OFFICE OF INFORMATION TECHNOLOGY
PHYSICAL AND FACILITY SECURITY

I. PURPOSE AND SCOPE

This rule supplements the college's information security policy requirements and establish requirements for secure operations.

II. REFERENCES

A. Data Classification Roles Guide

B. Data Classification Guide

III. PROCEDURES

A. Physical Security Perimeters

1. Security perimeter zones will be clearly defined, and the controls applied to each zone should be commensurate with the security requirements of the Information Systems contained within.

2. The security perimeters of a building must be physically sound and include the following protections:

    a. the external walls must be of solid construction;

    b. the external doors must be protected against unauthorized access with appropriate control mechanisms including locks and/or alarms;

    c. doors and windows must be locked when unattended;

    d. only authorized personnel may access security zones and buildings;

    e. where appropriate and feasible, offices must use staffed reception areas to control building access; and

    f. fire doors on a security perimeter must be alarmed and monitored.

B. Physical Entry Controls

1. OIT must provide visitor logs to record the following visitor activities when deemed necessary:

    a. visitor name;

b. date and time of entry;

c. visitor's organization;

d. the employee accountable for visitors;

e. purpose of visit; and

f. time of departure.

2. All college employees, contractors, vendors, and visitors are encouraged to wear a form of visible identification.

3. Access to security zones storing or processing Critical, Restricted or college internal data, such as access cards or control code panels, will have additional controls to authenticate and validate authorized personnel.

    a. OIT logs and monitors all authorized access.

    b. OIT reviews authorized access and regularly reviews, updates, and revokes as appropriate.

    c. Unauthorized photographic, video, audio or other recording equipment are not allowed.

4. Data centers, data closets, and other points of access to data equipment should not have doors propped open and left unattended.

C. Protecting Against Natural and Facility Threats

1. Storage of hazardous or combustible materials must be maintained at a safe distance from secure areas.

2. Fire-fighting equipment appropriate to the area must be provided and suitably placed.

3. Back-up utilities, equipment and media must be maintained at a safe distance from secure areas to avoid damage from a disaster.

D. Information System Location and Protection

1. OIT or Facilities will assign equipment location to minimize unnecessary access into work areas.

2. OIT will position equipment storing or processing Critical, Restricted or College Internal data to minimize the line-of-sight viewing angle of unauthorized personnel.

3. OIT or Facilities will isolate equipment that requires special and/or elevated protection.

4. OIT or Facilities will adopt controls to monitor and minimize the risk of the following physical threats as appropriate:

    a. theft;

    b. fire and smoke;

    c. water and humidity;

    d. temperature fluctuations;

    e. vibration; and

    f. electrical supply or other electrical interference.

5. OIT and Facilities will ensure that the following supporting utilities are adequate for the information systems they are supporting:

    a. electricity;

    b. water supply;

    c. HVAC;

    d. back-up UPS;

6. OIT ensures only college information systems are plugged in to power outlets and/or network and communications ports in college data centers or other data access equipment.

E. Cabling Security

1. OIT will ensure:

    a. power and telecommunication lines into the college's facilities are placed underground;

    b. network cabling are protected using utilizing conduit or avoiding routing network cabling through public areas;

    c. power cables are segregated from network cabling to prevent interference;

    d. all cables are labeled; and

    e. open switchports are not utilized without OIT authorization.

F. Information System Maintenance

1. The college entity responsible for a computer asset or computer resource must:

    a. maintain equipment in accordance with the manufacturer's specifications;

    b. confirm that maintenance personnel are authorized to conduct repairs and servicing of identified equipment;

    c. require authorized maintenance personnel to fill out an entry and exit log for the facility when on-site repairs are conducted; and

    d. keep records and/or logs of equipment faults and the resulting preventative and corrective maintenance.

IV. GUIDELINES, FORMS AND OTHER RELATED RESOURCES

A. Reserved.