PURPOSE

The purpose of this regulation is to outline the procedure to be followed when managing and responding to information security incidents.

APPLICABILITY

This regulation applies to all employees and "users", as defined in CR (REGULATION) EXHIBIT, as anyone who utilizes and/or has access to the College District's technology resources.

DEFINITIONS

"Information security incident," (also referred to herein as "security incident"), for the purposes of this regulation, is defined as an event which results in accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of technology resources. Information security breaches are a common type of information security incidents.

These and other terms used herein are defined in the Glossary of Terms. [See CR (REGULATION) EXHIBIT]

SECURITY INCIDENT REPORTING

Information owners, data custodians, or College District employees who know of, reasonably believe that, or are uncertain whether a breach of confidential information or another security incident has occurred shall immediately report the relevant information to their supervisors or to the Executive Director of Cyber Security and Networks.

SECURITY INCIDENT COMMUNICATION

Any external communication and/or inquiries regarding a security incident shall be routed through the Office of Communications. Authorized College District personnel only are permitted to speak on behalf of the College District regarding security incidents.

SECURITY INCIDENT INVESTIGATION

Upon receipt of information regarding a potential security incident, the OIT shall conduct an investigation to confirm whether a security incident occurred, assess the risks involved, and determine a mitigation strategy.

The Investigation shall identify the type of security incident and the level of severity. The criteria that largely determine the level of severity of a security incident are as follows:

HIGH - Technology resources that:

(A) Contain confidential or other data such that unauthorized disclosure would cause real damage to the parties involved, or

(B) Impact a large number of people or interconnected systems.

MEDIUM - Technology resources that:

(A) Contain data items that could potentially embarrass or create problems for the parties involved if released, or
(B) Impact a moderate proportion of the customer base.

LOW - Information resources that:
(A) Contain published, generally available public information, or
(B) Result in a relatively small impact on the population.

Based on the information collected, an incident response team will:

- Mitigate the risk by isolating the compromised devices or systems;
- Determine if the information resources can be restored to service;
- Conduct a post security incident review to determine if additional risk mitigation controls need to be implemented; and
- Meet with the information owner and data custodian to present new controls that should be implemented.

The information owner or designee is responsible for ensuring that the new risk mitigation measures are implemented and monitored.

Based on risk management considerations and business functions, the information owner may determine that it would be appropriate to exclude certain risk mitigation measures. All exclusions must be approved by OIT.

SECURITY INCIDENT NOTIFICATION

Upon confirmation that a security incident involving confidential data has occurred, OIT shall notify appropriate College District personnel to provide notifications in accordance with applicable laws, methods, and timelines.

The incident notification, which will include a brief description of the security incident, a contact for inquiries, and helpful references for individuals regarding identity theft and fraud, shall be delivered using one of the following methods:

1. Written notice;
2. Electronic mail, if the College District has electronic mail addresses for the affected persons;
3. Conspicuous posting on the College District's Web site; or
4. Publication through broadcast media.

Notification may be delayed if College District officials/law en-

	forcement determine that a notification, notice, or posting will impede a criminal investigation. Notification shall be made as soon as the relevant law enforcement agency determines that the notification will not compromise any criminal investigation.
RECORD RETENTION	Records related to security incidents records shall be maintained in accordance with the College District's record management program. [See CIA]
OFFICE OF RESPONSIBILITY	Office of Information Technology