Security Incident Response Plan

Freedom & Liberty Worship Center Inc

Introduction

All security incidents must be managed in an efficient and time effective manner to make sure that the impact of an incident is contained and the consequences for your business and your customers are limited. This document sets out the Freedom & Liberty Worship Center Inc plan for reporting and dealing with security incidents.

What is a Security Incident?

A Security Incident means any incident that occurs by accident or deliberately that impacts your communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data, or services in Freedom & Liberty Worship Center Inc.

This includes unauthorized access to, use, disclosure, modification, or destruction of data or services used or provided by Freedom & Liberty Worship Center Inc

An 'Account Data Compromise' is a security incident specific to payment card data. It is an event that results in unauthorized access to or exposure of payment card data (cardholder data or sensitive authentication data). If an unauthorized person obtains payment card data from your business, they can use this data to commit fraud.

How to Recognize a Security Incident

A security incident may not be recognized straightaway; however, there may be indicators of a security breach, system compromise, unauthorized activity, or signs of misuse within your environment, or that of your third-party service providers. You need to look out for any indications that a security incident has occurred or may be in progress, some of which are outlined below:

- Monitor excessive or unusual log-in and system activity, in particular from any inactive user IDs (user accounts)
- Watch out for excessive or unusual remote access activity into your business. This could be relating to your staff or your third-party providers
- The occurrence of any new wireless (Wi-Fi) networks visible or accessible from your environment
- The presence of or unusual activity in relation to malware (malicious software), suspicious files, or new/unapproved executables and programs. This could be on your networks or systems and includes web-facing systems.
- Hardware or software key-loggers found connected to or installed on systems
- Suspicious or unusual activity on, or behaviour of, Web-facing systems, such on as your ecommerce website
- Point-of-Sale (POS) payment devices, payment terminals, chip & PIN/signature devices or dip/swipe card readers showing signs of tampering
- Any card-skimming devices found in your business
- Lost, stolen, or misplaced merchant copy receipts or any other records that display the full payment card number or card security code (the 3- or 4-digit number printed on the card)
- Lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain payment card data or other sensitive data

Roles and Responsibilities

Your security incident response plan must be followed by all personnel in your business. This includes all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of Freedom & Liberty Worship Center Inc, working with Freedom & Liberty Worship Center Inc's or your customers' data or on Freedom & Liberty Worship Center Inc premises. For simplicity, all of these personnel are referred to as 'staff' within this plan.

Roles

The Freedom & Liberty Worship Center Inc Security Incident Response Team (SIRT) is comprised of:

Role*	SIRT Responsibility	Name	Email	Telephone
Pastor	Incident Response Lead	Eddie Sawyers	pastor@fandl.org	Cell: (336) 345-0004
Elder, Finance	Incident Response Technical Lead	Wayne Stonestreet	Wayne.stonestreet@fandl.org	Cell: (336) 403-3616 Home: (336) 444-4041
Elder	Oversight	Bob Hauser	bhauser@surry.net	Cell: (336) 428-7097
Elder	Oversight	Adrian Joyce	adrian.joyce@fandl.org	Cell: (336) 972-1778
Treasurer	Financial Review	Barbara Lundquist	bel@fandl.org	Cell: (203) 448-7603

Responsibilities

The Incident Response Lead is responsible for:

- Making sure that your Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to make sure that the handling of security incidents is timely and effective.
- Making sure that the Security Incident Response Plan is up to date, reviewed and tested, at least once each year.
- Making sure that staff with Security Incident Response Plan responsibilities are properly trained, at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan, as and when needed.
- Reporting to and liaising with external parties, including the acquirer and card brands, legal representation, law enforcement, etc. as is required.
- Authorising on-site investigations by appropriate law enforcement or payment card industry security/forensic personnel, as required during any security incident investigation. This includes authorising access to/removal of evidence from site.

Security Incident Response Team (SIRT) members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.
- Investigating each reported incident.
- Taking action to limit the exposure of sensitive or payment card data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing, and analyzing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Reporting each security incident and findings to the appropriate parties. This may include the acquirer, card brands, third party service providers, business partners, customers, etc., as required.
- Assisting law enforcement and card industry security personnel during the investigation processes. This includes any forensic investigations and prosecutions.
- Resolving each incident to the satisfaction of all parties involved, including external parties.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All staff members are responsible for:

- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT);
- Reporting any security related issues or concerns to line management, or to a member of the SIRT;
- Complying with the security policies and procedures of Freedom & Liberty Worship Center Inc. This includes any updated or temporary measures introduced in response to a security incident (e.g. for business continuity, incident recovery or to prevent recurrence of an incident).

