Incident Response Policy

LFAS, LFF and LFCM

Policy ID: ISMC 38 LFAS LFF
Created: November 2025
Document Version: 2025.11
Prepared By: David Mauzey, Chief Information Officer

Product Lines:

LEVEL FOUR® Advisory Services
A DIVISION OF LEVEL FOUR GROUP, LLC

LEVEL FOUR® Financial
A DIVISION OF LEVEL FOUR GROUP, LLC

LEVEL FOUR® Capital Management
A DIVISION OF LEVEL FOUR ADVISORY SERVICES, LLC

Policy: Incident Response Policy LFAS, LFF and LFCM

Introduction and Document purpose

This Information Security Policy provides an outline of the principles, responsibilities, and practices that govern the response to a cyber or data incident across our organization. Its primary purpose is to ensure the confidentiality, integrity, and availability of data associated with Level Four Group's core products:

- Level Four Financial
- Level Four Advisory Services
- Level Four Capital Management

This program applies to employees, contractors, and third-party partners who interact with these systems. The policy is owned and maintained by David Mauzey, Technology Contact, with oversight provided by Jill Zacha, Corporate Counsel and CCO, Level Four Advisory Services, LLC and Level Four Capital Management, LLC , and Kimberly Miller, CCO, Level Four Financial, LLC, to ensure alignment with regulatory requirements and organizational standards.

The focus of this policy is on Incident Management and Response. For a full view of all components of our Information Security Policy, please refer to "LFG Information Security Program" documentation which contains the comprehensive security guidelines and references to supportive policies.

Plan Review and Updates

Programs, policies, standards and guidelines are reviewed and updated annually in collaboration with our parent company, Carr, Riggs and Ingram (CRI) Security and Technology departments.

Summary of Reg-SP

The SEC's amendments mandate that covered institutions (including wealth management firms) implement a written incident response program that includes:

- Development and management of a customer information protection program that safeguards customer data.
- Manage an Incident Response Program built to detect, respond to, and recover from unauthorized access to or use of customer information, which includes procedures to:
    - Assess and categorize the scope of any incident and identify affected systems/data.
    - Contain and control the incident to prevent further unauthorized access or use.
    - Notify affected individuals whose sensitive customer information was accessed or likely accessed, as soon as practicable and no later than 30 days after awareness.
    - Diagnose and adjust based on root cause analysis.
- Service provider oversight including without limitation the requirement for vendors to notify the firm within 72 hours of discovering a breach.

- Recordkeeping policies including the maintenance of written documentation of incidents, responses, and notifications for five years.

Sensitive customer information includes any data that could cause substantial harm if compromised (e.g., SSNs, account numbers) and only "applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes."

Regulation S-P

Name of Supervisor ("designated Principal"):	LFF – Kimberly Miller LFCM and LFAS – Jill Zacha
Frequency of Review:	Ongoing in daily course of business
How Conducted:	Customer file reviews Enforce information security procedures; train personnel in information protection
How Documented:	Account information Records of monitoring and testing, if required, of internal systems; ensure and document third party monitoring/testing of systems, if applicable.
WSP Checklist:	SEC Regulation S-ID
Comments:	Also reference Business Continuity Plan for technical details on document back-up and the Firm's Cybersecurity and ID Theft Prevention Program, if applicable.

Level Four Group, LLC., Level Four Financial, LLC., Level Four Advisory Services, LLC., and Level Four Capital Management, LLC, Level Four Insurance Agency, LLC. (Collectively "the Firms") have adopted the following procedures in addition to those contained within its Cybersecurity and Identity Theft Prevention procedures to comply with Reg. S-ID and related state regulations regarding the protection of confidential client information and the reporting of breaches.

The Firms are committed to protecting the confidentiality of all nonpublic information regarding its clients and Associated Persons ("Nonpublic Personal Information").

It is each of the Firm's policy to protect and maintain the accuracy of client personal information. To protect client personal information, the Firms have developed this Written Information Security Program ("WISP"). The intent of this WISP is to safeguard the Firm's storage of access to, and disposal of client personal information, obtained and/or maintained in hard copy and/or electronically, as well as access and protection of its computer and information systems.

1.0 Purpose

With Level Four being a part of CRI, they help provide Level Four with a strong information security policy foundation and framework. These policies work in tandem and complement Level Four centric policies also included in this document. Since these policies complement each other, we leverage the CRI policy where alignment to SEC's Reg-SP framework aligned.

