Incident Response and Management Policy (IT-16)

Incident Response and Management Policy (IT-16)

NIST Reference:		
SP 800 171 3.6 Family		
SP 800 53r4 IR Family		
CMMC 1.02 C016:IR.2.092	Plan Incident Response	Maps to 800-171 3.6.1
CMMC 1.02 C017:IR.2.093	Detect and Report Events	No 800-171 Mapping
CMMC 1.02 C017:IR.2.094	Detect and Report Events	No 800-171 Mapping
CMMC 1.02 C018:IR.2.096	Develop and Implement Response	No 800-171 Mapping
CMMC 1.02 C018:IR.3.098	Develop and Implement Response	Maps to 800-171 3.6.2
CMMC 1.02 C019:IR.2.097	Perform Post Incident Reviews	No 800-171 Mapping
CMMC 1.02 C020:IR.3.099	Test Incident Response	Maps to 800-171 3.6.3

16.1. Background

Cybersecurity events continue to increase and create a continuous stream of cybersecurity threats to COMPANY X (hereafter COMPANY X), its business assets, the privacy of staff, and threats to industry and national security. The COMPANY X approach is to adapt to the changing environment and be at the forefront of recognizing these cyber events and reporting and correcting situations caused by cyber events.

16.2. Purpose

This policy defines how COMPANY X responds to incidents or events impacting a system covered by this policy. An incident or event could relate to the company's computing equipment, data, or networks, or to the physical office space. It could also relate to an application. When using third-party application hosting, the third party's policies and procedures shall apply to those system aspects for which they have responsibility.

16.3. Scope

The policy applies to all COMPANY X employees and contractors working for COMPANY X.

This policy applies to all general incidents and to incidents related to Controlled Unclassified Information when supporting clients having that requirement.

The policy aligns to NIST SP 800-171 and CMMC 1.02 practices described in the Appendices document up to Level 3.

16.4. Policy

COMPANY X will create and implement incident handling procedures and train COMPANY X employees and contractors to follow the procedures.

16.5. Definitions

The following terminology/definitions are common to and used throughout this policy document.

16.5.1. Information Security Officer (ISO)

The Information Security Office (ISO), (Person/Role), can be reached at xxx-xxx-xxxx.

16.5.2. Computer Security Incident

A cybersecurity incident is an act or circumstance that deviates from the requirements of security regulations. Compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are security incident examples and include any unauthorized activity that threatens the Confidentiality, Integrity, or Availability (CIA) of an application, data or system, or physical office space protection.

16.5.3. Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that law, regulation, or government-wide policy requires having safeguarding or disseminating controls, excluding classified information. Practically, the government is to designate in each contract what data is CUI.

16.5.4. Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is any piece(s) of information that can potentially be used to identify, contact, or locate a single person. Data that provides personal information that should not be publicly available. For example, PII could be an individual's Social Security Number (SSN), name, or address in conjunction with one or more of the following: date of birth, SSN, tax identification number or equivalent, financial account number, or credit or debit card number.

16.5.5. Security Breach

A security breach is the unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the application.

16.5.6. Suspicious Event

Suspicious events are difficult to define and require users to apply common sense to identify the events. Table 1 is a list of some, but not all, suspicious events.

Table 1: Events

Events	Descriptions
Exposure, release, or destruction of CUI by any means	An incident on a system or device containing CUI
Loss or theft of a laptop or data media (USB drive, CD, or DVD)	Theft, loss, or misplacing a briefcase or pack containing COMPANY X or client papers
Finding an open or unlocked entrance door to COMPANY X office location during non-working hours	Unusual disturbance of desk area during non-working hours
Finding another client's laptop or papers at second client's site	Finding USB disk at a client site used by a former COMPANY X staff member
A virus/worm on laptop	Operation of an unauthorized program or sniffer device to capture network traffic
Attempts to 'social engineer' or otherwise convince users/administrators to provide information to unauthorized parties	Suspicious entries in the system or network logs
Unexplained modification or deletion of data	Unexplained user accounts
Denial/disruption of service or inability of one or more users to log in to an account	Unusual time of usage, such as late at night
Misuse of system resources by valid users	An indicated last time of usage of a user account does not correspond to the actual last time of usage of that user
Multiple unsuccessful login attempts	Unexplained new files or unfamiliar file names
Unexplained attempts to write to system files or changes in system files	Unexplained modifications to file lengths and/or dates, especially in system executable files
Unusual usage patterns	Compromised password information

