IAFI Information Security Policy

Ice Age Floods Institute
(Company Name)

December 17, 2024
(Date)

Contents

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information.

2. Information Security Policy

Ice Age Floods Institute does not handle sensitive cardholder information

Ice Age Floods Institute commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end IAFI is committed to maintaining a secure environment in which to process customer information so that we can meet these promises.

Employees handling Sensitive cardholder data should ensure they:

- Handle account data including cardholder information in a manner that fits with their sensitivity;
- Limit personal use of Ice Age Floods Institute information and telecommunication systems and ensure it doesn't interfere with job performance;
    - Ice Age Floods Institute reserves the right to monitor, access, review, audit, copy, store, or delete any IAFI electronic communications, equipment, systems and network traffic for any purpose;
- Do not use email, 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 customer and cardholder information;
- Do not use e-mail or other end messaging technologies such as messenger WhatsApp, Signal to share sensitive data including account data in the form of 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 IAFI management.

3. Acceptable Use Policy

Ice Age Floods Institute's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Ice Age Floods Institute's established culture of openness, trust and integrity. Management is committed to protecting the IAFI representatives, partners and Ice Age Floods Institute from illegal or damaging actions by individuals, either knowingly or unknowingly. Ice Age Floods Institute will control approval of technologies, devices and personnel with access to devices.

- IAFI representatives are responsible for exercising good judgment regarding the reasonableness of personal use.
- IAFI representatives should ensure that they have appropriate credentials and are authenticated for the use of technologies
- IAFI representatives should take all necessary steps to prevent unauthorized access to confidential data, which includes cardholder data.
- IAFI representatives should ensure that technologies be setup and used in acceptable manners
- IAFI representatives should keep passwords secure and not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- IAFI representatives must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

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 authorized responsibility and action. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non compliance.

5. Compliance Policy

This policy aims to ensure that Ice Age Floods Institute conducts its business in full compliance with all national and international laws and regulations that pertain to its industry, as well as professional standards, accepted business practices, and internal standards.

- The data processed by Ice Age Floods Institute need to be handled in accordance with the relevant laws, regulations and industry standards.
- Ice Age Floods Institute assets, network diagrams, dataflow diagrams and data storage repositories need to be maintained in accordance with identified laws and regulations.

6. Information Security Procedures and Standards Policy

In relation to this Information security policy and relevant laws, regulations and industry standards, Ice Age Floods Institute needs to maintain up to date documentation and ensure it is relevant, updated when changes are made, and reviewed for accuracy. The documentation may include procedures, standards, asset lists, network diagrams, cardholder flow diagrams.

7. Protect Stored Data

No sensitive cardholder data is stored or handled by Ice Age Floods Institute or its employees.
It is strictly prohibited to store:

- The contents of the payment card magnetic stripe (track data) on any media whatsoever.
- The sensitive authentication data in form of CVV2/CVC2/CAV2/CID (the 3 or 4 digit number on the reverse of the payment card) on any media whatsoever.
- The PIN or the encrypted PIN Block under any circumstance.

8. 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 Ice Age Floods Institute if disclosed or modified. **Confidential data includes account data and cardholder 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.

9. Access to the sensitive cardholder data

All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- Any display of cardholder data should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
- 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 cardholder information such as PAN's, personal information and business data is restricted to IAFI representatives that have a legitimate need to view such information.
- No other IAFI representatives should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Third Party Service Provider (TPSP) or a TPSP that can affect the security of cardholder data, then a list of such TPSP's will be maintained.
- Ice Age Floods Institute will ensure a written agreement that includes an acknowledgement is in place that the TPSP will be responsible for the cardholder data that the TPSP possesses or can affect the security of.
- Ice Age Floods Institute will ensure that there is an established process including proper due diligence is in place before engaging with a TPSP.

- Ice Age Floods Institute will have a process in place to monitor the PCI DSS compliance status of the TPSP.

10. 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.

- IAFI representatives are responsible for exercising good judgment regarding the reasonableness of personal use.
- IAFI representatives should ensure that they have appropriate credentials and are authenticated for the use of technologies
- IAFI representatives should take all necessary steps to prevent unauthorized access to confidential data which includes cardholder data.
- IAFI representatives should ensure that technologies are used and setup in acceptable manners
- POS devices (POI/Terminals) 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 cardholder information must be handled and distributed in a secure manner by trusted individuals.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Strict control must be maintained over the external or internal distribution of any media containing cardholder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media

11. Disposal of Stored Data

- All data must be securely disposed of when no longer required by Ice Age Floods Institute, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed as when no longer required for valid and justified business reasons.

12. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness.

- Review handling procedures for sensitive information.
- Make this security policy document available to all IAFI representatives to read.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Security awareness training needs to include awareness on phishing.

13. Network security

- Ice Age Floods Institute does not maintain a separate computer network. It relies on Google Drive for storage of materials and does not store any sensitive cardholder information.

