Major Incident Management Guideline

Date of Origin: 12 November 2013
Date of Revision: N/A

SOURCE

This guideline is issued under the authority of the Chief Information Security Officer (CISO). Inquiries concerning this guideline should be directed to the Guideline Steward.

PRINCIPLES

Major incident management allows the CISO to oversee and coordinate incidents of a serious nature.

SCOPE

This guideline applies to all Church organizations within the Corporation of the Presiding Bishop, the Corporation of the President, and international areas.

BACKGROUND

As the *Information Security and Compliance Incident Management Policy* describes, the Presiding Bishopric acts under the direction of the First Presidency to manage certain incidents, including information security and compliance incidents. Major incidents are escalated to the Chief Information Security Officer (CISO), who organizes a major incident management team as appropriate. Team representation usually includes executives of any affected organizations, delegates from ICS, Legal, Public Affairs, Privacy, Church Security, etc. This Guideline further describes escalation and coordination steps.

GUIDELINES

1. **Escalate to CISO.** The Security Engineering manager escalates to the CISO based on belief that a compromise has occurred that may involve one or more of the Major Security Incident considerations (see definition below).
2. **Major Incident Classification**. The CISO decides whether an incident is Major. The following questions may be used to help the CISO validate if an incident is Major:
   - Is more data needed and does any data need further validation?
   - Is immediate action needed to prevent or contain spiritual, operational, financial, reputational, regulatory, or physical harm?
   - Should the CIO be notified?
   - Do we need to notify legal, security, public affairs, intellectual property, or another Church process owner?
   - Are there victim-notification needs?
   - Are there regulatory or contractual obligations?
3. **Major Incident Procedures**. If the CISO classifies the incident as Major, the following steps should be followed:

   3.1. Gather known and suspected information about the incident, such as method(s) of attack, targets, impacts, perpetrators, motivation, and so on

   3.2. Act to prevent or contain imminent spiritual, operational, financial, reputation, regulatory, or physical harm

   3.2.1. If necessary, take action prior to constitution of the major security incident management team. To the extent possible, decide and implement as a team in steps 3.5 – 3.7.

3.3. Notify CIO (who further communicates with the Brethren)
3.4. Form security incident management (SIM) team
3.5. Create and implement an incident coordination plan (ICP, see *Appendix: Incident Coordination Plan Template* below)
    3.5.1. Establish status communication methods and frequency
    3.5.2. Create desired outcomes and next steps for each objective
    3.5.3. Document resolution, lessons learned
3.6. Monitor remaining Information Security Incident Management (ISIM) steps
3.7. Successfully manage the incident

REFERENCES

Information Security and Compliance Incident Management Policy and Protocol
Information Security Incident Management (ISIM) Process & Procedures, 21 September 2012

DEFINITIONS

Significant Security Incident. A cyber-attack that was successful or targeted a sensitive Church asset.
Major Security Incident. The CISO classifies whether an incident is Major based on such considerations as:

- Spiritual, operational, financial, reputational, regulatory, and physical safety
- Need to coordinate with senior leaders
- Need to involve legal, public affairs, intellectual property, or security
- Potential impact to key Church operations or reputation
- Need to notify victims
- Regulatory or contractual obligations

STANDARD STEWARD

Tony Blackham +1 (801) 240-3802

EXECUTIVE SPONSOR

Michael Carter +1 (801) 240-0633

REVISION HISTORY

Version	Date	Description	Author
1.0	11/12/2013	Original Publication; minute number ICSSTDS-A-2014-0002.	M. Carter B. Hendricks D. Stovall M. Sanderson

Appendix: Incident Coordination Plan Template

INCIDENT SHORT TITLE:

INCIDENT DESCRIPTION

- Known targets:
- Suspected targets:
- Method(s) of attack:
- Date initially reported or detected:
- Earliest date of known associated events:
- Is activity ongoing? Yes/No
- Impact Description:
- Perpetrator and Motivation Description:
- Other:

GATHER INFORMATION

- Throughout coordination, continue to add to and validate information used to build the incident description, above

ACT

- Take any immediate steps urgently needed to prevent or contain harm to persons or vital Church assets or processes

NOTIFY CIO

- Method and date of CIO notification:

FORM SIM TEAM

- Use the following table as a reference for constituting a SIM team

Standing SIM Team Roles	Key Duties
Office of the CISO	Team Lead
Affected Managing Directors	- Provide needed information and resources - Take appropriate corrective action
Affected Data Stewards	- Validate data sensitivity - Strengthen data handling controls as needed
ICS Engineering	- Provide systems analysis and resources - Implement containment and strategic corrections
ICS Security Engineering	Validate initial containment

Ad Hoc SIM Team Roles	Key Duties
General Counsel (Matt Richards, 801-328-3600)	Analyze legal requirements and give counsel
Church Security (Greg Dunn, 2-9912)	- Investigate internal criminal activities - Manage interaction with law enforcement

Public Affairs (Michael Otterson, 2-7439)	Manage media interaction
Intellectual Property (Berne Broadbent, 2-8099)	Lead privacy analysis and privacy-breach notification
ICS Security Operations (Ryan Gibbons, 2-4173)	Assist with containment and resolution validation
Church Controller (Alan Bott, 2-0640)	Assess financial data issues
Church Records Management (Alan Johnson, 2-0849)	Lead records management analysis
Human Resources (Ben Porter, 2-4773)	Manage interaction with involved employees
Church Auditing (Greg Dahl, 2-6294)	Investigate material impact and associated controls

> List selected SIM team members:

STATUS COMMUNICATION METHOD(S) AND FREQUENCY:

Method	Frequency
>	
>	
>	

COORDINATION OBJECTIVES

Desired Outcome	Lead	Needed Resources	Next Step	Resolution Description and Date
>				
>				
>				
>				
>				

MONITOR ISIM

ISIM Phase	Resolution Description and Date
> ISIM 3.0 Short-Term Containment	
> ISIM 4.0 Long-Term Containment	
> ISIM 5.0 Eradicate	
> ISIM 6.0 Recover	
> ISIM 7.0 Close	

LESSONS LEARNED

>

Template last revised: 11/7/2013