Ventura County Community College District Security Incident Handling Framework

Prepared by: Brandon Jones, Information Security Analyst, VCCCD
Version: 1.0
Date: 7/08/2022

Change Log

Status	Change	Date	Version	Approved by
Published	Reviewed processes, Added Appendix A, Cleared Draft change history, Fixed ToC and updated To-Do	July 07, 2022	1.0	Dan Watkins, Assoc. Vice Chancellor

THIS PAGE INTENTIONALLY LEFT BLANK

Ventura County Community College District Incident Handling Framework

Table of Contents

Purpose

This document broadly describes the policy for responding to information security incidents at Ventura County Community College District. It defines roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of this Computer Security Incident Response Plan is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

Mission Statement of VCCCD CSIRT

VCCCD's Computer Security Incident Response Team (CSIRT) is a group of identified individuals working at each VCCCCD campus, assigned specific roles, and chartered to respond to security incidents related to VCCCD's trust, identity and services so that they may be relied upon by VCCCD participants for mission critical and sensitive operations on an ongoing basis. To that end, the VCCCD CSIRT will:

- Receive information about cyber threats to VCCCD infrastructure
- Receive information about cyber threats to VCCCD participant systems
- Assess the risk of such threats
- Develop response and remediation plans where appropriate to address these threats
- Execute, with the possible addition of needed externa resources, incident response according to a documented incident handling framework
- Report to stakeholder communities on the nature of incidents responded to, status of response, and to communicate as needed with affected parties

Definitions

Cybersecurity Event

An exception to the normal operation of IT infrastructure, systems, or services, indicating a possible breach of information security, failure of controls, or a previously unknown system state that may be security relevant.

Cybersecurity Incident

A violation or imminent threat of violation of computer security policies, applicable laws and regulations, acceptable use policies, or standard security practices, which have a significant probability of compromising business operations.

Breach

A serious cybersecurity incident that involves the release of personally sensitive, protected and/or confidential data

Breach Notification Requirements

For the purpose of breach reporting relating to personal information, protected health information, or PCI cardholder date, at least one of the following criteria must be met:

Personally Identifiable Information (PII)

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- State-issued identification card number
- Financial account number in combination with a security code, access code or password that would permit access to the account
- Medical and/or health insurance information
- Uniquely Identifying Student Data

Protected Health Information (PHI)

PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium by a Covered Component. Covered components are (1) health plans, (2) health care clearing houses, and (3) health care providers who electronically transmit any health information in connection with transactions for which VCCCD has adopted standards. Generally, these transactions concern billing and payment for services or insurance coverage. PHI is considered individually identifiable if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age (if over 89)
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code that could identify an individual

PCI Cardholder Data

The PCI Security Standards Council (SSC) defines 'cardholder data' as the full Primary Account Number (PAN) or the full PAN along with any of the following elements:

- Cardholder name
- Expiration date
- Service code

Methodology

This plan outlines the most general tasks for Incident Response and will be supplemented by specific internal guidelines and procedures that describe the use of security tools and/or channels of communication. These internal guidelines and procedures are subject to amendment as technology changes. It is assumed that these guidelines will be documented in detail and kept up-to-date.

Constituencies

The CSIRT represents the entire District's Information System(s) and Institutional Data, supporting the Users. Some departments and schools maintain their own IT staffs and some branches of the district are located in other cities. To the extent possible, the CSIRT will attempt to coordinate its efforts with these groups and to represent the District's security posture and activities. Since the CSIRT is primarily concerned with preventing the disclosure of PII, PCI and PHI data, its responses to incidents and threats will be conditioned by the role of the Users with regard to sensitive data.

Evidence Preservation

The goal of Incident Response is to reduce and contain the scope of an incident, and ensure that IT assets are returned to service as quickly as possible. Rapid response is balanced by the requirement to collect and preserve evidence in a manner consistent with the requirements of rules 26-34 of the Federal Rules of Civil Discovery, and to abide by legal and Administrative requirements for documentation and chain of custody. CSIRT will maintain and disseminate procedures to clarify specific activities with regard to evidence preservation, and will adjust those procedures as technologies change.

