EXTREME FUNDING

Incident Management Policy, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted

Document Owner: Information Security Committee

Last Review Date: December 2022

Incident Management Policy

Purpose

The purpose of the Extreme Funding Incident Management Policy is to describe the requirements for dealing with information security incidents.

Audience

The Incident Management Policy applies to executive management and other individuals responsible for protecting Extreme Funding Information Resources.

Contents

Policy

Incident Handling Team (IHT)

- An Incident Handling Team (IHT) will be established; consisting of legal experts, risk managers, and other department managers that should be involved in decisions related to incident response.
- The IHT is responsible for:
  - ensuring that incident response activities are carried out in accordance with legal, contractual, and regulatory requirements.
  - internal and external communications pertaining to information security incidents.
  - ensuring that personnel are trained on how to report a potential incident.

Response Team

- An Incident Response Commander will be appointed to oversee and direct Extreme Funding incident response activities.
- The Incident Response Commander will assemble and oversee a Cyber Security Incident Response Team (CSIRT).
- The CSIRT will respond to identified cyber security incidents following the Incident Response Plan.
- The Incident Response Commander is responsible for appropriately reporting incidents to the CIO/IHT.

Incident Response Plan (IRP)

- The Incident Response Commander is responsible for overseeing the creation, implementation, and maintenance of an Incident Response Plan (IRP).
- The Incident Response Plan must be tested by the CSIRT and IHT no less than annually.

Incident Reporting

- Management must provide a means for all personnel to report potential incidents. Reporting methods should ensure that a potential incident is promptly escalated to the appropriate person.
- IT is responsible for monitoring event logging, vulnerability management, and other logs for suspicious activities.
- All reported incidents must be assessed by a member of the CSIRT or IHT to determine the threat type and activate the appropriate response procedures. All members of the CSIRT or IHT must be familiar with how to assess and escalate a potential incident.
- The Incident Response Commander must report the incident to senior leadership.
- Senior leadership must report any potential breaches and/or incidents involving customer data to the Incident Handling Team (IHT) promptly.

Notification and Communication

The IHT is responsible for ensuring that notification and communication both internally and with third parties (customers, vendors, law enforcement, etc.) based on legal, regulatory, and contractual requirements take place in a timely manner.

All Information concerning an incident is considered confidential, and at no time should any information be discussed with anyone outside of Extreme Funding without approval of executive management and our legal counsel.

- Personnel
  - Personnel should be notified whenever an incident or incident response activities may impact their work activities.
  - Internal communications should aim to avoid panic, avoid the spread of misinformation, and notify personnel of appropriate communication channels.
- Interaction with Law Enforcement
  - Interaction between law enforcement and emergency services personnel should be coordinated by the Incident Response Commander or a member of the IHT.
  - Legal counsel should be consulted in communications with law enforcement.
- Customers and Partners
  - All customers and partners who are affected by the incident must be notified according to applicable contract language, service level agreements (SLAs), applicable statutes and/or regulations.
  - Communications with customers and partners must be consistent, with the same or similar message delivered to each.
- Regulatory Authorities
  - Only members of the IHT are permitted to discuss the nature and/or details of an incident with any regulatory agencies.

  - The IHT must contact regulators as required or as soon as practical. (See Incident Response Plan **Error! Reference source not found.**)
- **Public Media**
  - The IHT or executive management will assign a designated spokesperson responsible for communication with the media.
  - Inquiries from media agencies must be directed to the designated spokesperson and the IHT.

Refer to Incident Response Plan: **Error! Reference source not found.** for guidance in communicating with the Media.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 16
- NIST CSF: PR.IP, DE.DP, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS-IM, RC.CO
- Incident Response Plan
- Vulnerability Management Policy
- Logging Standard
- Vulnerability Management Standard

Waivers

Waivers from certain policy provisions may be sought following the Extreme Funding Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	**December 2022**		**Extreme Funding**	**Document Origination**

EXTREME FUNDING

CYBERSECURITY INCIDENT REPORT FORM

Use this form to report any cybersecurity issues, breaches, hacks, malware, or any other incidents involving a 3rd party.

Date and Time of Incident: [DATE/TIME]

CONTACT PERSON

Full Name: [NAME] Address: [ADDRESS]

Job Title: [TITLE]

Phone: [PHONE] E-Mail: [E-MAIL]

THE INCIDENT

Date of Incident: [DATE] Time: [TIME] ☐ AM ☐ PM

Type of Incident: ☐ Malware ☐ Data Breach ☐ Other: [OTHER]

How was the incident detected / discovered? [DESCRIBE DETAILS]

ATTACK VECTOR

Do you know how the attack was made? ☐ Yes ☐ No

If yes, describe: [DESCRIBE]

IMPACTED SERVICES

Was anything permanently impacted by the incident? ☐ Yes ☐ No

If yes, describe: [DESCRIBE]

INFORMATION IMPACT

Was there any data, records, or information breached? ☐ Yes ☐ No

Was there any data, records, or information modified specifically? ☐ Yes ☐ No

If yes, describe: [DESCRIBE]

CONTAINMENT

Were any containment measures made? ☐ Yes ☐ No

If yes, describe: [DESCRIBE]

OTHER

Is there any other information you would like to include in this report? ☐ Yes ☐ No

If yes, describe: [DESCRIBE]

OFFICE USE ONLY

Report received by: [NAME] Date: [DATE]

Follow-up action taken: [DESCRIBE]