1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all Gateway employees and volunteers. Everyone must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by the Board on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2. Information Security Policy

Gateway Credit Union handles sensitive information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Gateway commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process members information so that we can meet these promises.

Employees handling Sensitive data should ensure:

- Handle Company information in a manner that fits with their sensitivity;
- Limit personal use of Gateway information and telecommunication systems and ensure it doesn't interfere with your job performance;
- Gateway reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Gateway's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly. Gateway will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorized access to confidential data.
- Employees should ensure that technologies should be used and setup in acceptable network locations
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- No information should be held on the hard drive of any laptop or PC, but always saved to the appropriate area on the server.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- USB sticks used for Credit Union business must not also be used for personal business or in personal machines.
- With the exception of the daily backup stored in the safe, no members' data should ever be exported to a USB stick or mobile device.
- Any personal information sent by email must be password protected.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non compliance.

5. Protect Stored Data

- All sensitive members data stored and handled by Gateway and its employees must be securely protected against unauthorised use at all times. Any sensitive data that is no longer required by Gateway for business reasons must be discarded in a secure and irrecoverable manner, in accordance with the retention and destruction schedule.
- Payment card data must never be stored by Gateway Credit Union

6. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Gateway Credit Union if disclosed or modified. **Confidential data includes members personal and financial data**.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure;
- **Public data** is information that may be freely disseminated.

7. Access to members data

All Access to sensitive information should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined. All staff and volunteers are required to have signed confidentiality agreements and to have had training on privacy and data protection

- Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (Role based access control)
- Access to sensitive members information such as financial data, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If members data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained by the Board.
- Gateway Credit Union will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the information that the Service Provider possess.
- Gateway Credit Union Ltdwill ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.

8. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Staff and volunteers should not use Gateway Credit Union systems for personal use.
- Staff and volunteers should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Staff and volunteers should take all necessary steps to prevent unauthorized access to confidential data which includes members personal and financial data .

- Staff and volunteers should ensure that technologies should be used and setup in acceptable network locations
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- If POS devices are used, surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive members information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

9. Protect Data in Transit

All sensitive members data must be protected securely if it is to be transported physically or electronically.

- Paper documents being transported between offices must be held in an opaque folder or sealed envelope.
- Electronic transmission (scanning) should be restricted to known devices. Scans should be deleted once saved to their end file position.

10. Disposal of Stored Data

- All data must be securely disposed of when no longer required by Gateway CU regardless of the media or application type on which it is stored, in accordance with the retention and destruction schedule.
- No payment cardholder data must ever be stored on Gateway systems

11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and volunteers.

The Board member for Data Protection is Philip Jenkins, who will report to the Board at least annually on the operation of this policy.

12. Network security

- Any Gateway CU information must be held within a firewalled environment.
- No non-Gateway device must ever be introduced into the Gateway network.
- Any wireless network must be entirely separate to the network on which members' data is held.
- All hardware and software must be regularly updated and security scans/ antivirus kept up to date
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the Gateway environment.
- All inbound and outbound traffic must be restricted to that which is required for the Gateway data environment.
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- All outbound traffic has to be authorized by management (i.e. what are the whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented
- Disclosure of private IP addresses to external entities must be authorized.
- A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.

13. System and Password Policy

All users, including staff and volunteers with access to Gateway systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:

a) Be as long as possible (never shorter than 6 characters).
b) Include mixed-case letters, if possible.
c) Include digits and punctuation marks, if possible.
d) Not be based on any personal information.
e) Not be based on any dictionary word, in any language.

Passwords must be changed at least quarterly and not written down. Where a record of passwords is kept this must itself be in a password protected file.

Passwords to external systems should only be known to the authorised users of those systems.

14. Anti-virus policy

- All machines must be configured to run the latest anti-virus software as approved by Gateway

Credit Union, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.

- The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
- All removable media (for example floppy and usb others) should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months online and 1 year offline.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans
- End users must not be able to modify and any settings or alter the antivirus software
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

15. Patch Management Policy

- All Workstations, servers, software, system components etc. owned by Gateway must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
- Where ever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches have to be installed within one month of release from the respective vendor and have to follow the process in accordance with change control process.
- Any exceptions to this process have to be documented.

16. Remote Access policy

- It is the responsibility of Gateway employees, volunteers, contractors, vendors and agents with remote access privileges to Gateway's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.
- Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.
- Vendor accounts with access to Gateway network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.
- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity
- All hosts that are connected to Gateway internal networks via remote access technologies will be monitored on a regular basis.

