**Policy 4125: Incident Response**

Note: While CU PolicyPro does not contain a Cybersecurity Policy per se, Policies 4120 and 4125 used together fulfill cybersecurity policy expectations. It is also important to note that Policy 4120 is more than a cybersecurity policy, in that it includes physical security and other, non cybe’ security considerations.

**Model Policy Revised Date12/24/2024**

**General Policy Statement:**

[[CUname]] (Credit Union) recognizes its responsibility to safeguard member information and will treat the private financial information of the Credit Union's members ("member information") with appropriate care to maintain the confidentiality, integrity, and security of member information. The Credit Union will ensure that incidents of unauthorized access to member information are addressed immediately, including notice to the membership as well as the proper authorities. The purpose of this policy is to set forth the guidelines for management and staff to use in establishing and maintaining policies and procedures to address incidents of unauthorized access to member information. The Credit Union will comply with all applicable laws and regulations governing the safeguarding of member information including NCUA Guidelines for Safeguarding Member Information (12 CFR Part 748 Appendices A and B, Part 749 Appendix B) (the "Guidelines") and all other applicable laws and regulations regarding the safeguarding of member information.

**Definitions:**

* **Compromise**means the unauthorized disclosure, modification, substitution, or use of sensitive data or the unauthorized modification of a security-related system, device, or process to gain unauthorized access.
* **Cyber Incident**is an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system or actually or imminently jeopardizes, without lawful authority, an information system.
* **Cyberattack**means an attack, via cyberspace, targeting an enterprise's use of cyberspace to disrupt, disable, destroy, or maliciously control a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
* **Disruption** means an unplanned event that causes an information system to be inoperable for a length of time.
* **Event**Any observable occurrence in a system and/or network. Events sometimes indicate that an incident is occurring (CNSSI-4009). Events occur without supporting log evidence of an incident.

**Event examples:**

* Employee visits website prohibited by policy
* Brief exposure of unpatched system
* Limited-service disruption
* **Incident**An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies (NIST SP 800-53). Incidents may include but are not restricted to, the following: violation of policy, unauthorized information system use, denial of resources, and information system changes without consent.

**Incident examples:**

* Malicious hacker gains unauthorized access to a database containing sensitive member information,
* Criminal commits fraud by manipulating transaction data, Corporate Account Takeover, email account takeovers, used voice-based fraud tactics (vishing),
* Distributed denial-of-service (DDoS) attack launched against critical Credit Union information system resources,
* Ransomware deployed through phishing email campaigns, etc.
* Advanced Persistent Threats (APTs) (highly skilled threat actors often backed by nation-states or criminal organizations),
* Exploitation of artificial intelligence (AI) or Internet of Things (IOT) vulnerabilities,
* **Sensitive data**means any information which by itself, or in combination with other information, could be used to cause harm to a credit union or credit union member and any information concerning a person or their account that is not public information, including any non-public personally identifiable information.
1. **RESPONSE PROGRAM.**Management will be responsible for developing and implementing a risk-based response program to address incidents of unauthorized access to sensitive and/or member information.

	1. **Security Response Team and Security Response Leader.** Credit Union management shall establish a security response team responsible for preventing, detecting, and handling suspected incidents involving member and other sensitive information. The team will have a designated [team leader] as well as a deputy team leader who assumes authority in the absence of the team leader. Members of the team shall be adequately trained and equipped to develop, document, and enact an Incident Response Plan. Team members should include personnel from several Credit Union departments including, but not limited to, the following: information technology, business management, legal, human resources, internal auditing, and facilities. Involving personnel from multiple departments ensures that the Incident Response Plan will cover mission-critical business processes, systems, and information assets.

Instead of creating a security response team, the Credit Union may appoint a single employee to oversee incident response. The incident response leader will work with internal personnel and third-party service providers to ensure that an Incident Response Plan is in place, incorporates appropriate third-party services, is tested, and is approved by Credit Union officials.

Lastly, either the security response team or the leader will be responsible for acquiring outsourced incident response services, as needed, to ensure that the Credit Union has access to the requisite knowledge and tools to handle security incidents.

* 1. **Service Providers.** Contracts with service providers will stipulate that the provider take appropriate actions to address incidents of unauthorized access to or use of the Credit Union’s member information, including notification to the Credit Union as soon as possible of any such incident, to enable the Credit Union to implement its Incident Response Plan promptly.
	2. **Incident Severity Levels.** The security response team or leader will develop criteria for measuring the severity of incidents based on their impact on business functions, their impact on member information, and the amount of effort and time required to recover from them. The severity of an incident is a subjective measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response.

