Credit Union		IT Credit Union IT Security Policy			
Policy No: CU-P15	**Version:** 2.0	**Original Issue Date:** June 2023		Page 1 of 19	
Ver.	**Amendment Description / Review information**	**Created / Revised / Modified By**	**Date**	**Approved by Board**	**Review Date**

Signed: Position: Date:

_____ Chairman

_____ Secretary

Table of Contents

1.0 Introduction

1.1 Purpose

This policy forms part of a complete set of Information Technology Security Policies for Credit Union. Their primary purpose is to protect the organisation's data and information systems and the investments made by the organisation in technologies that support the business's operations on a day to day basis.

1.2 Scope

This document is intended to set out the policies as they relate to the general control of Information Technology services and the underlying technical infrastructure in Credit Union.

1.3 Audience and Responsibilities

This document forms part of the organisation's Information Technology services policies, standards, procedures and guidelines. The content of this document must be made available to and known by all employees both permanent and temporary.

The content of this document must also be made known and made available to suppliers, contractors and sub-contractors who supply services in support of any computer device or computing resource, where their access level may result in them being able to view the organisation's data.

All staff volunteers', directors, 3rd vendors and contractors are responsible for the enforcement of these policies. All permanent and temporary employees are responsible for monitoring and reporting breaches of these policies. Any person allocated a computer device or with access to any computing resource is responsible for observing the policies set out in this document.

1.4 Updating and Distribution

The document must be reviewed at a minimum annually.

Proposed revisions to this document must be agreed by the following:

- *The CEO*
- *The RISK Officer/Compliance Officer*
- *The Board of Directors*

A revision history must be maintained on the front page.

Revised and updated version of this document must be distributed to the following:

- *All permanent and temporary employees, directors and volunteers*
- *Suppliers, contractors and sub-contractors who are responsible for maintaining and managing equipment, services and applications on the Credit Union network*

1.5 Non-Compliance

Any failure to observe the policies contained in this document will be subject to the organisations disciplinary procedures, this may result in the ceasing of any third-party agreements.

The organisation reserves the right to monitor the use of any Information Technology computer device or computing resource to ensure compliance with this and all Information Security policies.

1.6 Definitions

A **computer device** includes, but is not limited to, any mainframe, server, personal computer, laptop, tablet devices, terminal devices, mobile phones including smartphones and any device running an embedded or full operating system.

A **computing resource** includes any system or components that forms part of the overall Information technology infrastructure of the organisation. Computing resources include, but are not limited to, removable media, any telecommunication resource, any network environment, fax machines, printing and copy machines, scanners, multifunction machines, applications, data and information, data and information storage devices, electronic transmission systems, security systems, cabling systems, recording machines both voice and video.

An **Operating System** is software that manages a computer device and installed software.

Data is raw unstructured information.

Information is structured giving meaning to raw data that results in advancing knowledge.

User is an officer, member of staff, volunteer, service provider or 3rd party contactor who has access to CU's IT assets, services, infrastructure, applications or network.

2.0 Policy Statements

2.1 Account Management

- Requests for new accounts must be submitted to the CEO
- Generic accounts other than special system accounts must not be used
- User accounts must not be shared
- Default admin accounts must be disabled on all devices, infrastructure, operating systems and databases
- An initial user password must be temporary and set to change immediately on first logon
- A user password must never be set permanently by the IT vendor
- Password properties must be set in accordance with the password policy
- Access rights must be based on least privilege access that is users must only be given access to systems and information based on what they need to perform their duties
- Remote access is not permitted for internal users
- Passwords must be changed on the day of leaving for users that depart the organisation
- Temporary employees must have their account set to expire on the last day of their contract

2.2 Admin and Special Access

- All admin or special access accounts must be made known to the Management Team along with the reason for the existence of the account
- All users of these accounts must have signed a confidentiality and non-disclosure agreement
- All users of these accounts must observe the information technology policies of the organisation
- All users of these accounts must understand their obligations under Data Protection legislation and GDPR
- Admin or special access accounts, where practical, must only have the level of access they need to perform a task or tasks
- The password for these accounts must be strictly controlled
- The use of these accounts must be logged including log on and log off times
- Network access and application access reports are available to the Credit Union Management to support oversight and access controls. These are to be reviewed monthly.
- Change Requests must be completed for changes that may impact the integrity or security of systems and data.
- Remote and vendor-initiated network access must only be completed using secure encrypted channels.