16.6. Procedures

16.6.1. Planning

Company X must plan how an incident response is to be handled and by whom. Planning must include, at least, the following steps:

16.6.1.1. Create a draft Playbook

The Incident Response Playbook/Plan should define activities, team process workflows, and assigned team member responsibilities. The Playbook must cover the incident process from the beginning until the closure and final administrative activity of an incident.

16.6.1.2. Team Formation

The team must be identified in advance to respond efficiently. At a minimum, the team must include:

- Legal Counsel – coordinates the plan and incident response.
  Having the team members report to and through an attorney will protect your organization since the plan and results of an investigation and/or incident response together with the recommended remediation will be protected from disclosure to outsiders by attorney-client privilege and work product doctrine.
- Incident Response Manager – coordinates and directs the technical effort.
- Information Security Officer (ISO) – performs as the deputy to the Legal Counsel and handles the administrative internal coordination and notification (when necessary) to external entities (Clients, DoD, law enforcement, etc.)
- Technical Analysts – investigates the incident (internal and external).
  Identify whether IT infrastructure engineers or security analysts are needed to perform the detailed analysis to determine what happened or is happening.
- External Technical Resources – fills other gaps in your team.
  Identify external resources that may be needed and contact or pre-arrange with them to be available when needed.

16.6.1.3. Establish and Ensure that Network Time Protocol is Active

The network time protocol (NTP) enables all devices to use a common time for producing event records. The IT infrastructure team must ensure that all devices capable of using NTP are doing so.

16.6.1.4. Implement Centralized Logging and Monitoring

Incidents are likely to be undiscovered unless tools are installed to produce logs of security information and security events. Install tools that provide real-time monitoring of the network and devices to be aware of activity that needs real-time attention. Logging and monitoring must be centralized to afford analysis of potential incidents in an efficient manner.

16.6.1.5. Current Inventories

Maintain current inventories of all hardware devices and software in the IT infrastructure. Having current inventories will greatly improve the incident response team's response and outcome.

16.6.1.6. Training and Testing

Establish training requirements for the incident response team and fund and perform the training. Skills and exposure to practice are needed to effectively perform incident response. Set periodic testing events to drill the team in conducting incident response scenarios. The team's timeliness will improve in its proficiencies by actual practice.

16.6.2. Detection and Identification

When the ISO or COMPANY X management is informed of an incident, the ISO or his/her delegate will initiate action with COMPANY X infrastructure support personnel and support contractors (known as the Incident Response Team) to identify and contain the incident. Since speed is of essence, the Incident Response Team will begin immediately to act.

The IT infrastructure personnel and support contractors will use the Incident Response Playbook and perform tests and activities to:

- Identify who discovered the incident
- Determine when the incident occurred or is occurring
- Determine how it was discovered
- Determine what areas in the IT infrastructure have been impacted
- Does the incident impact overall infrastructure operations or is it limited to discrete areas?
- Discover the incident source
- Determine the exposure scope of personally identifiable information or controlled unclassified information
- Identify any required special assistance or resources to handle the infrastructure incident

During these tests and activities, the ISO will be frequently updated on the identification and containment effort status. COMPANY X management shall be notified and updated every 24 hours as the investigation continues.

Since client contracts and Federal regulations require timely notifications of incidents, the ISO and/or Legal Counsel will prepare to notify the appropriate Client or agency. (See 16.6.6.2 Notifications).

There are 24- and/or 72-hour notification rules that must be performed as the incident investigation continues.

16.6.3. Reporting the Incident

All COMPANY X employees and contractors are to notify their project manager or the ISO directly if they encounter or suspect an incident as defined in the definition section.