14. System and Password Policy

All users, including contractors and vendors with access to Ice Age Floods Institute systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- System configuration standards are developed by Google along industry-acceptable hardening standards (SANS, NIST, ISO) which include common security parameter settings
- All users must use a password to access Ice Age Floods Institute electronic resources
- All user ID's for terminated users must be deactivated or removed immediately.
- The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.
- 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 8 characters).
    b) Include mixed-case letters, if possible.
    c) Include digits and punctuation marks, if possible.
    d) Not be based on any personal information.

15. Anti-virus policy

- All systems with access to sensitive data must be configured with anti-virus protections approved by Ice Age Floods Institute.
- Email with attachments coming from suspicious or unknown sources should not be opened. All such emails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any email, which they suspect may contain virus.
- Emails need to be checked for phishing attempts.

16. Patch Management Policy

- Wherever possible all systems and software must have automatic updates enabled for system patches released from their respective vendors.
- Any exceptions to this process have to be documented.

17. System Administration Access policy

- It is the responsibility of Ice Age Floods Institute representatives with administrative access privileges to Ice Age Floods Institute's digital records to ensure that their administrative access connection is strictly controlled.

18. Vulnerability Management Policy

- As part of the PCI-DSS Compliance requirements, Ice Age Floods Institute will regularly run internal and external network vulnerability scans.
- All the vulnerabilities are to be assigned a risk ranking such as High, Medium and Low based on industry best practices.

19. Configuration standards:

- Information systems that process, transmit, or store cardholder data must be configured in accordance with the applicable standard for that class of device or system.
- All network device configurations must be maintained to ensure the configuration continues to meet required standards.
- All discrepancies will be evaluated and remediated by Network Administration.

20. Change Control Process

- Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

- Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with retention and storage management policies.
- All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

21. Audit and Log review

- The following Operating System Events are to be monitored:
  a) Any additions, modifications or deletions of user accounts.
  b) Any failed or unauthorised attempt at user logon.
  c) Any modification to system files.
- The following Database System Events are monitored by the network monitoring system (WordFence on IAFI.org or Google):
  a) Any password that has been changed for an application role.
  b) Any database that has been created, altered, or dropped.
- The following Firewall Events are configured for logging, and are monitored by the network monitoring system (WordFence on IAFI.org or Google):
  a) Invalid user authentication attempts.
  b) Logon and actions taken by any individual using privileged accounts.
  c) Configuration changes made to the firewall (e.g. policies disabled, added, deleted, or modified).
- The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system (WordFence on IAFI.org or Google):
  a) Any vulnerability listed in the Common Vulnerability Entry (CVE) database.
  b) Any generic attack(s.
  c) Any known denial of service attack(s).
  d) Any traffic patterns that indicated pre-attack reconnaissance occurred.
  e) Any attempts to exploit security-related configuration errors.
  f) Any authentication failure(s) that might indicate an attack.
- For any suspicious event confirmed, the following must be recorded:
  a) User Identification.
  b) Event Type.
  c) Date & Time.
  d) Success or Failure indication.
  e) Event Origination (e.g. IP address).
  f) Reference to the data, system component or resource affected.

22. Penetration testing methodology

Penetration testing is handled by WordFence on IAFI.org or Google.

23. Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage your company.
Employees of Ice Age Floods Institute will be expected to report any security related issues to the security officer.

- Ice Age Floods Institute PCI security incident response plan is as follows:
  - Each department must report an incident to the PCI Response Team.
  - A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform Ice Age Floods Institute PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

- Ice Age Floods Institute PCI Security Incident Response Team includes:
    - Webmaster and Communications Director - Lloyd DeKay
    - Assistant Webmaster - Chris Sheeran

Incident Response Notification

- In the event of a suspected security breach, alert the information security office immediately.
    - The security officer will carry out an initial investigation of the suspected security breach.
    - Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.
- Escalation Members
    - Escalation – First Level
        - Ice Age Floods Institute Communications Director: Lloyd DeKay - Webmaster
    - Escalation – Second Level
        - Ice Age Floods Institute President
        - External Contacts (as needed)
        - Merchant/Card Provider
- In response to a systems compromise, the PCI Response Team and designees will:
    - Gather, review and analyze the logs and related information from various central and local safeguards and security controls
    - Contact internal and external departments and entities as appropriate.
    - Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
    - Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.
- Incident Response notifications to various card schemes, card companies have individually specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data.

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after the initial report of the incident to VISA. The following report content and standards must be followed when completing the incident report. Incident reports must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret"*.