2.3 Security Incident Management

- All security concerns and breaches must be reported to the Management Team immediately
- The Compliance Officer will record the event and report this to the appropriate authority that may include but is not limited to:
    - The Board of Directors
    - The Central Bank of Ireland
    - The Gardaí where a breach of any law is committed
    - The Data Protection Commissioner's office for data breaches
    - The relevant IT vendor responsible for managing and supporting the IT system affected

2.4 Password Policy

- All users of credit union information systems are assigned a unique user account administered by a central server.
- User accounts are composed of three elements: a user name, a password, and a configuration record on the server.
- A network user must submit his/her user name as a means of identifying his/her specific account.
- The password is used to authenticate - or to verify—that the user is who he/she claims to be.
- Users are responsible for understanding and adhering to the following principles when creating or renewing passwords for their user account.
- Users must never share passwords with anyone (including administrators)
- Users must never write down passwords (always memorise it)
- Where an application or environment is capable of enforcing password length, complexity and time then a minimum of 8 characters with enforced complexity and enforced change after 42 day must be created as a policy.
- Users must always use a combination of alpha-numeric special characters (p@$sw0rd)
- Users must not use words from the dictionary or well-known phrases (instead mix words that don't go together & special characters)
- Users must change the password frequently. Specific application vendors will enforce this per environment under the direction of the credit union or automatically as part of the environment's password parameter rules.
- Setting passwords
    - Passwords that can be guessed (by unauthorised persons) create the opportunity for breaches of security. To ensure maximum security, passwords must be difficult to guess—not just by other users but by password cracking programs or pre-defined scripts. Users are required to create strong (hard-to-guess) passwords by following these instructions:
    - Password must be at least eight characters long.
    - Password must be a combination of uppercase and lowercase letters, numerals, punctuation marks, and other special characters.
        - An example of a strong password is - Park#R1ghT— this password has a mix of three of the categories mentioned. Notice there are two unrelated words joined together, but with mixed case and with a special character between them. Joining two words this way also helps you remember your password.
    - Passwords must NOT:
        - contain the word the following - 'password', 'password1' or 'Password1' (this is the most commonly used password)
        - contain the user's real name (first, middle, or last), e-mail name, or any derivative of these
        - contain the name of the application or system

2.5 Network Security

- All network equipment including but not limited to routers, firewalls, switches and cabling patch panels must be secured in a locked room or at a minimum in a locked computer cabinet
- Access to the room and/or cabinet must be restricted to only those requiring access
- The computer cabinet must also be locked if housed in a locked room that is used for other non-IT purposes
- Changes to any network equipment must only be performed by the preferred IT support vendor and follow category approval controls as per CU's Change Management Policy

2.6 Physical Security

- The door to the secure network and comms cabinet must be kept locked at all times
- Access is controlled and is limited to designated personal
- Computer cabinets must be kept locked when not being worked on
- The room area and computer cabinet must be kept clear of obstacles
- The storage of combustible material is prohibited in the computer room area
- Access to the comms cabinet is recorded via a sign in and sign out log for non-routine access
- An internal record of access must be retained regarding access to the comms room

2.7 Software Licencing

- All software applications installed must observe the licencing requirement of the software provider
- All software will be kept within manufacturer support
- Copying and distributing licenced or unlicensed software is prohibited
- All software must be installed by or with the agreement of Management Team
- No unauthorised software installs must take place

2.8 Security Monitoring

- The organisation reserves the right to monitor all computer network traffic regardless of origin that transverse the internal and external network connections used by the organisation
- The organisation reserves the right to monitor and filter any network traffic including but not limited to Internet and email traffic

2.9 Vendor Access

- Remote access to systems must be tightly controlled
- Remote access must only be granted to known and approved vendors
- All access, whether on site or remotely by a third party, must receive prior approval and agreement with the Management Team
- A data protection agreement/NDA must be in place prior to granting remote access
- Secure and encrypted communication technologies must be used when accessing systems remotely
- Full logging and auditing of remote access sessions must be in place including the log on and log off times of each connection