The notification will be immediate both by email and oral reporting. Project managers will notify the ISO upon notification by their project team member.

For non-COMPANY X Information Technology (IT) infrastructure applications, failed login attempts to any application exceeding that application's threshold shall be reported to the application owner. The application owner will determine if the incident needs escalating to the ISO.

For COMPANY X staff working at client sites, they will follow client procedures for incident notification. When there is doubt as to whom to notify at the client site, immediately notify the incident client project lead. After notifying the project lead or whomever the client procedures mandate, the COMPANY X practice lead and ISO must also be notified of the incident.

16.6.4. Containment

If the incident has exposed personally identifiable information or controlled unclassified information, an approach to quarantine and capture the source must occur. This captured source may be required to be sent to other organizations if so requested. However, different incidents will have different containment strategies that will be documented in the Incident Response Playbook. As an example of simple containment, a breach of a single endpoint like a laptop would be to disconnect that laptop from the network and quarantine it for further investigation

If it is decided to permit the cause of the incident to "continue in place," the impact on the business must be determined, and any clients or agencies notified as required.

Part of the containment process is to categorize incidents and priorities for action.

The ISO categorizes incidents based on the following:

- Incident type (e.g., data breach, destruction of data, virus, denial of service, lost laptop, opened office door, etc.)
- Severity/Criticality of the affected resources (e.g., public Web server, user workstation, PII, client or company data, CUI)
- Incident Impact and current and potential technical effect, such as root compromise or data destruction
- Intended response and by whom
- Who should be notified

The combination of the criticality of the affected resources and the current and potential technical effect of the incident determines the incident's business impact. For example, data destruction on a user workstation might cause a minor productivity loss, whereas an

application server "root" compromise might result in loss of major revenues, productivity, access to services, and reputation, and/or the release of confidential data.

16.6.5. Eradication

After putting a containment strategy in place, steps must be taken to investigate fully and eliminate the cause of the incident. Data must be collected, and a root cause analysis must occur.

COMPANY X must determine if "in-house skills" can detect and eradicate the cause or if external resources are required. If external resources are required, these resources should be acquired in a timely manner.

Sample questions to aid in the eradication are:

- How will you eradicate the vulnerability you are facing?
- What system changes (hardening, patching, other configuration activities) will need to be implemented?
- Are user accounts affected?
- What vulnerability scans/tools will you use to validate the eradication process?
- Will you implement changes at once, will you have a work-around in the short term, and will significant investment be required to implement new solutions?
- Will you need to wipe and re-image systems?
- Has the environment been hardened to reduce a potential recurrence?
- What are your preservation obligations and where should they be maintained?

16.6.6. Recovery

Recovery is the process of restoring your affected systems back to "normal" operating status. The process starts when the eradication step is complete or when quarantine removes the threat. Recovery ends when all systems are in production, client/agency notifications are complete, and all administrative activities are finished

16.6.6.1. Technical Recovery

The ISO and management must create the priority for recovery actions. Implement these actions in a step-by-step, serial manner. Do not initiate all restorations at once since this may cause unexpected results should problems in the recovery occur.

Sample questions to aid in the recovery are:

- Have systems been patched and hardened (to a standard)?
- Can the system be restored from a trusted back-up?
- How will you know that systems are clean and fully operational?

- Have the systems been tested, has data been validated, and when can systems be returned to production?
- How long will you continue to monitor the systems for abnormal behaviors?
- What abnormalities will you look for?
- What reporting obligations do you have to regulators and/or customers?
- Are you implementing monitoring to check for repeat events?
- Are the COMPANY X security controls in place after the recovery and before production is restarted?

16.6.6.2. Notifications

The 24- and 72-Hour Rule

The ISO, or his/her delegate, must submit an incident report within 24 hours of the incident, and will continue to provide status on the incident until it is resolved.

If the incident involves client Controlled Unclassified Information (CUI), a report MUST BE MADE within 72 hours to the client agency (particularly Department of Defense [DOD]) of the occurrence and the status.