I. Executive Summary
    a. Include overview of the incident
    b. Include RISK Level (High, Medium, Low)
    c. Determine if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures
    a. Include forensic tools used during investigation

V. Findings
    a. Number of accounts at risk, identify those stores and compromised
    b. Type of account information at risk

c. Identify ALL systems analyzed. Include the following:
    - Domain Name System (DNS) names
    - Internet Protocol (IP) addresses
    - Operating System (OS) version
    - Function of system(s)
d. Identify ALL compromised systems. Include the following:
    - DNS names
    - IP addresses
    - OS version
    - Function of System(s)
e. Timeframe of compromise
f. Any data exported by intruder
g. Establish how and source of compromise
h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
i. If applicable, review VisaNet endpoint security and determine risk

VI. Compromised Entity Action
VII. Recommendations
VIII. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand

MasterCard Steps:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured email to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.
2. Distribute the account number data to its respective issuers.

Employees of Ice Age Floods Institute will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within Ice Age Floods Institute and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.
Discover Card Steps 1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention 2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances 3. Prepare a list of all known compromised account numbers 4. Obtain additional specific requirements from Discover Card
American Express Steps 1. Within 24 hours of an account compromise event, notify American Express Merchant Services 2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances 3. Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express

24. Roles and Responsibilities

- Chief Security Officer (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to:
    - Creating and distributing security policies and procedures.
    - Ensure that security controls are maintained
    - 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
    - Manage the vulnerability management and penetration testing program
    - Maintain a list of service providers.
    - Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
- The Information Technology Office (or equivalent) shall maintain administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).
- Network Administrators shall:
    - Maintain network devices.
    - Ensure that networks are securely configured.
- System and Application Administrators shall:
    - Monitor and analyse security alerts and information and distribute to appropriate personnel.
    - Administer user accounts and manage authentication.
    - Ensure that systems and devices are securely configured.

25. Third party and security of cardholder data

- All third-party companies providing critical services to Ice Age Floods Institute must:
    - Adhere to the PCI DSS security requirements.
    - Acknowledge their responsibility for securing the CardHolder data.
    - Acknowledge that the Cardholder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
    - Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.

- Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.

26. User Access Management

- Access to Ice Age Floods Institute's website, IAFI.org, is controlled through a formal user registration process.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions.
- There is a standard level of access that will inform IT operations of all leavers and their date of leaving.

27. Access Control Policy

- Access Control systems are in place to protect the interests of all users of Ice Age Floods Institute.
- 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
- 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.

28. Encryption Policy

- Cardholder Data (CHD) must be rendered unreadable when stored and use strong encryption such as AES 256 or Triple DES 168-bit encryption and associated key management.

Appendix A - List of Third Party Service Providers

- Name of Service Provider
  - WooCommerce
  - PayPal

Appendix B – POI Management Policy

Where Ice Age Floods Institute are utilizing POI's the following policies are applicable:

- POI Device Inventory and Management:
  - Maintain an up-to-date inventory of all POI devices, including make, model, location, and serial number.
  - Establish procedures for securely adding, relocating, and decommissioning POI devices.
- Physical Security Measures:
  - Secure POI devices to prevent tampering or substitution. This includes using tamper-evident seals or enclosures.
  - Regularly inspect devices for signs of tampering or substitution.
  - Implement secure storage for devices not in use.
- Device Inspection and Maintenance:
  - Conduct regular inspections and maintenance of POI devices to ensure they are functioning correctly and haven't been compromised.
  - Document and maintain a record of all inspections and maintenance activities.
- Secure Configuration and Software Management:

    - Ensure that POI devices are configured securely and in compliance with PCI DSS requirements.
    - Implement measures to prevent unauthorized changes to software and configuration settings.
    - Regularly update POI device software, including patches for known vulnerabilities.
- Access Controls:
    - Restrict access to POI devices to authorized personnel only.
    - Use strong authentication methods for administrative access to POI devices.
    - Implement role-based access controls and segregate duties to minimize the risk of unauthorized access or changes.

Appendix C – eCommerce Configuration and Hardening Policy

Where Ice Age Floods Institute are utilizing redirect and iFrame solutions to take payments for the eCommerce environment, Ice Age Floods Institute need to apply system configuration and hardening of these systems as follows:

- Establish a Standard eCommerce Server Configuration that includes necessary services, protocols, and settings to:
    - Ensure that vendor default accounts are changed, removed or disabled.
    - Disable unnecessary services and protocols to minimize vulnerabilities.
    - Ensure that all security settings are aligned with industry best practices.
- Implement Hardening Procedures:
    - Implement strong authentication and authorization mechanisms.
    - Use file integrity monitoring tools to detect unauthorized changes.
    - Enforce the use of antivirus and anti-malware solutions.
- Regularly Review and Update Configurations:
    - Periodically review server configurations against the established standard.
    - Update the configurations in response to new threats, vulnerabilities, or changes in organizational needs.
- Maintain a Vulnerability Management Program:
    - Regularly scan for vulnerabilities and address identified weaknesses.
    - Include both software and physical components in your vulnerability assessments.
    - Establish a process to check for new security vulnerabilities and include the following:
        - Industry recognized sources
        - Risk ranking process based on industry best practices and identification of vulnerabilities that are high risk.
    - Regularly update and patch operating systems and software to fix vulnerabilities.