The following factors are considered in determining the severity of an incident:

Four levels of incident severity will be used to guide incident response: high, medium, low, and NA (“Not Applicable”).

***High***
The severity of a security incident will be considered “high” if any of the following conditions exist:

High-severity incidents require an immediate response and focused, dedicated attention by the Incident Response Coordinator and other appropriate Credit Union officials until remediated. These incidents also have extensive notification and reporting requirements, as outlined in the Incident Response Summary Table below. A Post-Incident Report is required.

***Medium***
The severity of a security incident will be considered “medium” if any of the following conditions exist:

Medium-severity incidents require a quick response by appropriate personnel (usually from the affected unit) who have primary responsibility for handling the incident. Notification requirements are outlined in the Incident Response Summary Table below. A Post-Incident Report is not required unless requested by the [4125-1]] or another appropriate administrator.

***Low***
Low-severity incidents have the following characteristics:

Since a single compromised system can “wake up” and negatively affect other systems at any time, appropriate personnel (usually the technical support staff responsible for the system) must respond as quickly as possible, no later than the next business day. Notification requirements are outlined in the Incident Response Summary Table below. A Post-Incident Report is not required unless requested by the [[4125-1]].

***NA ("Not Applicable")***
This is used for events reported as a suspected IT security incident, but upon investigation, no evidence of a security incident is found. This usually corresponds to the incident category, "No Incident."

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Incident Severity** | **Characteristics (one or more condition(s) present that determine the severity** | **Response Time** | **Incident Manager** | **Who to Notify** | **Post-Incident Report Required** |
| **High** | 1. Significant adverse impact on a large number of systems and/or people
2. Potential large financial risk or legal liability to the Credit Union
3. Threatens confidential data
4. Electronic funds have been compromised
5. Adversely impacts a critical enterprise system or service
6. Significant and immediate threat to human safety
7. High probability of propagating to a large number of other systems causing significant disruption
 | Immediate | Incident Response Coordinator | [[4125-1]] | Yes |
| **Medium** | 1. Adversely impacts a moderate number of systems and/or people
2. Adversely impacts a non-critical enterprise system or service
3. Adversely impacts a departmental system or service
4. Disrupts a building or departmental network
5. Moderate risk of propagating and causing further disruption
 | 4 Hours | Appointed by unit head | [[4125-1]] | No, unless requested by [[4125-1]] or other appropriate administrator |
| **Low** | * + 1. Adversely impacts a very small number of non-critical individual systems, services, or people
		2. Disrupts a very small number of network devices or segments
		3. Little risk of propagation and further disruption
 | Next Business Day | Technical support for the affected device | [[4125-1]] | No |
| **N/A** | “Not Applicable” – used for suspicious activities which upon investigation are determined not to be an IT security incident. |