General Report Not CUI

A general report shall contain the following:

- Point of contact
- The threat(s) and threat actor(s), vulnerabilities, and impacts relating to the incident
- Affected systems and locations
- System description, including hardware, operating system, and application software
- Type of information processed (public, confidential, PII)
- Incident description
- Incident resolution status
- Damage assessment, including any data loss or corruption
- The status of compliance of the affected information systems with applicable security requirements at the time of the incident
- The risk assessments conducted of the affected information systems before the date on which the incident occurred
- Organization(s) contacted
- Corrective actions taken
- Lessons learned

For non-COMPANY X IT infrastructure applications, the staff members directly involved in addressing the incident are responsible for submitting a follow-up report upon resolution.

For the COMPANY X IT infrastructure, the ISO is responsible for submitting a follow-up report upon resolution.

The incident report for both applications and IT infrastructure will be filed in the COMPANY X Secure Data Repository (Preveil, GCC High, Box Enterprise or alternative) Incident Response encrypted file storage area.

DoD Special Reporting for CUI

The following DoD special reporting procedure for CUI incidents is valid as of April 2020 and must be adhered to:

- A cyber incident report is submitted via https://dibnet.dod.mil/
- A medium assurance certificate is required and is obtained at https://public.cyber.mil/eca/.
- If COMPANY X isolates the malware software submit the malicious software to the DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer.
- Do not send the malicious software to the Contracting Officer.
- Indicate the cyber incident report number associated with this malware
- Preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of DFARS 252.204-7012 clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.
- Be prepared to supply more information if requested later by DoD.
- To the maximum extent practicable, Company X will identify and mark attributional/proprietary information.
- If assistance is needed, contract DCISE@dc3.mil
- When submitting the initial report, include as much of the following as can be obtained within the 72-hour discovery window:
    - Company Name and point of contact
    - Data Universal Numbering System (DUNS) Number
    - Contract number(s) or other type of agreement affected or potentially affected
    - Contract or other type of agreement clearance level
    - Contracting Officer or other agreement contact
    - USG Program Manager point of contact (address, position, telephone, email)
    - Facility Clearance Level (unclassified, confidential, secret, top secret, not applicable)
    - Facility Commercial and Government Entity Code (CAGE) code
    - Incident location CAGE code

- Location(s) of compromise
- Date incident discovered
- Incident/Compromise narrative
- Type of compromise (unauthorized access, unauthorized release, unknown, not applicable)
- Description of technique or method used in cyber incident
- Incident outcome (successful compromise, failed attempt, unknown)
- Impact to Covered Defense Information or Controlled Unclassified Information
- Impact on ability to provide operationally critical support
- DoD programs, platforms, or systems involved
- Any additional information relevant to incident

16.6.6.3. Administration Actions (Quarterly)

The ISO will compile and deliver a quarterly report to the COMPANY X Executive Team for all security incidents from the past quarter. The intent of this report and subsequent discussion is to 1) create incident awareness with COMPANY X management, 2) give special consideration to client-related incidents that may need additional handling, and 3) to direct the resourcing of follow-on actions that arise from the incidents.

The quarterly report will be stored on the COMPANY X SharePoint (or alternative) site.

16.7. Schedule

Task	Frequency	Responsibility
Identification of an incident as it occurs	As Needed	Individual noticing the incident
Project Lead and ISO notified immediately after awareness	As Needed	Individual noticing the incident
Initial brief logging of incident upon notification	As Needed	ISO, IT Lead
Incident Detection and Identification	As Needed	Incident Response Team
Incident containment	As Needed	Incident Response Team

Incident Categorization and Priority Setting	As Needed	ISO
Incident Eradication	As Needed	Incident Response Team, IT
Incident Recovery	As Needed	Incident Response Team, IT
Notification clients, individuals, or DoD	As Needed	ISO, General Counsel
After Action Review	As Needed	ISO
Report to CEO	As Needed	ISO
Quarterly Report to Exec Management	Quarterly	ISO
Develop and Test Plan	As Needed	ISO
Review Policy	Annually	CEO

16.8. Section Version Control

Section Number	Date	Reviewed and Approved by	Comments
1.0	May 2020	Approved:	