Staffing for an Incident Response Capability, Resiliency

The CSIRT will endeavor to maintain sufficient staffing and third-party augmentation to investigate each incident to completion and communicate its status to other parties while it monitors the tools that detect new events. Insufficient staffing will impact rapid response capability and resiliency, as will degradation of the tools used for detection, monitoring, and response.

Training

The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested and translated into recommendations for enhancements. VCCCD will be periodically trained on procedures for reporting and handling incidents to ensure that there is a consistent and

appropriate response to incidents, and that post-incident findings are incorporated into procedural enhancements.

Initial Contact/Notification and Triage

Any party may make VCCCD's CSIRT aware of a relevant security incident or disclosure via one of the following mechanisms (available 24x7x365)

DO NOT communicate any sensitive information via these channels. VCCCD staff will set up a secure communications channel with you, if need be, after your initial request is received

1) ***Call this number: +1 805 652 5598 (PREFERRED)***
2) ***Send an email to: security@vcccd.edu***

Outside of normal business hours, it may take up to 12 hours for staff to be notified of your email. In critical emergencies, please call the number above.

Inquiries from any law enforcement agency regarding a security incident, including formal legal process such as subpoenas and warrants, must be directed to the General Counsel of VCCCD.

VCCCD's CSIRT will accept, evaluate and reply (when necessary and deemed appropriate) to valid submissions as soon as possible, but in no event later than 24 hours after receipt of the notice.

Listing of third parties which may be notified is located here (login required)

Generalized Incident Response Procedure

Upon receipt of information about a possible security threat to VCCCD, the CSIRT will:

1. Identify an incident handling lead.
2. Assign the lead to perform a brief initial assessment of the situation, including initial classification of the incident or disclosure as: "Normal," "Escalation," or "Emergency" in nature.
3. The lead will determine and execute next steps based on assessment of initial event classification, including the formation of an incident handling team as necessitated by nature, criticality and scope. Lead may call in resources for the incident handling team, and those resources are obligated to help with further analysis, remediation and other necessary incident handling steps. Normal procedures to follow are documented in the Incident Handling Actions Matrix below.
4. All relevant details of the incident including classification, handling, communication, resolution and disposal will be documented at the request of Counsel in a shared file repository within VCCCD.
5. An incident is closed when the Executive Sponsor determines that the event has been handled appropriately and is no longer an active threat. In some cases, one or more reports may be issued to relevant stakeholders.

Roles and Responsibilities

Specific make-up of each team is subject to availability and appropriateness at the discretion of the Incident Lead and CSIRT Executive Sponsor

CSIRT Executive Sponsor

Typically, the Associate Vice Chancellor, Information Technology, or delegated representative. Determines need, in conjunction with Incident Lead, for outside support and reporting.

Incident Lead

Local manager (e.g., Director of Campus IT Services or delegated representative) responsible with categorizing and managing next steps for the duration of the incident.

Incident Response Coordinator

Employee who is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation.

Incident Response Handlers

Employees who respond to outages, gather, preserve, and analyze evidence so that an incident can be brought to a conclusion. May Include System and Network administrators, IT Support Specialists, and other specialized personnel as required.

Additional members when external reporting or criminal proceedings are required

- Law enforcement Representative and Liaison
- Legal Representative
- VCCCD Communications Representative

Assessment of an Incident

This section is a set of guidelines to allow the named incident handling lead to assess the classification of an incident, for use as input in determining next steps, in the next section.

Scope

Any incidents that originate from, are directed towards, or transit VCCCD controlled computer or network resources will fall under the purview of this policy.

If an incident is not in scope, it will be documented and handed off to the appropriate party (internal to or external to VCCCD) for further assessment and handling.

Nature

Answer the question: “Is the event an Incident?” I.e.