17. Roles and Responsibilities

- The General Manager is responsible for overseeing all aspects of information security, including but not limited to:
- Creating and distributing security policies and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.
- creating and distributing security incident response and escalation procedures that include:
    - Training staff and volunteers in IT and data security and ensuring ongoing awareness and a culture of challenge and care.
    - Ensuring that users have the correct level of access and that passwords are changed/ access deleted when someone leaves. The Board member with responsibility for Data Protection is responsible for reporting on compliance with GDPR and data security.

18. Access Control Policy

- Access Control systems are in place to protect the interests of all users of Gateway Credit Union computer systems by providing a safe, secure and readily accessible environment in which to work.
- Gateway will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.

- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification
- Users are obligated to report instances of non-compliance to the General manager/Board member.
- Access to The Company IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any The Company IT resources and services will be provided without prior authentication and authorization of a user's Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by Gateway policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights

19. Wireless Policy

- Installation or use of any wireless device or wireless network intended to be used to connect to any of the Gateway CU networks or environments is prohibited.
- A quarterly test should be run to discover any wireless access points connected to Gateway network

- Usage of appropriate testing using tools like net stumbler, kismet etc. must be performed on a quarterly basis to ensure that:
- Any devices which support wireless communication remain disabled or decommissioned.
- If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the security officer or any one with similar job description has the authorisation to stop, cease, shut down, and remove the offending device immediately.

If the need arises to use wireless technology it should be approved by Gateway and the following wireless standards have to be adhered to:

1. Default SNMP community strings and passwords, passphrases, Encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves the company.
2. The firmware on the wireless devices has to be updated accordingly as per vendors release schedule
3. The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
4. Any other security related wireless vendor defaults should be changed if applicable.
5. Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of cardholder data.
6. An Inventory of authorized access points along with a business justification must be maintained. (Update Appendix B)

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

_____
Employee Name (printed)

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the Company by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Company, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.
I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the Company security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.
I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

_____
Employee Signature

Practical Aspects of Data and Information Security

Data Protection and Confidentiality: Practical reminders for staff and volunteers serving members

We are registered under the GDPR and bound by duties of confidentiality.

- Ensure that you are talking to the right person. Check signatures or ID if you are unsure. Check signatures on documents against the signature we hold, use telephone security questions, check mobile numbers.
- Every contact is an opportunity to check we hold up to date information on the member.
- Avoid discussing sensitive business in front of other people. Take the member somewhere more private.
- Be aware of phone calls being overheard with confidential information, for instance the member’s balance, NI number, etc.
- Don't discuss a member's business with ANYONE, even your nearest and dearest, or with members of their family. For instance, you can't tell Mr Jones that his wife just came in.

- When you have served the member, their paperwork should be filed out of site. Keep the Collection Sheet entries covered so that members can't see who else has paid in.

- At the end of the working day, all confidential information should be filed, scanned, or shredded.
- Don't leave the computer screen visible to members.
- Avoid discussing a member's Credit Union business if you meet them socially or in the street.
- Keep paperwork in transit secure in a folder/envelope, and deliver to Head Office as soon as possible.
  In some cases, keeping confidentiality can be a matter of personal safety. We have some members who save secretly, and could be at risk if confidentiality is broken.

Access to records:

Members have the right to request copies of information we hold on them.

This needs to be borne in mind when making file notes/ loan assessment notes or adding a telegram on Curtains. Keep anything written factual and brief, please.

Mailing preferences

We aim to send every member an annual statement and invitation to the AGM.

We are encouraging members to opt in to email communication to save us money on postage and printing and to opt in to email news letters.

We will not pass a member’s details to any third party without their written specific consent. (For instance to claim a bonus from their housing association, or refer to debt advisers).

We wish increasingly to contact members to tell them about new services, reminding them to save etc. Every contact with a member is an opportunity to ensure we have their preferences up to date.

Be very careful when posting documents that we have the latest address for the member, and that only the correct document is going in the envelope.

IT Security- practical tips.

No confidential information should be held on a laptop/ C drive in remote offices. Always save to the server.

You must not write your passwords down.

You must not use personal USB sticks on gateway devices or connect personal devices to the Gateway network.

Be alert for scam and virus emails. Delete unopened and empty your junk/deleted folders.

Check emails from members/organisations against the emails we hold for them.

If you have to send confidential information by email (eg a payroll form) it should be password protected, and the password sent separately. We have established passwords with all our partners.

Data Breaches

A data breach is

Losing information.

Accidentally sending the wrong information to the wrong person.

Sharing information that shouldn’t have been shared

Malicious access to our systems.

Keeping information we should not have kept.

All data breaches however minor should be reported on a data breach form and passed to Phil Jenkins