INCIDENT RESPONSE POLICY

Contents

Authority 3
Purpose 3
Definitions and Terms 3
Scope 4
Policy Statement 4
Incident Response Plan Requirements 5
Computer Security Incident Response Teams 6
Incident Declaration and Categorization 6
Performance Measures 7
Program Operation, Monitoring, and Improvement 7
Policy Violations 8
Roles and Responsibilities 9
Reference Documents 10
Relevant Standards 11

TEMPLATE information (DELETE BEFORE USING)

This template is provided as an example of a policy or procedure that is based on the NIST 800-171 standards. It should be used as a reference point to create your own policy. It is important to note that no policy or procedure is "one-size fits all" and this document will require modification before use.

Authority

State Administrative Manual (SAM) 5300.

NIST 800-171r2: Protecting Controlled Unclassified Information (CUI) in Non-Federal Information Systems

NIST SP.800-61r2: Computer Security Incident Handling Guide

NIST Cybersecurity Framework

Purpose

The purpose of this policy is to:

- Declare the intent of [COLLEGE] regarding incident response.
- Establish expectations for creating, maintaining, monitoring, and improving incident response capabilities.
- Assign ownership and accountability for fulfilling those expectations.

[COLLEGE] utilizes the NIST Cybersecurity Framework (CSF) to guide creation of this policy, specifically the NIST SP.800-61r2: Computer Security Incident Handling Guide. Stakeholders are responsible for following all applicable compliance standards concerning their work, including but not limited to HIPAA, PCI-DSS, FERPA, and CCPA.

This policy primarily addresses the following NIST CSF Function:

- PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

Definitions and Terms

Computer Security Incident Response Team (CSIRT): A team set up for the purpose of assisting in responding to computer security-related incidents; also called an Incident Response Team (IRT), Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

Event: Any observable occurrence in a network or system

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

For more information, refer to NIST 800-61r2 Appendix C (Glossary).

Scope

This policy applies to [COLLEGE], employees, contractors, subcontractors, vendors, consultants, advisors, and other personnel who have access to [COLLEGE] information assets without regard to data ownership.

Exceptions

No exceptions for this policy are currently in place.

[COLLEGE] reserves the right to amend, revoke or terminate this policy in part or in its entirety, as it may deem necessary from time to time in accordance with applicable law.

Policy Statement

The [COLLEGE] will develop and operate an Incident Response (IR) program to:

- Manage information security risks associated with incidents
- Detect, respond to, and limit consequences of malicious cyberattacks against information systems and data
- Establish expectations for local authorities to create incident response plans, procedures, and CSIRTs
- Establish guidelines regarding incident-related information sharing and communication
- Preserve all necessary artifacts resulting from incidents and response procedures
- Train stakeholders on their responsibilities
- Verify these requirements are being met
- Communicate, govern, operate, and improve the above activities

Incident response documents for the [COLLEGE] will be considered templates for local teams to follow. Links to those documents can be found in the Reference Documents section below.

Incident Response Plan Requirements

An Information Security Officer (ISO) shall be designated by [COLLEGE] as a functional role responsible for the oversight and management of the incident response program. The ISO is required to be at a level high enough to allow that individual to speak with authority and effectively manage incident response.

The ISO and their designees will develop, maintain, and update a written incident response plan that:

1. Identifies CSIRT members and assigns their roles and responsibilities
2. Indicates when to use the plan and when to activate the CSIRT
3. Details incident reporting, declaration, categorization, prioritization, and escalation methods, processes, and procedures
4. Identifies when, how, and under whose authority external parties are engaged
    a. Counsel must approve the extent, form, and content of all engagement with law enforcement or the public
    b. Public relations and/or human resources representatives should also guide external communications
    c. Document processes and timetables identifying when to notify affected individuals, partner organizations, and/or regulatory agencies in compliance with notification deadlines regulations
5. Maintains an Incident Response (IR) contact list that includes:
    a. CREs, LLAs, and CSIRT members
    b. Internal stakeholders such as senior executives, department managers, technical experts, counsel, and human resources
    c. Relevant government agencies
    d. Local, state, and federal law enforcement
    e. Third-party resources such as outside counsel and forensic investigators
6. Documents procedures for incident handling, including at a minimum:
    a. Detection and analysis processes and verification methods
    b. Evidence gathering and preservation
    c. Incident prioritization and documentation
    d. Containment, eradication, and recovery strategies
    e. Post-incident activities including
        i. Evaluation of lessons learned
        ii. Reporting findings
        iii. Conducting incident follow-up
        iv. Taking required technical actions.
        v. Reviewing procedures and team effectiveness.
        vi. Developing recommendations and next steps.
7. Notes how and when to account for special circumstances, such as suspected insider threats or conflicts of interest
8. Plans for annual, or more often, testing of the incident response plan

9. Documents training methods and timetables to ensure all stakeholders adequately understand their responsibilities

Computer Security Incident Response Teams

The CSIRT is authorized to oversee the incident response process and execute the incident response plan and associated procedures. The CSIRT may authorize or expedite changes to information systems and confiscate or disconnect equipment, as necessary.

During incident investigations, the CSIRT is authorized to monitor relevant resources and retrieve communications and other relevant records of specific users, including login session data and the content of individual communications without notice or further approval. The CSIRT is authorized to share external threat and incident information with third party organizations.

The Information Security Officer (ISO) will appoint members of the CSIRT. Individual CSIRTs will vary but at a minimum will include the ISO, IT staff, information security staff, legal counsel, and public relations representatives. For more information, see the Roles and Responsibilities section.