1. Discovery of the neglect of a system or systems by a human actor responsible for maintaining that/those systems that prevents misuse or exploitation of the system(s) to harm VCCCD or its participants’ networks or as those networks or systems function in a core or role within the portfolio of VCCCD trust services.
2. Use of a system or network in any way that compromises VCCCD or its participants’ networks or systems as those networks or function in a core or supporting role within the portfolio of VCCCD trust services.
3. Any other use or misuse of computing resources, intentional or otherwise, which would cause harm to networks or systems that have a core or supporting role within the portfolio of VCCCD trust services (for more information on VCCCD services, see: status.vcccd.edu).
4. Unauthorized disclosure of a security vulnerability known to affect systems or services used in the operation of VCCCD’s infrastructure.

If an event is determined to be an “Incident” in nature, it should be further analyzed for elements of criticality in order to determine necessary actions. If the event is not an “Incident,” it should be handed off to operations for further analysis and handling.

Criticality

Incidents can be broken down into three criticality categories:

Normal

An event that does not affect critical production systems or the trustworthy flow of identity/trust-related data across VCCCD services.

Escalation

An event that affects production systems and requires change control steps be followed as part of a response.

Emergency

A change to a production system impacting one or more of the following:

- Health and safety
- Critical controls on systems which are relied upon for the trustworthy exchange of identity/trust data between VCCCD participants and which utilize VCCCD services for facilitation of this data exchange
- Ability of VCCCD or one or more of its participants to provide services or conduct business via VCCCD services
- Anything deemed an emergency by virtue of related VCCCD policies or the CSIRT Executive Sponsor

Communications

Communication of an incident is a critical step in the response plan, to be formulated in accordance with the matrix below. It is important that a communication plan be designed in a way that does not disclose information about an incident to an inappropriate audience. In many cases it is also important to let participants and other stakeholders know about an incident in a timely manner based on their need to know and need to share indicators of compromise. At a minimum, for an Escalation or Emergency-level Incident, an after-action review will be prepared at the request of Counsel. The review will include root cause analysis and remediation steps, and should be conducted by the Incident Lead, and a report should be prepared which may be shared with appropriate audiences.

A designated communication representative should be named as part of each Escalation or Emergency-level incident. This person will provide needed input to a decision-making process about what information to share with which audiences, and in particular, what information may be shared outside of VCCCD and the CSIRT, when, via what channels, and in what format. The Executive Sponsor will have ultimate authority for decision-making about the release of information, in consultation with the Incident Lead and general counsel.

Notification call sheet can be located at:

Traffic Light Protocol for Exchange of Information

For the purposes of communications between the CSIRT and external parties during the handling of an active incident (and for further information sharing with other parties after the incident), the Traffic Light Protocol [3] must be used as a way to identify, label, and ensure compliance with scoping of the information shared. The Incident Lead, Executive Sponsor and Incident Response Coordinator are primarily responsible for assigning TLP categories of information to be shared, although there are times when other members of the CSIRT and external parties will need to make an assessment about TLP categories and label information they are sharing. When there is uncertainty on the classification of a communication item, the party should verify with the Incident Response Lead. Generally, the originator of new information will need to initially label that information.

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could Lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or Conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal no foreseeable of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Reference: TLP levels matrix from US-CERT [4]

Incident Handling Actions Matrix

This matrix is intended as a generalized guide for the broad steps required in the classification and handling of information during events. The matrix below is partially derived from information available from EDUCAUSE [2].

All information known by VCCCD relating to the security incident, including, as applicable, log files and other digital evidence, will be retained by VCCCD for 7 years.