* + 1. Scope of impact – how many people, departments, or systems does it affect?
		2. Criticality of the system or service – how important is it to the continuing operation of the institution? What would be the impact on the business, either functional or financial, if this system or service were unavailable or corrupted?
		3. Sensitivity of the information stored on or accessed through the system or service – does it contain confidential data, such as personal identity information or account information?
		4. Probability of propagation – how likely is it that the malware or negative impact will spread or propagate to other systems, especially to other systems?
		5. Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)
		6. Poses a potential large financial risk or legal liability to the Credit Union.
		7. Threatens confidential data (for example, the compromise of a server that contains names with social security numbers or account information)
		8. Electronic funds have been compromised
		9. Adversely impacts an enterprise system or service critical to the operation of a major portion of the Credit Union (for example, e-mail, financial information system, human resources information system, Internet service, or a major portion of the Credit Union’s network)
		10. Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group
		11. Has a high probability of propagating to many other systems causing significant damage or disruption
		12. Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building
		13. Adversely impacts a non-critical enterprise system or service
		14. Adversely impacts a departmental system or service, such as a departmental file server
		15. Disrupts a branch or departmental network
		16. Has a moderate probability of propagating to other systems and causing moderate damage or disruption
		17. Adversely impacts a very small number of systems or individuals
		18. Disrupts a very small number of network devices or segments
		19. Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate
	1. **Incident Response Preparedness.** The Credit Union shall prepare an incident response toolkit containing items for effective administration and communication of the Incident Response Plan (e.g., smartphones and contact information) as well as dedicated incident response hardware and software (e.g., laptops, blank removable media, and packet sniffers). The Credit Union will be prepared to handle incidents arising from common methods of attack.
	2. **Incident Detection.** The Credit Union shall monitor information system events to detect indicators of information security incidents and threats to sensitive member information. To facilitate forensic activities, event data produced by system monitoring tools will be regularly backed up and protected from unauthorized access. Examples of security incident indicators include the following: IDS/IPS alert; physical evidence of break-in or theft of assets; or a threat made to the Credit Union. The security response team leader will have the authority both to define what events constitute incidents and to define what events must be monitored. The Credit Union can include tools such as endpoint detection and response systems (EDR), and managed detection and response systems (MDR) to help automate some of the detection capability. Additionally, expanded detection capabilities to include reconnaissance activities (e.g., unusual scanning) and privileged escalation attempts should be monitored.
	3. **Assessment of Incident.** The security response team will assess the nature and scope of an incident and identify what member information has been accessed or misused. The team will use the severity levels defined in Section 1.C to prioritize incident response actions.
	4. **Containment and Control.** Appropriate steps will be taken to contain and control an incident to prevent further unauthorized access to or use of member information while preserving records and other evidence. Examples include monitoring, freezing, or closing affected accounts. The security response team shall work to secure and preserve evidence by acquiring and protecting a system snapshot or record before further actions are taken. The team will establish a chain of custody for evidence and ensure that all incident response activities are documented. The team leader will witness and record the technical team member’s evidence-handling tasks. Special attention should be placed on provisions for the Credit Union to securely communicate and collaborate during incident response.
	5. **Recovery.** The Credit Union recognizes that restoring the affected information system to a trusted state will require skilled technicians, dual-control procedures, and a potentially significant interruption of services. Possible remediation of the vulnerabilities that resulted in the incident will be included in the recovery process. The Credit Union will, as practicable, heighten monitoring of mission-critical information system assets potentially affected by the incident. Testing of backup capability should occur, at a minimum, annually, with specific scenarios such as ransomware and critical system failures.
	6. **Internal Reporting.** Following discovery of an intrusion or disaster to the Credit Union's systems or facilities, the CEO or acting Senior Management officer shall report to the Chairman of the Board and the Supervisory Committee as soon as reasonably possible following a receipt of a report of an intrusion or disaster and the initial implementation of the Incident Response Plan.
	7. **External Reporting.** Following the discovery of an intrusion or disaster to the Credit Union's systems or facilities and upon completion of internal reporting and implementation of the Incident Response Plan, management will report the incident to its bonding company, casualty insurance company, local law enforcement agencies, the appropriate regulatory agency and complete and file a Suspicious Activity Report (SAR) as necessary.
	8. **Post-Incident Activities**
		1. After an incident has been handled, the security response team will produce a report containing, but not limited to, the following information regarding the incident:
			1. Scope
			2. Cause and costs
			3. Short-term and long-term impacts
			4. Short-term and long-term recovery expectations
			5. Lessons learned documentation focused on root cause and enhancement of control measures
		2. By documenting lessons learned, the security response team will determine what aspects of the Incident Response Plan must improve and consider adding or improving information security controls to avoid repeat incidents. Vulnerabilities that were not remediated as part of incident handling will be documented and a plan of action will be devised to remediate them. Incident metrics such as Mean Time to Detect (MTTD) and Mean Time to Restore (MTTR) can assist with assessing the effectiveness of the response activities. Incident response evidence shall be retained for attacker prosecution purposes. All post-incident activities must be reported to Credit Union officials and approved by the Board and/or Supervisory Committee.
	9. **Denial-of-Service and Ransomware Incidents.** To mitigate the impact of denial-of-service (i.e. attrition) attacks, the security response team will, if possible, leverage boundary protection devices to filter traffic, increase capacity and bandwidth, and/or employ service redundancy (NIST SP 800-53). To respond to a ransomware attack, the security response team will work to recover the data from backups if possible or contact a predetermined third-party service provider capable of rendering assistance.
	10. **Corporate Account Takeover.** A form of business identity theft where cyber criminals can control a business' financial account by stealing employee passwords and other valid credentials. These criminals can then initiate fraudulent wire and ACH transactions to accounts they own. To mitigate the impact of a takeover, the credit union will comply with existing Bank Secrecy Act (see 2110), Digital Banking (see 2225) policies, and corresponding procedures to comply with the identification of high-risk members and associated activity.
	11. **Notifying Members.** As per NCUA requirements specified in 12 CFR Part 748 Appendix B, members will be notified of an incident when it is warranted. When an incident occurs on information systems maintained by service providers, the Credit Union, under the guidance of legal advice, will notify the appropriate regulatory authority and its members. (The service provider contract may authorize the service provider to meet these obligations, but the Credit Union incident response leader will be ultimately responsible for ensuring that this is done.) More details regarding member notification policies are provided in Section 2 of this Policy.
	12. **Staff Training**. Management will develop procedures to ensure that staff are trained to appropriately handle member inquiries and requests for assistance. Staff shall be trained to be able to detect suspicious activity and to know how and to whom to report the activity. This training will be conducted both before and after an actual incident. Members of the incident response team shall receive adequate training to carry out their duties in the Incident Response Plan. General training and specialized training shall occur upon hire or initial adoption of responsibilities and at a Credit Union-defined frequency.
	13. **Incident Response Testing.**
		1. Management will test the effectiveness of the incident response plan. Examples of effective testing methods include checklists, tabletop exercises, and scenario simulations. Examples of scenarios include, but are not limited to, the following:
			1. Employee reports suspicious email (i.e. phishing)
			2. Compromised application database revealed by log review
			3. Intrusion detection system alert triggered on (unscheduled)
		2. Incident response testing results shall be documented, incorporated as lessons learned in incident response improvement efforts, and reported to Credit Union officials. Incident response testing shall occur at a Credit Union-defined frequency (at a minimum, annually) All incident response testing plans will be submitted to the Board and/or Supervisory Committee for approval.
1. **MEMBER NOTICE.** Notification to members will be made timely and in consultation with legal counsel to minimize the Credit Union’s reputation and legal risks. Member notice procedures shall adhere to NCUA guidance in 12 CFR Part 748 Appendix B.