Incident Declaration and Categorization

The Information Security Officer is responsible for declaring and categorizing incidents. Every event, incident, and local team is unique. Declaration and categorization procedures will require independent judgment, but special attention should be paid to any event that affects PII, sensitive data, or critical business processes.

Incidents will be categorized into high, medium, and low severity ratings by the ISO, based on the guidelines below. It is important to note that the severity rating may change as IR procedures are implemented and more information is discovered.

High severity incidents require immediate activation of the Computer Security Incident Response Team (CSIRT) and notification of the Chancellor's Office. Remediation actions must place as soon as possible. High severity incidents include any the following:

- Impacts or threatens to impact systems critical to the ability of the college to function normally
- Poses a serious threat of financial risk or legal liability
- Exposes or threatens to expose PII or ePHI
- Threatens to propagate to or attack other networks or organizations
- Threats to human safety or property
- Elements from lower-level incidents that, when combined, represent a larger impact

Medium severity incidents require notification of the CSIRT, which may be activated at the discretion of the ISO. Remediation actions should take place within a reasonable amount of time. Medium security incidents may include the following:

- Threatens to or active impact against significant number of systems or people
    - For example, the organization can still function, but a group, department, unit, or building may be unable to perform its mission
- Poses a moderate threat of financial risk or legal liability
- Impacts a non-critical system or service

Low severity incidents do not necessarily require notification of the CSIRT. Low severity incidents have no characteristics from the "medium" or "high" categories and may include the following:

- Only a small number of people or non-critical systems are impacted
- Little to no threat of financial risk or legal liability
- Little to no risk of the incident spreading or impacting other organizations or networks

Performance Measures

Incident response programs will collect and store incident response data in a central, accessible location. This is useful for lessons learned activities, to measure success, and to inform program refinements. Local programs should detail the location for performance measurement data and storage procedures.

- Data collection will vary based on local requirements, but at a minimum should include:
    - Number of incidents
    - Time per incident
    - Objective incident assessments
    - Subjective incident assessments
    - Incident reports, including estimated service interruptions and person-hours spent
- For more information, refer to NIST 800-61r2 section 3.4.2: Using Collected Incident Data.

Program Operation, Monitoring, and Improvement

Primary responsibility for developing, maintaining, measuring, testing, and improving the Incident Response Program rests with the Information Security Officer (ISO). To fulfill those duties, the ISO will:

- Review the performance of the [COLLEGE] Incident Response Program (at least annually)

- Review operational reports and metrics associated with the Incident Response Program (at least annually)
- Host or attend an Incident Response tabletop and review results (at least annually)
- Review and update this policy (at least annually)
- Ensure that this policy is communicated as appropriate to all stakeholders (at least annually)
- Submit an annual incident response report to the Chancellor's Office

Policy Violations

Violations of this policy could result in significant technology, employee, student, reputation, and other damages to [COLLEGE].

As such, all stakeholders have a responsibility to report security incidents and breaches of this policy as quickly as possible through procedures specified in the Incident Response Plan. This obligation also extends to any external organizations contracted to support or access internal information systems or data.

Vendor noncompliance with this policy could result in the immediate termination of contracts and loss of access to related information systems and data. [COLLEGE] will take appropriate measures to remedy policy violations. If damages or compromises result from the noncompliance, legal action may be considered.

For all internal violations, noncompliance will be investigated, and appropriate disciplinary measures will be taken.

Questions

Questions regarding the information in this Policy should be directed to [COLLEGE IT or SECURITY GROUP].

Roles and Responsibilities

Team / Role	Responsibilities	Currently Assigned Staff / Dept
College Board of Directors	Review and approve all information security policies Assign authority to develop processes and procedures required to execute and enforce policies Ensure that this policy is communicated to all stakeholders	
Information Security Officer	Responsible for overall development, execution, improvement, and maintenance of local incident response program Appoint CSIRT members Lead CSIRT Activate the CSIRT as necessary Ensure that resources are assigned to respond to incidents Assign severity ratings to incidents Act as communication point to other stakeholders	
Technical Staff	Act as member of CSIRT Provide technical subject matter expertise Update procedures under the guidance of the ISO	

Team / Role	Responsibilities	Currently Assigned Staff / Dept
Legal Counsel	Act as member of CSIRT Advise on legal risks and obligations Approve the extent, form, and content of all disclosures to law enforcement and the public Serve as communication point for law enforcement Make legal determinations related to the scope and nature of investigations	
Public Relations Representative	Act as member of CSIRT Serve as communication point for third parties other than law enforcement Guide incident response communications content	
Employees, vendors contractors, subcontractors, and other stakeholders	Comply with IR policy Report all potential security incidents immediately	

Reference Documents

Document	Link
NIST Cybersecurity Framework	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
NIST SP.800-61r2: Computer Security Incident Handling Guide	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
California Joint Cyber Incident Response Guide	https://www.caloes.ca.gov/LawEnforcementSite/Documents/California-Joint%20Cyber%20Incident%20Response%20Guide.pdf

CA State Administrative Manual (SAM), Incident Response Guidance	INFORMATION SECURITY INCIDENT MANAGEMENT – 5340 INCIDENT RESPONSE TRAINING 5340.1 INCIDENT RESPONSE TESTING 5340.2 INCIDENT HANDLING 5340.3 INCIDENT REPORTING 5340.4 RISK MANAGEMENT 5305.6
CA State Information Management Manual (SIMM), Incident Response Instructions	SIMM 5340-A – Incident Reporting and Response Instructions SIMM 5340-C – Requirements to Respond to Incidents Involving a Breach of Personal Information (PDF)

Relevant Standards

Area	NIST Reference
NIST CSF	RS.RP-1, RS.CO-1:5,
NIST 800-53	RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6), PS-7