External Contacts

External Party	Contact Name (if known)	Email	Telephone
ACS Technologies Site #163209	Support	clientupdates@acst.com	(800) 669-2509
Surry County Sheriff's Office	Sheriff Steve Hiatt	[Insert Details]	(336) 401-8900
DOJ: REPORTING COMPUTER, INTERNET-RELATED, OR INTELLECTUAL PROPERTY CRIME	Reporting computer hacking, fraud, and other Internet related crime.	Report online: https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime	(202) 514-2000
For use if you are unable to contact your acquirer:			
Visa Inc Incident Response - US	-	usfraudcontrol@visa.com	(650) 432-2978

*note: country-by-country data protection and breach notification legal requirements can be found on global law firm DLA Piper's Data Protection Laws of the World (https://www.dlapiperdataprotection.com/) or ICLG's Data Protection Comparison site (http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016).

Payment Card Brands:

The payment card brands have specific requirements for reporting and responding to suspected or confirmed breaches of payment card data. As a merchant business your primary contact if an incident occurs should always be your acquirer. It is worthwhile referring to the links below to familiarize yourself with the detail of the card brands' recommendations around how to respond to Account Data Compromises and what their specific requirements are.

MasterCard:
https://www.mastercard.us/content/dam/mccom/en-us/documents/account-data-compromise-manual.pdf

Visa Global:
https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

American Express:
https://www209.americanexpress.com/merchant/services/en_US/data-security (includes links to all information for all territories)

Discover Card:
http://www.discovernetwork.com/merchants/fraud-protection/index.html

Incident Response Plan Steps

There are a number of steps and stages that you must be taken to make sure that you protect your business by reacting to a security incident appropriately.

Report

1. Information security incidents must be reported, without delay, to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT). The member of the SIRT receiving the report will advise the Incident Response Lead of the incident.
   In the event that a security incident or data breach is suspected to have occurred, we recommend the staff member discuss their concerns with their line manager, who in turn may raise the issue with a member of the SIRT.

Investigate

2. After being notified of a security incident, the SIRT will perform an initial investigation and determine the appropriate response, which may be to initiate the Security Incident Response Plan.
   If the Security Incident Response Plan is initiated, the SIRT will investigate the incident and initiate actions to limit the exposure of cardholder data and in mitigating the risks associated with the incident.
   Initial incident containment and response actions

Make sure that no-one can access or alter compromised systems.

- Isolate compromised systems from your network and unplug any network cables – without turning the systems off.
- If using a wireless network, change the SSID (Service Set Identifier) on the wireless access point and other systems that may be using this wireless network (but not on any of the systems believed to be compromised).
- Preserve all logs and similar electronic evidence, e.g. logs from your firewall, anti-virus tool, access control system, web server, application server, database, etc.
- Perform a back-up of your systems to preserve their current state – this will also facilitate any subsequent investigations.
- Keep a record of all actions you and all members of the SIRT take.
- Stay alert for further indications of compromise or suspicious activity in your environment, or that of your third parties.
- Seek advice before you process any further payment card transactions.
- If you can, gather details of all compromised or potentially compromised payment card numbers (the ‘accounts at risk’).

Inform

Once the SIRT has carried out their initial investigation of the security incident:

3. The Incident Response Lead will alert the SIRT’s senior management primary contact.
4. The Incident Response Lead and / or the SIRT personnel responsible for communications / PR will inform all relevant parties. This includes your acquirer and local law enforcement, and other parties that may be affected by the compromise such as your customers, business partners or suppliers. This also includes the personal data breach notification contacts, as applicable to the incident under investigation.

Maintain Business Continuity

5. The SIRT will engage with operational teams in your business to make sure that your business can continue to operate while the security incident is being investigated.

Plan Ahead!

Be prepared - in advance of any security incident that may impact your business, you should make sure you have a plan for how your business would operate if your systems and processes were unable to operate as normal.
For example:

- Make sure you have system and data backups available in the event of loss of data, system corruption/virus infection or hardware failure.
- Consider what offline or alternative payment acceptance methods you could use if you were unable to take card payments on your ecommerce website, in-store or over the telephone using your usual methods.

Resolve

6. The SIRT will liaise with external parties, including your acquirer, law enforcement, etc., to ensure appropriate incident investigation (which may include on-site forensic investigation) and gathering of evidence, as is required.
7. The members of the SIRT will take action to investigate and resolve the problem to the satisfaction of all parties and stakeholders involved. This will include confirmation that the required controls and security measures are operational.
8. The Incident Response Lead will report the investigation findings and resolution of the security incident to the appropriate parties and stakeholders (including your acquirer, local law enforcement, etc.) as is needed.

Recovery

9. The Incident Response Lead will authorize a return to normal operations once satisfactory resolution is confirmed.
10. The SIRT will notify the rest of the business that normal business operations can resume. Normal operations must adopt any updated processes, technologies or security measures identified and implemented during incident resolution.