	1. **Investigation.** Once the Credit Union becomes aware of an incident of unauthorized access, the [[4125-1]] or security response team will conduct a reasonable investigation, with any necessary assistance from third-party agencies such as: Cyber Insurance Company, Digital Forensics Firm, Legal Counsel, and/or technical assistance, to promptly determine the likelihood that the information has been or will be misused. If the likelihood is high, the affected member(s) will be notified as soon as possible. However, if an appropriate law enforcement agency determines that such notice would interfere with a criminal investigation and provides a written request for delayed notification, notice to the member(s) will be provided as soon as it would no longer interfere with the investigation.
	2. **Affected Members.** Notification may be limited to those members to whom the Credit Union knows to have been affected by an intrusion whenever the Credit Union believes misuse of the information has occurred or is reasonably possible. If a group of files has been accessed improperly, but the Credit Union is unable to specify the affected members and the misuse of their information is likely, the Credit Union will notify all of the members in the group.
	3. **Content of Member Notice.** Notice to members will be developed in consultation with legal counsel and comply with NCUA regulations.

1. **Threat Intelligence and Information Sharing.** The Credit Union may also share information regarding information security incidents to federal and/or federally sponsored resources such as the National Credit Union Information Sharing and Analysis Organization (NCU-ISAO), Financial Services Information Sharing and Analysis Center (FS-ISAC), InfraGard, Cyber Information Sharing and Collaboration Program (CISCP), etc.
2. **CYBER INCIDENT REPORTING**. In compliance with NCUA Part 748, Management must notify the NCUA point of contact via email, telephone, or other similar method of a **reportable cyber incident** as soon as possible, but no later than 72 hours after a possible **reportable cyber incident** is believed to have occurred.

	1. **Reportable Cyber Incident** is any substantial cyber incident that leads to one or more of the following:

		1. A substantial loss of confidentiality, integrity, or availability of a network or member information system that results from the unauthorized access to or exposure of **sensitive data**, disrupts vital member services, or has a serious impact on the safety and resiliency of operational systems and processes.
		2. Disruption of business operations, vital member services, or a member information system resulting from a **cyberattack** or exploitation of vulnerabilities.
		3. Disruption of business operations or unauthorized access to **sensitive data** facilitated through, or caused by, a **compromise** of a credit union service organization, cloud service provider, or other third-party data hosting provider or by a supply chain compromise.

**References:**

National Institute of Standards and Technology (NIST). Special Publication 800-53 (Rev. )5 Security Controls and Assessment Procedures for Federal Information Systems. Incident Response Control Family and NIST Cybersecurity Framework (CSF) 2.0