In an instance where you have a question specific to either the CRI General Organizational Policies or the Level Four Group Centric policies, please reach out to Level Four Compliance and Technology leadership to get further information.

The purpose of this policy is to establish a formal framework for detecting, responding to, and recovering from cybersecurity incidents involving unauthorized access to or use of customer information, in compliance with SEC Regulation S-P amendments effective December 3, 2025.

The policy will also provide guidelines and references to tools which may be used to help respond, communicate and return to normal operations once a breach has been identified. Tools may include key activity check lists templates, identification of Incident Response team members and communication templates.

2.0 Scope

Applies to entities who have oversight of Level Four Advisory Services (LFAS), Level Four Financial (LFF) and Level Four Capital Management (LFCM) systems, networks, and processes handling customer information, including data managed by third-party service providers.

The program "applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes." As referenced in the Reg-SP documentation, "publicly available" data not under definition of an incident include: data available in government records (real estate records, etc), "widely distributed media" (phone directories, etc) and "disclosures to public" which are required by government agencies.

This policy does not apply to non-SEC, non-FINRA product lines including, but not limited to, Level Four Business Solutions and Level Four Insurance Agency, LLC *(to the extent products solicited and sold are strictly fixed insurance products)* . For incident response policies related to these entities, please refer to the LFG Information Security Program documentation and the ISCM 38 – Incident Response policies.

3.0 Roles and Responsibilities

As a part of this policy, an Incident Response Team (IRT) will be activated to help manage the incident and help ensure alignment to the policy details.

Roles and Responsibilities

- **Chief Information Security Officer (CISO):** Overall accountability for policy implementation and compliance.
- **Legal & Compliance:** Ensures regulatory adherence and manages breach notifications.
- **Chief Advisor Operations Officer:** Executes technical and operational response steps
- **Incident Response Team (IRT):** Executes technical and operational response steps.
- **Third-Party Vendors:** Must comply with contractual obligations to report breaches within 72 hours.

Incident Response Team (IRT) Roster

Department	Role	Named Resource	Email
	Chief Information Security Officer		
Technology	Chief Information Officer	David Mauzey	dmauzey@levelfourfinancial.com
Legal & Compliance	Corporate Counsel | Chief Compliance Officer, Advisory	Jill Zacha	jzacha@levelfourfinancial.com
Compliance	Chief Compliance Officer, Brokerage | AML Compliance Officer	Kimberly Miller	kmiller@levelfourfinancial.com
Operations	Chief Advisor Operations Officer	Claudia Martin	cmartin@levelfourfinancial.com
Vendor	Various	Various	Various

The team will gather once an incident has been identified. In addition, the team will meet annually to review and align to the annual policy review.

4.0 Policy

As a part of this policy, an Incident Response Team (IRT) will be activated to help manage the incident and help ensure alignment to the policy details.

Cyber-security Framework

- **Protect**
  - MFA, SAML, PIM, Abnormal email security
  - Tools: Palo Alto, iManage, MS Defender, Insight
- **Incident Detection & Assessment:**
  - Identify
    - Approach: Early, continuous learning
    - Tools: InsightIDR, MS Defender/DLP, Spirion, etc

- Detect
  - MFA, SAML, PIM, Abnormal email security
  - Tools: Palo Alto, iManage, MS Defender, Insight
- Quarterly: Review current user access and privileges to impacted systems
- Identification of an Incident
  - Initial Assessment:
    - Determine if sensitive customer information was accessed.
    - Evaluate potential for substantial harm or inconvenience.
  - After the initial assessment of an incident, gather the IRT to discuss available information. Common origination sources include
    - Communication from CRI network team
    - Communication from Vendor
    - Internal communication from an employee or contractor
    -
  - The IRT Team will review the information and provide a scope based upon scope of the incident.
  - Begin an investigation and start working the items in the Incident Checklist.
    - Identify unauthorized access, determine scope, classify severity.

- **Containment & Control:** Isolate affected systems, revoke compromised credentials, prevent escalation.
  - Tools**:** MS Defender, InsightIDR, InsightConnect
- **Recovery:** Restore systems and validate integrity before resuming normal operations.
  - Approach: Shadow copies, High-availability, modern architecture and recovery
  - Tools: Avamar, One drive, sFTP
- **Service Provider Oversight:** Written agreements requiring timely breach reporting and cooperation. Periodic reviews of incidents.
- **Documentation:** Maintain records of incidents, investigations, notifications, and remediation actions for five years.

