County of Cumberland
Cybersecurity Incident Response Plan

Published By: Cumberland County Department of Information Technology
Rev. 3_24

INCIDENT RESPONSE PLAN

PURPOSE

The purpose of the Incident Response Plan is to establish a consistent and organized approach for preparing for, identifying, reporting, and managing information security incidents that may compromise the confidentiality, integrity, availability, and privacy of the County's information and information systems.

KEY TERMS

Incident - An incident, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services

REPORTING INFORMATION SECURITY INCIDENTS

All department personnel who are provided authorized access to department information assets are responsible for promptly reporting suspected or actual security incidents.

Suspected information security incidents may be reported via the following channels:

- Immediate supervisor;
    - If the person who discovers the incident is not an Information Technology Employee, they will call the **Information Technology Hotline (856-391-3189).** Outside of normal business hours the person who discovers the incident will call our **911 dispatch center (856-455-6886).**
    - If the person receiving the call is an Information Technology Employee, the IT staff member who receives the call (or discovered the incident) will log the information received in the same format as the 911 Dispatch center in the previous step. The staff member could possibly add the following:
    - Is the equipment affected business critical?
    - What is the severity of the potential impact?
    - Name of system being targeted, along with operating system, IP address, and location.
    - IP address and any information about the origin of the attack.

- The IT staff member will immediately email & text the IT Group. In addition to the email & text to the group, the staff member will contact the Chief Information Security Officer (CISO) individually via phone call. The CISO will contact the County Administrator of an active threat and will keep them briefed during the process. Contacted members of the IT Department will discuss the situation and determine a response strategy.
    - Is the incident real or perceived?

- Is the incident still in progress?
- Does this affect any CJIS computer equipment?
- What data is threatened and how critical is it?
- What system or systems are targeted, where are they located physically and on the network?
- Is the incident inside the trusted network?
- Is the response urgent?
- Can the incident be quickly contained?
- What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

- If the person receiving the call is from our Dispatch Center, They will log the following and immediately contact the on-call person for that day:
    - The name of the caller.
    - Time of the call.
    - Contact information about the caller.
    - Location of equipment or persons involved.
    - What equipment or persons were involved?
    - Description of the incident.
    - How the incident was detected.
    - When the event was first noticed what supported the idea that the incident occurred.

The CSIO will report all incidents to the New Jersey Cybersecurity Communications and Integration Cell for de-confliction, trending, and assistance in responding to an incident.

Any attempt to interfere with, prevent, obstruct, or dissuade a user in their efforts to report a suspected security incident or violation is strictly prohibited and cause for disciplinary action, up to, and including termination. Any form of retaliation against an individual reporting or investigating a security incident or violation is also prohibited.

INCIDENT RESPONSE PLANNING

The County Chief Information Security Officer (CISO) shall be responsible for the development, maintenance and promulgation of a Cumberland County Cybersecurity Incident Response Plan. County Departments are responsible for incorporating the strategies included in the plan into their respective incident response plans

(a) The Department of Information Technology (DoIT) will use all available resources, including forensic techniques, such as reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing individuals involved to determine how the incident occurred. Members of the IT department will recommend changes to prevent the occurrence from happening again or infecting other systems.

(b) The plans shall define the roles and responsibilities of incident response team participants, the characterization of incidents, relationships to other policies and procedures, and reporting requirements;

Guidelines: Training should incorporate simulated events and tests or exercises of the County's incident response capabilities. Incident response training should be linked to the assigned roles and responsibilities of department personnel. Role-based training for the department's ISIRT team and incident identification and reporting for all department personnel should be training priorities.

INCIDENT RESPONSE TEAM

The CISO shall establish an department Information Security Incident Response Team (ISIRT) that is charged with promptly and correctly handling information security incidents that may impact the department, including its systems, networks, services, data, customers, and employees.

(a) The ISIRT should be comprised of capable members from the DoIT team, the department legal representative, the department public information office, the department human resources department, and auxiliary functions or resources, as necessary;

(b) The ISIRT will restore the affected system(s) to the uninfected state. They may do any or more of the following:

   a. Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.

   b. Make users change passwords if passwords may have been sniffed.

   c. Be sure the system(s) have been hardened by turning off or uninstalling unused services.

   d. Be sure the system is fully patched.

   e. Be sure real time virus protection and intrusion detection is running.

   f. Be sure the system is logging the correct events and to the proper level.

