

RECOVERY POLICY

| | |
|---|--|
| Policy: | Recovery |
| Policy Owner: | CIO |
| Change Management | |
| Original Implementation Date: | 3/7/2018 |
| Effective Date: | 3/7/2018 |
| Revision Date: | |
| Approved By: | Executive Staff |
| Crosswalk | |
| NIST Cyber Security Framework (CSF) | RC.RP, RC.IM, RC.CO |
| NIST SP 800-53 Security Controls | CP-2, CP-3, CP-4, CP-9, CP-10, IR-4, IR-8, PE-17 |
| NIST SP 800-171 Protecting Controlled Unclassified Information | 3.2.1, 3.2.2, 3.6.1 |
| Center for Internet Security Critical Security Control | 10 |
| Payment Card Industry Data Security Standard (PCI DSS) v3.2 | |
| Procedure Mapping | |
| | |

PURPOSE

To provide Pomona College with guidance to developing and implementing the appropriate activities, maintain plans for resilience, and to restore any capabilities or services that were impaired due to an information security event impacting the confidentiality, integrity, and/or availability of the Pomona College system and/or information.

POLICY

Pomona College maintains appropriate contingency plans that address the processes, procedures, and technical measures to enable quick and effective recovery following an information security event or a disruption. Pomona College periodically reviews, tests, and improves on its contingency operations. When enacting contingency operations, Pomona College's restoration activities are coordinated with appropriate internal and external stakeholders.

CONTINGENCY PLAN

- ❖ Pomona College provides for the recovery and reconstitution of the Pomona College system to a known state after a disruption, compromise, or failure.
- ❖ Pomona College:
 - Develops contingency plan(s) for the Pomona College system that:

- Identifies essential mission and business functions and the associated contingency requirements
- Provides recovery objectives, restoration priorities, and metrics
- Addresses contingency roles, responsibilities, assigned individuals with contact information
- Addresses eventual, full information restoration without deterioration of the security safeguards originally planned and implemented
- Is reviewed and approved by the Security Official
- Distributes copies of the contingency plan(s) to key personnel
- Coordinates contingency planning activities with incident handling activities¹
- Coordinates the development of the contingency plan(s) with the development of other related plans
- Protects the contingency plan(s) from unauthorized disclosure and modification
- ❖ Pomona College contingency plans include, but are not limited to:
 - Business Continuity Plan (BCP)²
 - Disaster Recovery Plan (DRP)³
 - Incident Response Plan⁴
- ❖ As part of the contingency plan development and maintenance process, Pomona College will conduct Business Impact Analyses (BIA) in order to:
 - Determine business process and recovery criticality
 - Identify outage impacts and estimated downtime
 - Identify resource requirements
 - Identify recovery priorities for the Pomona College system
- ❖ The Pomona College contingency plan(s) assign specific responsibilities to designated staff to facilitate the recovery and/or continuity of essential functions.
 - Resources necessary to ensure the viability of the contingency plan(s) must be acquired and maintained
 - Personnel assigned contingency plan responsibilities are trained to properly execute contingency procedures
- ❖ Pomona College personnel assigned contingency plan responsibilities are to be trained in the following elements:
 - Purpose of the contingency plan(s)
 - Cross-team coordination and communication
 - Reporting procedures
 - Security requirements
 - Team-specific processes (Activation and Notification, Recovery, Reconstitution)
 - Individual responsibilities (Activation and Notification, Recovery, Reconstitution)
- ❖ Pomona College personnel assigned contingency plan responsibilities are to be trained:
 - Within no more than 30 days of assuming a contingency role
 - When required by the Pomona College system
 - Annually thereafter

ALTERNATE WORK SITE

- ❖ As part of contingency operations Pomona College:
 - Employs moderate security controls at alternate work sites

¹ See Incident Response policy.

² The BCP focuses on sustaining Pomona College's mission and business processes during and after a disruption.

³ The DRP applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period of time.

⁴ See Incident Response policy.

- Assesses as feasible, the effectiveness of security controls at alternate work sites
- Provides a means for faculty, staff, and students to communicate with Pomona College information security personnel in case of security incidents or problems

RECOVERY IMPROVEMENTS

- ❖ Pomona College:
 - Reviews the contingency plan(s) for the Pomona College system annually
 - Post-activation, Pomona College reviews the contingency plan(s)
 - Plan reviews include, but are not limited to, the following elements:
 - Operational requirements
 - Security requirements
 - Technical procedures
 - Hardware, software, and other equipment
 - Names and contact information of team members
 - Names and contact information of vendors
 - Alternate and offsite facility requirements
 - Vital records
 - Updates the contingency plan(s) to address changes to Pomona College, the Pomona College system, or environment of operations and problems encountered during implementation, execution, or testing of the contingency plan(s)
- ❖ The Pomona College contingency plan(s) are tested annually to determine the effectiveness of the plan(s) and Pomona College's level of readiness to execute the plan(s).
- ❖ Pomona College contingency plan elements to be tested include:
 - Notification procedures
 - System recovery on an alternate platform from backup media
 - Internal and external connectivity
 - System performance using alternate equipment
 - Restoration of normal operations
- ❖ Pomona College includes exercises as a part of the contingency plan testing process. These exercises include:
 - Tabletop Exercises⁵
 - Functional Exercises⁶

RECOVERY COMMUNICATIONS

- ❖ Pomona College communicates changes to the contingency plan(s) to senior leadership.
- ❖ When applicable, Pomona College provides appropriate notification to affected users and manages public relations upon enacting contingency or related plans.
- ❖ Pomona College will make reasonable efforts to maintain and/or repair its reputation during the recovery phase after an incident or disruption.

⁵ Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation.

⁶ Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment.

- ❖ Recovery activities are communicated to appropriate internal and external stakeholders, senior leadership, and management teams.