Program Operational Support

- Formal Policies & Procedures
  - Uniform corporate policies & standards
  - Formal change control program
  - Adherence Monitoring
- Employee Training

    - Ongoing training, targeted modules by job responsibilities, Regulatory and Security
    - Tools: KnowB4
- Governance
    - Uniformed corporate security policies and standards
    - Formal Change Control policy and process
    - Platform to monitor and track adherence to NIST framework throughout all of CRI <-- this is in active development
    - Security team reports directly to the Director of IT who reports directly to the CEO and Board
    - This allows security initiatives and concerns to be addressed at the highest level
    - Dedicated Security Team
    - Annual Security training and awareness
    - Regular Phishing Test
- Access Controls
    - Physical
        - Keycard access, targeted video monitoring
        - Location Physical best-practice training
        - Geolocation tracking on company devices
    - Technology
        - Host and Perimeter firewalls
        - Host and server antivirus and antimalware
        - Endpoint protection and endpoint response
        - Long complex passwords with expiration
        - Password Manager to secure non-AD accounts
        - Office 365 email threat & behavior analysis
        - Multi-Factor authentication
        - Local disk encryption
        - Formal Data Destruction Policy and process
        - Geolocation tracking on physical assets
        - Access to network and cloud resources from foreign countries denied
        - VPNs which require certificates
        - Network segregation through VLans
        - Vulnerability Management
        - Regular patching from corporate
        - Regular vulnerability scanning
        - Centralized logging and SEIM platform
- BCP/DR
    - High availability, WORM,
    - Formal DR and BCP programs
    - Vendor Management
        - Tiered approach depending on sensitivity of data

        - Risk Classifications
        - Due Diligence requests
        - 3rd part attestations
        - Vendor security questionnaires
        - Centralized platform for documentation of all CRI vendors
- Compliance
    - Dedicated technology security team
    - Dedicated regulatory compliance team
    - Monitor ongoing regulatory rule changes

Initial Reg-SP Program Configuration

- Vendor Alignment to Policy Changes and Reg-SP scope: Each vendor will need to align to the Reg-SP notification requirements of 72 hours.
    - Level Four will deliver communication with our expectations of Reg-SP to all vendors that utilize, process or house client PII.
    - Supply our vendors with incident response contact information.
- Establish a "named" Incident Response Team.
- Create sample client communication templates
- Creation sample internal communication templates
- Create a checklist of internal action items
- Set up an annual policy review which includes evaluating the tools, Response team, templates and check lists.

Ongoing Reg-SP Configuration

- General Duties
    - Annually: Incident Response Team to meet to review, discuss and finalize any adjustments to the Incident Response Policy.
    - Annually: Certify new Incident Response Policy by receiving approval from the IRT team.
    - Annual Policy Review:
        - Provide a copy of Incident Response Policy to internal teams
            - Operations
            - Compliance
            - Technology
            - Executive Committee
    - Annually: IRT to Review and align email templates to current Reg-SP guidelines.
    - Annually: IRT to review and align check list templates to current Reg-SP guidelines.
    - Periodically: CRI IT Security to re-assess current vendor.

4.1 Incident Management

- Notification of an incident:
  - 4.1.1 Once notification has been received, the information should be moved to the CIO for initial assessment. If the CIO is not available, to the CAOO (Chief Advisor Operations Officer).
  - 4.2.1 Vendor breaches require notification within 72 hours of discovery.
  - 4.3.1 CIO to provide an initial analysis and perform a high-level severity classification. Note: This classification is only an initial review, severity can change once more information has been gathered and analyzed.
  - 4.4.1 Perform an initial review and provide an initial impact assessment to IRT.
  - 4.5.1 IRT Team will review known facts at the time of identification and confirm or adjust the initial severity classification on the incident. As new information is discovered, classification may be adjusted to align to new facts.
- Forms of Communication

  Under the December 2025 amendments to Regulation S-P, firms must notify affected individuals as soon as practicable and no later than 30 days after determining that sensitive customer information was accessed or likely accessed without authorization. The rule does not prescribe a single channel but requires that notices be clear, timely, and effective. Common and recommended methods include:

  4.1.1 Written Notices (Primary Requirement)
  - Postal Mail: Traditional letters remain the most common and SEC-preferred method for official breach notifications.
  - Email: Permitted if the customer has consented to electronic delivery or if email is the firm's standard communication channel.
  - Secure Portal Message: For firms that maintain client portals, posting a secure message combined with an email alert is acceptable.