	Normal	Escalation	Emergency
Gather incident facts and prepare Initial Assessment of Situation and send to CSIRT	X	X	X
Determine whether Protected Identity Information or Protected Health Information is involved	X	X	X
In the event the incident is reportable, contact Legal representative and begin preparing all material at the request of Counsel	X	X	X
Legal Representative determine whether to notify insurance carrier	X	X	X
Contact Executive Sponsor		X	X
Convene CSIRT Members on established real-time communication channel		X	X
Deliver initial assessment to CSIRT team via secure channel	X	X	X
Re-assess Nature, Scope and Criticality in conference		X	X

If re-assessment leads to a demotion to “Normal” criticality, document and delegate further handling to non-CSIRT team(s). If re-assessment supports original or higher assessed criticality, execute further steps in the table.			
Lead determines whether external help is required, if so, request Exec to engage appropriate help		X	X
Lead determines initial remediation steps, distribute to CSIRT team via secure channel		X	X
Executive determines whether or not to involve other needed representatives or resources		X	X
CSIRT team conference and agree on remediation steps, timeline, dependencies, and *Initial* notification requirements. These decisions are documented by the Lead or designee.		X	X
CSIRT team engage relevant actors using Traffic Light Protocol, to act on remediation plan, ensuring discretion on the part of needed actors		X	X

CSIRT and action team act on plan		X	X
CSIRT team evaluate post-action situation and develop initial report to Executive		X	X
Executive conferences with CSIRT team and determines need for further measures, next steps, and reporting requirements, including complying with all applicable laws and regulations. These decisions are documented by the Lead or designee.		X	X
CSIRT team and executive act on any needed next steps and reporting requirements		X	X
CSIRT team conducts an after-action review as part of security continuous improvement process. These decisions are documented by the Lead or designee.		X	X

Incident Response Phases

The basic incident process encompasses six phases: preparation, detection, containment, investigation, remediation and recovery. These phases are defined in NIST SP 800-61 (Computer Security Incident Handling Guide). The CSIRT's overall incident response process includes detection, containment, investigation, remediation, and recovery, documented in specific procedures it maintains. This plan is the primary guide to preparation phase from a governance perspective; local guidelines and procedures will allow CSIRT to be ready to respond to any incident. Recovery includes re-evaluating whether the preparation or specific procedures used in each phase are appropriate and modifying them if inappropriate.

Preparation

Preparation includes those activities that enable the CSIRT to respond to an incident: policies, tools, procedures, effective governance and communication plans. Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post-mortem analysis from prior incidents should form the basis for continuous improvement of this stage.

Detection

Detection is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident.

Containment

Containment is the triage phase where the affected host or system is identified, isolated or otherwise mitigated, and when affected parties are notified and investigative status established. This phase includes sub-procedures for seizure and evidence handling, escalation, and communication.

Investigation

Investigation is the phase where CSIRT personnel determine the priority, scope, and root cause of the incident.

Remediation

Remediation is the post--incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been contained. The determination of whether there are regulatory requirements for reporting the incident (and to which outside parties) will be made at this stage in cooperation with general counsel. Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.

Recovery

Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of "lessons learned" into future response activities and training.

Appendix A: Response Processes

[1] Initial Response and Containment
[2] Compromised Account Workflow
[3] Phishing Process

Appendix B: Foundational Documents

[1] Sensitive Data Exposure Checklist v1.1, EDUCAUSE
[2] Traffic Light Protocol, US-CERT
[3] NIST SP800-61, Computer Security Incident Handling Guide
[4] Computer Security Incident Response Plan, Carnegie Mellon University
[5] Handbook for Computer Security Incident Response Teams(CSIRTs), West Brown, Stikvoort, Kossakowski, Killcrece, Ruefle, Zajicek.

Appendix C: Acknowledgements

Thanks to the following individuals and groups for their contributions to this document:

Kim Milford, REN-ISAC
Thomas Barton, The University of Chicago
Jane Drews, The University of Iowa
REN-ISAC
Big Ten Academic Alliance CISOs
EDUCAUSE
Internet2 and InCommon
Information Security Office, Carnegie Mellon University

Appendix D: Planned Improvements

Area of Improvement	Corrective Action
External Communication Procedures	Develop crisis communication plan in conjunction with marketing
Protected info unclear when communicating externally	Update TLP based on crisis communication plan and identified protected information.
Response processes not current	Review and update workflows based on existing security stack