Review

The SIRT will complete a post-incident review after every security incident. The review will consider how the incident occurred, what the root causes were and how well the incident was handled. This will help to identify recommendations for better future responses and to avoid a similar incident in the future.

Changes and updates that may be required include:

- Updates to the Security Incident Response Plan and associated procedures.
- Updates to your business' security or operational policies and procedures.
- Updates to technologies, security measures or controls (for example, improved measures to inspect payment terminals for card skimmers).
- The introduction of additional safeguards in the environment where the incident occurred (for example, more effective malware protection).

11. The SIRT Executive Officer/Risk Owner (the senior management primary contact) will ensure that the required updates and changes are adopted or implemented as necessary.

Specific Incident Response Types

Plan for Your Business!

This Security Incident Response Plan provides the generic steps that must be followed when dealing with a security incident. You must update the plan to include security incident types and responses that are specific to your business environment and operational activities.

Some specific incident types requiring additional response actions are provided below.

Malware (or Malicious Code)

i. Disconnect devices identified with malware from the network immediately.
ii. Examine the malware to identify the type (e.g. rootkit, ransomware, etc.) and establish how it infected the device. This will help you to understand how to remove it from the device.
iii. Once the malware has been removed a full system scan must be performed using the most up-to-date signatures available, to verify it has been removed from the device.

iv. If the malware cannot be removed from the device (as is often the case with rootkits) it should be rebuilt using original installation media or images. Prior to restoration from back-up media/images you must verify that the back-up media/images are not infected by the malware.

v. Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack.

Tampering of payment terminals, chip & PIN/signature devices or card readers detected, Card-skimming devices found, or devices substituted

i. Stop using the substituted/tampered devices

ii. Report the substitution/tampering to your device provider and your acquirer

iii. Follow your device provider or acquirer's advice to ensure the security of all future card payments, e.g. inspect and confirm the integrity of your remaining devices, deploy replacement devices, etc.

iv. Follow your device provider or acquirer's guidance to investigate the incident e.g. send the substitute/tampered devices to them, allow on-site investigations, etc.

Unauthorized Wireless Access Points

If unauthorized wireless access points are detected, or reported by staff, these must be recorded as a security incident.

i. SIRT will investigate to identify the location of the unauthorised wireless access point/device.

ii. The SIRT will investigate as to whether the unauthorised wireless access point/device is being used for a legitimate business purpose/need. If a legitimate business reason is identified, then this wireless access point or device must be reviewed and go through the correct management approval process. This is to make sure that the business justification is documented, and the wireless access point/device is securely configured (e.g. change default passwords and settings, enable strong authentication and encryption, etc.).

iii. All other unauthorised wireless access points/devices must be located, shutdown and removed.

Loss of Equipment

i. The theft or loss of an asset, such as a PC, laptop, or mobile device, must be reported immediately to a member of the SIRT and local law enforcement. This includes losses/thefts outside of business hours and at weekends.

ii. If the device that is lost or stolen contained sensitive or payment card data, and the device is **not** encrypted, SIRT will complete an analysis of the sensitivity, type and volume of data stolen, including any potentially exposed payment card numbers.

iii. Where possible, SIRT will use available technology/software to lock down/disable lost or stolen mobile devices (e.g. smart phones, tablets, laptops, etc.) and initiate a remote wipe. Evidence should be captured to confirm this was successfully completed.

Non-Compliance with your Security Policy

This covers incidents resulting from deliberate or accidental actions that are in breach of your security policy and which put sensitive and payment card data at risk. This includes any systems or data misuse, unauthorized exposure of data to external parties, unauthorized changes to systems or data.

i. SIRT will engage with the relevant business area to establish an audit trail of events and actions. They will determine who is involved in the policy violation and the extent of the violation.

ii. SIRT and/or line managers will notify Human Resources of the incident.

iii. SIRT will liaise with Human Resources and line managers to determine whether disciplinary action is needed.

iv. SIRT will undertake an assessment of the impact and provide advice and guidance to the business area to prevent reoccurrence, for example re-training of staff.

Testing and Updates

Annual testing of the Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the SIRT are aware of their obligations, unless real incidents occur which test the full functionality of the process.

1. The Incident Response Plan will be tested at least once annually.
2. The Incident Response Plan Testing will test your business response to potential incident scenarios to identify process gaps and improvement areas.
3. The SIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
4. The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.

Document Control

Document Name:	Security Incident Response Plan
Current Version:	20200520-01
Plan Owner:	Wayne Stonestreet
Plan Approver:	Elders- Eddie W. Sawyers, Adrian Joyce, Robert Hauser and Wayne Stonestreet
Date of Last Review:	May 20, 2020
Organization:	Freedom and Liberty Worship Center 171 Key Street Pilot Mountain, NC 27041 (336) 444-8052