# ABC Credit Union
# Computer Incident Response Team – Access & Authorization Policy

**Course Name: IAP401**
**Student Name: Dang Hoang Nguyen**

## Policy Statement:

In the case of a security breach or other incident, ABC Credit Union's Computer Incident Response Team (CIRT) has complete access to and authority over all IT systems, applications, data, and physical IT assets. This policy gives CIRT members permission to carry out tasks that are required to uphold Chain of Custody while conducting forensic investigations and gathering evidence.

## Purpose/Objectives:

- Describe the Security Incident Response Team's makeup.
- Give CIRT members permission to act during emergencies or security events.
- Make ensuring that IT security best practices and the GLBA are followed.
- During forensic investigations, preserve Chain of Custody and improve incident response capabilities.

## Scope:

This policy is applicable to all ABC Credit Union CIRT members and pertinent staff. This policy's scope includes all of the organization's systems, applications, data, physical facilities, and IT assets. CIRT members are given access and authority beyond what is often expected of them in order to carry out forensic analysis and evidence collection, among other tasks required for incident response.

## Standards

This policy for incident response and forensic investigations is in line with industry best practices. It places a strong emphasis on following Chain of Custody procedures in order to protect the authenticity and acceptability of evidence. It also facilitates GLBA compliance and complies with pertinent IT security regulations.

## Procedures

Composition of CIRT:

- Members of the CIRT are specially trained individuals with knowledge of IT security, forensic investigation, and incident response.

Authority and Permission:

- CIRT members are permitted to access and look into any IT systems, apps, data, and physical IT assets that belong to the company in the event of a security breach or other issue.
- Members of the CIRT are authorized to carry out essential tasks, such as system analysis, data gathering, evidence preservation, and remediation measure implementation.

Implement the six-step incident response approach as the incident response strategy. Steps to take include :

- preparation
- identification
- containment
- eradication
- recovery
- Knowledge Acquired

Chain of Custody:

- To guarantee the integrity and admissibility of evidence in court hearings, maintain Chain of Custody throughout the evidence collection process.
- Keep thorough records of all the actions done by CIRT members and document the processing of the evidence.

**Guidelines:**

- Give CIRT members the tools and training they need to improve their incident response and forensic analysis abilities.
- As needed, closely coordinate incident response efforts with law enforcement and legal counsel.
- Review and update incident response policies and procedures on a regular basis to take into account evolving risks, technological advancements, and legal requirements.

## Lab #8 – Assessment Worksheet

## Craft a Security or Computer Incident Response Policy – CIRT Response Team

**Course Name: IAP401**
**Student Name: Dang Hoang Nguyen**
**1. What are the 6-steps in the incident response methodology?**

The 6 steps in the incident response methodology are:

Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned

**2. If an organization has no intention of prosecuting a perpetrator or attacker, does it still need an incident response team to handle forensics?**

Yes, a company still requires an incident response team to handle forensics even if it has no plans to prosecute the attacker or offender. Assessing the scope of the breach, locating weak points, and putting preventative measures in place are all made easier with the aid of forensic analysis. Furthermore, forensic evidence can be required for internal investigations, insurance claims, or regulatory compliance.

**3. Why is it a good idea to include human resources on the Incident Response Management Team?**

Human resources can offer knowledge in employee relations, communication, and personnel management during a security crisis, so it is a good idea to include HR on the crisis Response Management Team. They may help with managing any HR concerns that may arise from the event, arranging communication with impacted employees, and guaranteeing adherence to HR regulations and procedures.

**4. Why is it a good idea to include legal or general counsel in on the Incident Response Management Team?**

It is crucial to have legal or general counsel on the incident response management team in order to help with compliance issues, legal advice, and regulatory needs in the event of a security incident. Legal counsel can assist in navigating potential legal ramifications, safeguarding the organization's interests, and making sure incident response procedures adhere to relevant laws and rules.

**5. How does an incident response plan and team help reduce risks to the organization?**

An incident response team and plan facilitate a prompt and well-coordinated response to security incidents, thereby mitigating risks to the enterprise. They lessen the effect of incidents on company operations, reputation, and financial stability by facilitating the quick discovery, containment, and mitigation of threats. Furthermore, incident response activities aid in locating holes and weak points in the company's systems and procedures, enabling upgrades to strengthen security posture overall.

**6. If you are reacting to a malicious software attack such as a virus and its spreading, during which step in the incident response process are you attempting to minimize its spreading?**

In the containment phase of the incident response process, you are trying to reduce the propagation of a harmful software attack, such a virus.

**7. If you cannot cease the spreading, what should you do to protect your non-impacted mission-critical IT infrastructure assets?**

In the event that the spreading cannot be stopped, you should segment or disconnect your non-affected mission-critical IT infrastructure assets from the compromised network, put in place extra security measures, and apply patches or updates to stop the malware from spreading further.

**8. When a security incident has been declared, does a PC technician have full access and authority to seize and confiscate a vice president's laptop computer? Why or why not?**

No, during a security issue, a PC technician does not have complete access or authorization to take a vice president's laptop computer and confiscate it. To maintain chain of custody and legal admissibility of evidence, only authorized members of the Incident Response Management Team with the necessary training and authorization should manage evidence collection and confiscation.

**9. Which step in the incident response methodology should you document the steps and procedures to replicate the solution?**

During the Lessons Learned phase of the incident response methodology, the steps and procedures to duplicate the solution should be documented.

**10. Why is a port mortem review of an incident the most important step in the incident response methodology?**

The most crucial phase in the incident response process is the post-mortem review since it offers the chance to evaluate how well the response worked, pinpoint areas that could have been improved, and put corrective measures in place to stop future occurrences of the same kind. It aids in improving the organization's security posture and helping it draw lessons from previous occurrences.

**11. Why is a policy definition required for Computer Security Incident Response Team?**

To effectively respond to security incidents, a Computer Security Incident Response Team (CSIRT) needs to define policies that provide clear rules, roles, duties, and processes. It guarantees accountability, consistency, and adherence to legal obligations as well as industry best practices.

**12. What is the purpose of having well documented policies as it relates to the CSIRT function and distinguishing events versus an incident?**

Well-documented policies pertaining to the CSIRT function serve as a guide for differentiating between events and incidents, establishing incident categorization thresholds, delineating response protocols, and guaranteeing accurate documentation and reporting of security occurrences. This aids in the organization's efficient coordination and communication, consistency maintenance, and streamlining of incident response procedures.

**13. Which 4 steps in the incident handling process requires the Daubert Standard for Chain-of-Custody evidence collection?**

Custody evidence collection are:

1. Identification
2. Containment
3. Eradication
4. Recovery

**14. Why is syslog and audit trail event correlation a critical application and tool for CSIRT incident response handling?**

Because it enables the collection, analysis, and correlation of log and event data from several sources to detect and investigate security issues, syslog and audit trail event correlation is an essential application and tool for CSIRT incident response handling. In order to enable prompt response and mitigation measures, it assists in identifying patterns, abnormalities, and indicators of compromise.

**15. Why is File Integrity Monitoring alerts/alarms a critical application and tool for the CSIRT inciden response identification?**

Data Integrity Because monitoring alerts/alarms track changes to important system files, configurations, and settings in real-time, they are an essential application and tool for CSIRT incident response identification. Any unapproved or unexpected changes may be a sign of malicious activity or possible security breaches, necessitating a quick CSIRT investigation and reaction.