2.10 Remote Access

- Remote access is not permitted for internal users and staff

2.11 Wireless Network Security

- Wireless Network is available on a separate network to corporate data

- Access to this network is password controlled
- Wireless network security is WPA/PSK
- Staff and Board will use this service as required.
- This network is segmented and segregated from the “live” production environment

2.12 Anti-Virus & End Point Protection

- All Computing devices must run up to date managed end point protection software
- It must be updated at least daily
- It must provide operational reports not less than monthly to indicate the Endpoint status of the network
- Full scans must be run on the machine every week, with quick scans ran daily
- The service will generate Monthly Reports which are to be reviewed by the IT Oversight Officer

2.13 Malware

- All Computing devices must run up to date Anti-Malware

2.14 Email-filtering and Web-filtering

- Email filtering is in place through Spam Titan.
- Reports are received daily and weekly on email filtering
- Web-filtering is enforced via Web-Titan and firewall restrictions

2.15 USB Storage Devices

- USB storage devices are blocked with the exception of one authorised user [CEO].
- USBs permitted for use can only be issued by the Management Team and must be encrypted.
- A register of USB storage devices will be maintained within the IT Asset Register.

2.16 Patch Management

- All software will be kept up to date by applying security updates on a scheduled basis.
- All updates will be tested prior to deploying to all machines.
- Critical updates are completed daily on workstations and completed via automatic update
- Critical Standard updates for servers are completed as they are available
- Non critical updates are updated weekly
- 3rd party updates such as Java, Adobe, Flash, Mozilla, Chrome, IE and firmware are managed by users themselves.
- Remote maintenance checks are completed quarterly to verify patch status of critical infrastructure

2.17 Encryption

- Encryption is required for all external connections and for all data transfers to and from the CU network
- This policy must be enforced for all data that is classified as “Confidential”, or that which is subject to Data Protection legislation and GDPR and for the following:
    - Stored on removable media this includes but is not limited to:
        - USB keys
        - Data storage capable devices such as mobile phones, media players, camera, camcorders
        - Portable hard drives
        - Laptops and Notebooks

        - Tablet PCs and devices
    - Emailed outside the organisation
    - Files transferred or uploaded to an external storage location or web site
- Password protection must be used where available
- Uploading of data is only permitted via secure data transfer, all data transfers to a third party or external service must be approved in advance by the Management Team
- Current Encryption levels of TLS 1.2 shall be used in the credit union for data transmission

2.18 Data Classification and Retention

- Data is classified as follows:
    - Confidential is classified as any sensitive information and any data that is defined under Data Protection legislation and GDPR including but not limited to:
        - Member or other person's personal data known as Personally Identifiable Information. Under the Data Protection Act ""*personal data*" *means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller*" (extract from the Data Protection Commissioner's web site)
        - Member account data or information including financial data
        - Personal Public Service Number (PPSN) numbers
        - Payroll data
        - HR data
        - Data or information that is considered copyright or Intellectual Property
        - Medical records or information
        - General accounting and financial data
        - Any document including electronic documents and emails marked confidential, sensitive or for *Internal Use Only*
    - Standard is classified as any data not included in #1 above but must only be distributed either internally or to a Member with a right to the data or information
    - Public is classified as data or information for public release
    - CU have a Data Retention Policy in place

2.19 Warranty

- Where possible all critical equipment will be kept under manufacturer warranty.
- These are Servers, Storage, Firewalls, banking software and operating systems.

2.20 Lifetime Asset Management

- The standard refresh policy for IT hardware equipment will be 5 years
- The standard refresh policy for IT software will be aligned with the most current version available for the vendor.

2.21 Power Protection

- All Critical Equipment will be protected by at least one UPS.

2.22 Personal Computing Devices

- The use of personal computing devices is strictly prohibited on the Credit Union network

2.23 Hardware Refresh

- Critical hardware such as servers, switches, firewalls and desktops will be refreshed as necessary and under advisement from vendors.
- These are Servers, Storage, Firewalls, banking software and operating systems.

2.24 Reporting

Operational Reports will be generated for:

- Backup
  - Alerts and notifications are sent to designated management on success /failure
  - On-site and remote preventative maintenance checks review backup logs
  - Reporting on backup checks are placed in a folder for management review once preventative maintenance is completed
- Security Updates / Patch Management
  - Reporting is provided monthly via Managed Service Providers Report
- Anti-Virus
  - Reporting is provided monthly via Managed Service Providers Report
- Support Ticketing
  - To be downloaded monthly via Managed Service Providers Report web service
- Change Requests
  - To be reviewed monthly against internal records and Managed Service Providers Report ticketing service
- These will be retained for the lifetime of the service and reviewed not less than monthly by the Management Team, external advisors and the managing vendor.