(c) Documentation—the following shall be documented:

   a. How the incident was discovered.

   b. The category of the incident.

   c. How the incident occurred, whether through email, firewall, etc.

   d. Where the attack came from, such as IP addresses and other related information about the attacker.

   e. What the response plan was.

   f. What was done in response?

   g. Whether the response was effective.

(d) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of individuals involved. Keep evidence as long as necessary to complete the internal and possible external investigation.

(e) Notify proper external agencies— If PII is involved is involved, notify Cowbell Cyber at 1-833-633-8666. If CJIS information was involved, the LASO officer of the respective department must be notified. If the LASO is unavailable, contact NJ State Police Information Security Unit at R038@gw.njsp.org or 609-882-2000 ext. 2701.

(f) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

INCIDENT CATEGORIZATION

To ensure a consistent approach to the reporting, response, handling, and tracking of incidents, agencies will use the following categorizations to describe the type of incident.

Category	Name	Description
Cat 0	Security Testing	This category is used during department approved vulnerability and penetration testing activities and other security exercises intended to test the network defenses or responses.
Cat 1	Unauthorized Access	An individual gains logical or physical access, without authorization to a department network, system, application, private or restricted data, or other information asset.
Cat 2	Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of department networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Cat 3	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, ransomware, or other code-based malicious entity) that infects a department operating system or application.
Cat 4	Improper Usage	A user violates the Rules of Behavior - County of Cumberland Computer Access Rules of Behavior and Acceptable Use Policy.
Cat 5	Scans, Probes, Attempted Access	Any activity that seeks to access or identify a department computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
Cat 6	Investigation	Unconfirmed incidents that are potentially malicious, or anomalous activity, deemed by the reporting entity to warrant further review.
Cat 7	Data Breach	A Data Breach is: • The compromise of the confidentiality of personally identifiable information; • The loss of data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of personally identifiable information; • Access to personally identifiable information that is for an unauthorized purpose; or • Access to personally identifiable information that is in excess of authorization.

Incidents that may include activity spanning across multiple categories will be classified according the category associated with the highest severity level.

INCIDENT SEVERITY AND PRIORITIZATION

Agencies shall classify the severity of the incidents using one of the following three (3) levels:

(a) High;

(b) Medium; or

(c) Low.

Guidelines: The severity of an information security incident determines the priority and resources necessary to handle the incident. It also determines the timing and extent of the response, the documentation and communications. Severity is a subjective measure of the incident's impact on, or threat to, the confidentiality, integrity, availability, and privacy of department information and information assets. An incident's severity level may be revised throughout the various incident response phases as dictated by information that is developed.

Agencies must consider the following factors when determining the severity of an incident:

- Threat to human safety;
- Scope of impact – number and criticality of systems, services, agencies and people affected;
- Financial impact to the County- loss of revenue, financial penalties, etc.;
- Sensitivity of the information – personally identifiable information (PII) or other sensitive information;
- Probability of propagation - likelihood that the malware or negative impact will spread, or propagate, to other systems or agencies;
- Reputational impact to the County; and
- Legal obligations and risks - notification requirements, regulatory issues, potential lawsuits, etc.

Other factors beyond those listed above may affect the severity rating of an incident.

INCIDENT TRACKING, DOCUMENTATION AND REPORTS

Guidelines: Individual security incidents may require completion of an incident report that provides a summary of the incident, its resolution, and any recommendations to help mitigate the risk of a reoccurrence. Review response and update policies—plan and take preventative steps so the intrusion can't happen again.

- Consider whether an additional policy could have prevented the intrusion.
- Consider whether a policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the policy is followed in the future.
- Was the incident response appropriate? How could it be improved?

- Was every appropriate party informed in a timely manner?
- Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
- Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
- Have changes been made to prevent a new and similar infection?
- Should any security policies be updated?
- What lessons have been learned from this experience?
- Changes will be implemented upon approval from the CIO.

REFERENCES

The requirements established in the Incident Response Plan have been derived from the following:

- NIST SP 800-53 Incident Response (IR);
- NIST CSF Protect/Information Protection Processes and Procedures (PR.IP), Detect/Anomalies and Events (DE.AE), Respond/Response Planning (RS.RP), Respond/Analysis (RS.AN), Respond/Mitigate (RS.MI), Respond/Communications (RS.CO); and
- NIST Special Publication (SP) 800-61 Revision 2, *Computer Security Incident Handling Guide*.