement policies must be followed.
- ICT acquisitions requiring the support of existing service providers must be agreed with the impacted service provider prior to purchase.

- All purchase of new systems hardware / software or new components must be made in accordance with relevant Information Security and other policies, as well as technical standards.
- Prior to deployment the Management Team will assign an ID to the asset and enter its information in the Asset Register.
- All assets maintained in the IT asset register must have an assigned owner.
- All equipment sourced from a supplier other than an CU approved supplier must be fully evaluated, assessed for fitness of purpose, hardened to industry security standards before being transferred to the live environment.
- The detail of all software based IS Assets must be entered into the asset register before the software is installed.
- Any information / instructions received at the time of purchasing the software should be filed away in a "software library" for safekeeping. The relevant asset number should be attached to each file. A copy of relevant contracts, support or maintenance agreements in relation to the software should also be included in the file.
- Where the version of existing software is upgraded or changed, a new entry must be created in the asset Register to record the details about the new version. This should include a reference to the IS Asset number of the older version. The older version of the software should be updated as being "withdrawn from service" and the record should be updated to include a reference to the IS number of the new version.
- Hardening standards must be followed for all new hardware and software prior to production implementation. This includes:
    - Keeping security patches updated and are subject to ongoing management
    - Ensuring firmware is update and subject to ongoing management
    - Keeping security certificates updated
    - Ensuring the device is subject to firewall rules
    - Ensuring email is subject to filtering
    - Ensuring web-filtering is applied
    - Reviewing ports and allowing access to only those required
    - Disabling file sharing capability
    - Installing endpoint security software/anti-virus
    - Change default credentials
    - Creating strong passwords as per CU's password policy
    - Ensuring the device is subject to CU's backup policy
    - Using 256 bit encryption where data will resides on the device
    - Disabling weak encryption

5.7 Business Continuity & Disaster Recovery

- In a business continuity or disaster recovery event the relevant sections and control items of this policy must be adhered to. These are:
    - Asset Disposal and Repurposing
    - Physical Management of Equipment
    - Use of Personal Computing / Bring Your Own Device
    - Audit Controls and Physical Reconciliation

5.8 Asset Disposal and Repurposing

- All data and configuration setting (including User IDs and passwords) must be permanently deleted prior to disposal.
- Computer Equipment must be disposed of in a safe and environmentally friendly manner.
- A certificate of safe destruction from a certified service provider must be obtained for each asset disposed of.
- Computer equipment cannot be disposed of via skips, dumps, landfill etc.
- Assets must not be gifted or repurposed without the permission of the Credit Union CEO
- Where assets are repurposed, they must be certified (by the managing vendor) to be completely sanitised and purged of data, credentials, system configuration. This includes cache memory and all trace data.
- All IS Assets should be disposed of in accordance with the Information System Security Policy. Assets that have a High Criticality can only be disposed of upon authorisation by the Credit Union CEO.

5.9 Physical Management of Equipment

- Employees, volunteers and directors must not remove IT assets supplied by the Credit Union from CU premises, except under the following conditions:
    - IT assets assigned to employees or directors which may include laptop or tablet computers and Personal Digital Assistant (PDA) or Smartphone devices, may be removed from for the following reasons only:
        - Teleworking.
        - Work that is outside of the office that is a part of an assigned position.
- Exceptions to this policy must be requested in writing and approved by the Credit Union CEO. Documentation of exceptions must include the business or technical justification and the duration of the exception.
- Employees and directors are responsible for safeguarding any IT assets they remove from the CU's offices must physically secure the assets when they are not under their direct physical control.
- Files containing confidential or sensitive data may not be stored on personal computing devices and storage devices.
- Users must immediately report the loss or theft of any assigned IT assets to the Credit Union CEO

5.10 Managing the Ownership of IT Assets

- Mobile devices such as laptops, tablets, removable storage devices etc. that are on a short-term loan to staff or committee members should be recorded in the loan asset register as being on loan to the individual.
- When IS Assets are issued on loan, a return date should be entered at the time of giving out the asset.
- Each IS Asset that is currently on loan, should be checked in the quarterly review to make sure the requirement hasn't expired and that the device is still required.
- When the IS Asset is returned, it should be checked to make sure it wasn't damaged and that it's still in working order. The loan asset register should include the full history of each loan for each IS Asset. This will include:
    - IS Asset number
    - Name of the person who requested the loan
    - Date Issued
    - Date Returned
    - Purpose of the loan
    - Name of the person who checked the asset upon return
    - Any issues with the asset upon return
- Mobile devices should be stored in accordance with the Information Systems Security Policy when not in use or out on loan. Removable media should be erased upon return after a loan.

5.11 Use of Personal Computing / Bring Your Own Device

- Staff and directors are not permitted to bring their own IT assets into work locations with the purpose of connecting to CU's private network and data.
- Connection of personal IT assets to networks provided by CU for guest or public access is not allowed.
- Exceptions to this policy must be documented in writing and approved by the Management Team. Documentation of exceptions must include the business or technical justification and the duration of the exception.
- CU owned confidential or sensitive data must only be stored on a personal device that is encrypted with a minimum of 256bit encryption.

5.12 Audit Controls and Physical Reconciliation

- A physical audit of assets under management must be conducted at least annually for all assets. The IT Asset Audit must at a minimum:
    - Verify the existence of each asset
    - Verify that attributes about each recorded asset in the Asset Register are accurate
    - Identify unauthorised assets (software and hardware)
    - Confirm that end of life assets have been noted in the Asset Register
- To ensure compliance with software licence requirements, the Asset Register must be reviewed at least annually to ensure required software licenses are active, and will remain valid throughout the next review period. This will form part of Credit Union CEO role.
- Review the maintenance log for patterns or problem assets that may need special attention or be recommended for replacement.

6. Reporting

On an annual basis the Board of Directors should receive an Information Systems Assets Report, and this report must include the following information at a minimum:

- List of assets deemed to be of High Criticality
- Evidence and results of the annual IT Asset Audit
- Evidence of software license compliance
- Recommended asset replacements during the ensuing 12 months
- Recommendation and justification for extending use of assets beyond their originally anticipated expiry date

7. Non-Compliance

Any failure to observe the policies contained in this document will be subject to the Credit Unions disciplinary procedures.

8. Distribution

- This policy will be distributed to all employees, directors and volunteers within the Credit Union.
- Revisions and updates will be distributed to all of the stakeholders named above.
- This policy must be located on the CU network “public folder”, in hard and softcopy at CU’s Disaster Recovery site, and within CU’s Disaster Recovery battle box.
- This policy and acknowledgement of this policy will form part of all employees, directors and volunteer’s induction program.

9. Significant Deviations

Any significant deviation from this policy is to be communicated to the Credit Union CEO in the first instance and reported to the Board as part of the next monthly CEO’s report. The CEO’s report of the breach will include both the reason(s) for the deviation(s) and any proposed action(s) to address same.

10. Policy review and updating

The Information Systems Asset Management policy will be formally reviewed by the CEO on an annual basis and proposals brought to the Board for its consideration. In between scheduled annual reviews the Risk Management Officer and Compliance Officer may make proposals to the CEO for consideration. The CEO may authorise routine changes or procedural updates to facilitate smooth and compliant operations and may bring the matter to the board for consideration.

11. Supporting Documents

Documents to be read in conjunction with this policy are:

- IT Asset Register
- Strategic Plan
- Change Management Policy
- IT Budget
- Information Security Policy
- Business Continuity Policy