2.25 Acceptable Use

2.25.1 Use of Personal Devices

- Confidential or sensitive data shall never be stored on a personal device.
- All access to IT resources and data must be authenticated by a valid user ID and password
  - See 2.4 for Password Policy and minimum permitted standards

2.25.2 Use of Email

- Use of email must not damage the credit union's brand or reputation.
- Its use must comply with the following:
  - Email MUST NOT to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, hair colour or national origin. Officers who receive any emails with this content must report the matter to the Data Protection Officer immediately
  - Users MUST NOT represent themselves as another individual in electronic communications
  - Users MUST NOT send chain letters or joke emails
  - Users MUST NOT use internet based email such as Gmail, Hotmail, Eircom, etc. for credit union business. A credit union email account will be issued to authorised users.
  - Users must not access personal email from credit union IT resources or devices

- Users MUST NOT use instant messaging programs (such as Google talk, Skype, AIM, MSN messenger, Yahoo messenger, Facebook IM etc.) from credit union IT resources or devices
- Email users must exercise extreme caution with any external attachments as these attachments may contain malware. Be particularly vigilant of email containing attachments.
- Users must be extremely vigilant of unsolicited emails
- Users must verify the provenance of such communications by speaking to a senior manager and if necessary contact the sender to authenticate the communication
- Users must not click on web links within emails without verifying the provenance of the email. Users must contact a senior manager before clicking on such links.
- Email by default is not encrypted therefore users should expect that emails could be read by others.
- Users must not send confidential data especially data which can identify an individual (personal data) or account information.
- Such confidential data must only be sent via a secure encrypted transfer service
- Email is a form of publishing and covered by relevant publishing Acts, libellous and defamatory material is not permitted. Users can be held personally libel for such actions.
- Credit union email accounts [yourname@cu.ie] must not be used for unreasonable personal use.

2.25.3 Internet Usage on Credit Union Equipment

- Standards governing internet usage are designed to ensure officers use the internet in a safe and responsible manner and to ensure that officer web use can be monitored or researched during an incident.
- Users MUST NOT use credit union facilities to download, display, generate and/or pass on to others material whether in text, pictures or any other form, which would be regarded as offensive.
- In law, possession of some material is deemed to be a serious criminal offence, whether in the workplace or otherwise and must be reported to the Gardaí.
- Users MUST NOT download software via the internet unless approved by the Management Committee.
- Users MUST NOT use unauthorised peer to peer or file sharing software
- Users MUST NOT deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others.
- These acts include, but are not limited to:
  - sending mass mailings or chain letters
  - spending excessive amounts of time on the Internet
  - failing to exit from websites
  - engaging in online chat groups
  - uploading or downloading large files

  - accessing streaming audio and/or video files (YouTube etc.)
  - or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.
- Users MUST NOT use the same passwords for login to Internet websites as they do internally for credit union systems.
- All computer activity including internet is logged for the purpose of information security and audit.
- The use of internet facilities is subject to the acceptance of auditing as a business requirement
- The credit union reserves the right to review, audit, intercept, access and where necessary disclose all access to the internet. This includes emails sent and received in addition to websites visited and files downloaded from the Internet.

2.25.4 Mobile Devices

- Mobile devices are valuable business tools but their portability makes them particularly vulnerable to physical damage, theft or loss.
- Mobile devices are defined to include laptops, iPads, iPhones, tablets, Netbooks, USB keys, CDs, Backup tapes, external hard drives and mobile/smart phones.
- All mobile devices containing stored data must use an approved method of encryption to protect data from unauthorised access.
- Officers are expressly forbidden from storing credit union data on devices that are not encrypted.
- Mobile devices must employ full disk encryption with an approved software encryption package. No credit union data may exist on a device in clear text. Devices such as laptops and iPads must be immediately switched off when not in use.
- Credit union data may not be stored on a mobile device.
- Where possible, remote wipe technology will be used to disable and delete any data stored on a credit union mobile device which is reported lost or stolen.
- All keys (i.e. passwords) used for encryption and decryption must comply with the credit union's password standards (as set out above).
- Loss or theft of any mobile device containing credit union data must be reported to the CEO and Risk Manager and Compliance Officer immediately.
- An incident report form must be completed by the user.
- If necessary the incident must be reported to the Office of the Data Protection Commissioner in compliance with its Personal Data Security Breach Code of Practice.
- Care must be taken when using mobile computers in public places, meeting rooms and other unprotected areas outside the credit union's premises.
- Users must not leave mobile devices unattended and must lock them away securely. Padded laptop bags to protect against accidental damage may be required.
- Officers must ensure laptops have the latest anti-virus software updates.
- Users who disconnect from the network must ensure they update anti-virus software when they are away from the office.