  4.2.1 Supplemental Channels
  - Phone Calls: Often used for high-risk incidents or VIP clients to ensure immediate awareness.
  - SMS/Text Alerts: May be used as an additional alert, but not as the sole method.
  - Website or Public Notice: Required only if individual contact details are unavailable or if the breach affects a very large population.

  4.3.1 Content Requirements
  - Description of the incident and compromised data.

- Steps the individual can take to protect themselves.
- Contact information for assistance.

4.4.1 **Timing**

- Delivered within 30 days of awareness, unless delayed for law enforcement or national security reasons.

- Severity classification:
  - Criteria used to classify data
    - Type of data involved (Public, PII, PHI, IP, other)
    - Number of Affected Individuals
    - Potential for financial or reputational harm

Severity	
Low	No sensitive data involved; minimal impact.
Medium	Sensitive Data involved; minimal impact
High	Sensitive data involved; broad impact.

Severity	
3	High Risk: PII compromised with greater than 500 Clients impacted.
4	Medium Risk: Under 500 Clients impacted.
5	Low Risk: Data impacted but incident does not contain PII.

- Check list creation:
  - Leverage the Check List Template to create a personalized incident check list.
  - Identify all layers of the organization who will participate in the management and recovery process.
  - Assigned named owners for each check list area.
  - Daily documented review of check list milestones, activities and status.

5.0 Communication Protocols

- Internal (For detailed tasks, please see the LFG Incident Response Checklist Processing Guide). Below are a few highlights.
  - Immediate alert to Internal Response Team “IRT”

    - Incidents categorized as “High” requires notification to executive leadership within 48 hours.
    - Incidents originating from vendors require a notification of 72 hours.
    - Ongoing status updates during active incidents to IRT team.
- External (For detailed tasks, please see the LFG Incident Response Checklist Processing Guide). Below are a few highlights.
    - Client Notification
        - Annual Client Privacy Notification to active clients.
        - Incident Communication
            - Letter and email Communication: Tenants of good communication
                - Use plain-language heading
                - Type fonts size and style that is easy to read
                - Provide wide margins
                - Bold/Italicize key words
            - Website Communication: Tenants of good communication
                - Place notification on a highly visible location
                - Place where clients typical navigate to
        - Timeframe: Notify client within 30 days of discovery
        - Scope of Notification: Create list of potential impacted clients with email and contact information.
        - Leverage email template to create the incident specific communication. The template will provide a framework; however, the communication should detailed information specific to the incident.
        - Leverage letter template to create the incident specific communication. The template will provide a framework; however, the communication should detailed information specific to the incident.
        - Leverage website template to create the incident specific communication. The template will provide a framework; however, the communication should be tuned to include information specific to the incident.
- **Outbound Regulatory Notification:**
    - Notify SEC and other applicable regulators as required.
    - Confirm address of regulatory address from Compliance and Legal.
- **Inbound Internal Escalation:** See incident response checklist for detailed tasks. Below are a few highlights.
    - Incident notification is received from various sources.

- The CIO will perform an initial broad evaluation of the incident reach and place a severity score.
- IRT will be convened.
- The Incident Response checklist will begin to be executed. For specific tasks, please see the Incident Response Checklist.
- Final approval of plan IRT.
- Work with credit bureau on sending out one year subscription to credit monitoring.
- Finish execution of incident checklist.

- **Inbound Vendor Notification:** Vendors must notify us within **72 hours** of discovering a breach and provide, at a minimum, the following information where available:

  - Date and time vendor discovered the incident
  - Date and time vendor determined it was a "security incident" involving customer information
  - Description of the incident (ransomware, unauthorized access, lost device, email compromise, etc.)
  - Systems, databases, or services affected
  - Whether your firm's customer information is involved
  - Type(s) of customer information exposed (name, address, SSN, DOB, account numbers, login credentials, etc.)
  - Estimated number of your clients affected (can be preliminary)
  - Whether the data was accessed, exfiltrated, altered, or deleted
  - Whether data was encrypted at the time of the incident
  - Whether the threat actor is known or suspected
  - Whether law enforcement has been engaged

- Required Vendor Supporting Documentation

  - Initial forensic summary, even if preliminary
  - Timeline of events
  - Description of containment actions taken
  - Description of remediation actions in progress
  - Expected timeline for further updates
  - Point of contact for continued communication