- All data must be stored on the network which is backed up rather than on mobile devices themselves.
- Where used, external back up devices must be encrypted.

2.25.6 Working from Home

The CEO is responsible for deciding which operational functions (in addition to those set out above) are appropriate for remote working. He will also ensure that all staff working from home have appropriate equipment and facilities to do so and are capable of adhering to the data security provisions set out in this policy. The CEO will endeavour to provide staff working from home with a reasonable workflow that is consistent with keeping to normal office hours.

- Staff working from home will maintain normal office hours and will make themselves available to deal with queries from colleagues by phone or email within those hours

- Laptops, PCs and other devices used for remote working must have full hard drive encryption, anti-virus, anti-malware and firewall protection. Where the device is provided by the credit union these will be included. Where a personal device is used, the credit union will assist staff in making suitable security arrangements

- Strong passwords must be used for devices and system access

o A strong password should be memorable to the person using it but impossible for someone else to guess

o Passwords used in connection with remote working must be unique. In particular, passwords used for email, online banking and other important personal matters must not be re-used for remote working

o Passwords must not contain personal information or common words and patterns and in particular must avoid the use of:

a. A nickname or initials

b. Names of children or pets

c. Important birthdays or years

d. Street names or numbers from the person's or the credit union's address

e. Obvious words and phrases like "password" or "letmein"

f. Sequences like "abcd" or "1234"

g. Keyboard patterns like "qwerty" or "qaswsx"

- Passwords must be at least 8 characters long, and contain a mix of capitals and characters

- Where the system or application permits the use of passphrases, these may be used, subject to the same caution as applies to passwords

- Ideally, 2 stage verification is recommended, requiring a staff member to enter both their password and a security question or texted code

- Secure WiFi connections must be used, noting that:

- Using an unsecured wireless network without a WPA key (password) is not a safe way to access the internet. Network sniffers are used by people looking to access internet traffic on unsecured wireless

- Many home installed WiFi hubs still use their factory installed admin password. This should be changed to a strong password

- Many home installed Wi-Fi hubs still use their factory installed user password. This should be changed to a strong password

- Where a laptop or other device used for remote working is provided by the credit union, it may be used only for work related activities and no other user accounts may be set up. Any social use of the device, e.g. personal use, on-line gaming, downloading of unauthorised apps, etc. increases the risk of a security breach and is therefore not permitted. Where a private laptop or other device is used for remote working, staff are expected to exercise appropriate caution and restrict access to the device

- While working from home, if a staff member needs to step away from a device for any period the device must be put to 'sleep'. This will require the staff member to re-enter their password to wake up the device and is intended to avoid any accidental keystrokes by curious children or pets

- Paper files may not be removed from the credit union premises. There are too many risks associated with doing this. Any materials required to facilitate remote working should be scanned onto the IT system to ensure secure transmission

- Materials should not be printed outside the credit union. Should this be unavoidable, staff must take all appropriate precautions and ensure documents are kept securely and for as short a time as possible, before being shredded or otherwise destroyed

2.25.7 Use of Social Media

These policy statements are designed to protect the privacy, confidentiality, integrity and interests of the credit union and our current and potential products, officers, partners and members. They apply only to work-related information and issues and are not intended to infringe upon officers' personal lives.

It should be noted that the CEO will be permitted to use social media for digital marketing purposes.

- The credit union recognises that officers may use social media such as Facebook, Twitter, LinkedIn, and YouTube amongst others.
- These media may expose the credit union to risk and vulnerabilities which could impact the brand, reputation and stability of the credit union.
- Publishing information on social media sites about their employment or the credit union could leave officers personally exposed to such threats.
- Publishing personal data regarding individual or commercially sensitive information regarding the credit union will result in disciplinary action being pursued.

- The credit union's name or any such similar term referencing employment at the credit union must NOT be used on social media sites such as Facebook, Twitter, Instagram, Pinterest etc.
- Officers with a Facebook or other social media account must not cite employment details on their profile.
- Any views expressed by any officer on a blog or website are his/hers alone and must not be stated or inferred to reflect the views of the credit union.
- No officer is authorised to publish on behalf of the credit union via social media sites and forms.
- Officers must not share confidential and proprietary credit union information including information about members, their accounts, finances, officers, company strategy, and any other information that has not been publicly released by the credit union.
- These are given as examples only and do not cover the range of what the credit union considers confidential and proprietary. If in doubt, refer to the Management Team.
- The credit union's name or logo must not be used without written permission from the Management Team to prevent the appearance that unauthorised officers may speak for or represent the credit union officially.
- Users are legally liable for anything they write or present online.
- Officers can be disciplined by the credit union for commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment.
- Users who post unlawful content can also be sued by any individual or company that views your commentary, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment.
- All data processed on computers is logged and can be monitored. All computers have a unique identifying address (IP address).

2.26 Asset Disposal and Repurposing (See also Asset Management Policy)

- All data and configuration settings (including User IDs and passwords) must be permanently deleted prior to disposal of equipment.
- 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 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.

2.27 Baseline security and hardening for devices

- 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
- Using containers or virtual machines
- 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

2.28 Clean Desk

Users must ensure that all confidential information, defined within the data classification policy, in hardcopy or electronic form is secure in their work area at the end of the day and for those times when you expect to be absent for an extended period

- Computer workstations must be locked by users before leaving their work area
- Computer workstations must be shut completely down at the end of the working day
- File cabinets containing confidential information must be kept closed and locked when not in use or when not attended. Access must be permitted only to those who are approved by the Management Team
- Keys used for access to confidential information stored in filing cabinets must not be left at an unattended desk
- Keys used for access to confidential information stored in filing cabinets must be under the control of a person approved to have access to the information
- Passwords must not be left on sticky notes posted on or under a computer, nor must they be left written down in an accessible location.
- Printouts containing Confidential Information must be immediately removed from any printer, copier or fax machine
- Upon disposal Confidential documents must be shredded in the official shredder bins or placed in the locked confidential disposal bins
- Whiteboards containing confidential information must be erased.
- Users must lock away portable computing devices such as laptops and tablets at end of day

2.29 System Upgrades (See also Change Management Policy)

- All significant system and software development (new services and modules, significant version upgrades) must follow recommended practices and CU's Change Management Policy.

2.30 Training and Awareness

- All staff will receive regular training and critical updates on cybersecurity and the threat landscape which will include an overview of:
  - Overview of threat landscape
  - Social engineering techniques
  - Awareness of viruses, phishing, and malware
  - Current controls and why they are in place

- Date Protection Responsibilities
- Reporting suspicious behaviour

2.31 Penetration Testing and 3rd Party Assurance

- Penetration Testing of the credit union environment will be conducted annually or after any significant change in the credit unions IT environment (change of firewalls, change of core business systems, change of network support providers, change of core infrastructure, change of connectivity partners).

3.0 Reporting

On a quarterly basis the Board of Directors must receive an IT Compliance Report, and this report must include the following information at a minimum:

- List significant IT events (breaches of policy, disciplinary action for non-compliance, data leak or breach, downtime or outages for key services or systems) and incidents in the previous 12 months
- Impact, downtime, costs, response and remediation for the above incidents
- Results of Penetration Tests and network security audits, outcomes and responses
- Results of DR Tests, outcomes and responses
- Review of training provided to staff and officers
- Review of support issues
- Review of Managed Services Reports
- Review of work completed and scheduled for IT Compliance and Governance

4.0 Policy review and updating

This policy will be reviewed annually by the Management Team. Updates and revisions will be brought to the Board for approval and adoption into the policy at least annually or sooner as deemed necessary.

5.0 Supporting Documents

Documents to be read in conjunction with this policy are:

- Change Management Policy
- Asset Management Policy
- Business Continuity Policy
- Data Protection Policy
- Data Retention Policy