Union County School Board

Incident Response Plan

The purpose of this Plan is to establish a rapid response to data security incidents, to improve incident reporting and related communications, to mitigate any potential damages caused by incidents, and to improve overall data security systems.

The Union County School District (UCSB) will maintain guidelines and procedures to provide the basis for appropriate responses to incidents that threaten the security, confidentiality, integrity, and/or availability of information assets, information systems, and/or the networks that deliver the information. A Critical Incident Response Team will be maintained to manage security incidents. Data security guidelines and procedures will be reviewed routinely and updated as necessary.

GUIDELINES AND DEFINITIONS

This procedure applies to all information systems and services of UCSB.
An incident is any event that threatens the security, confidentiality, integrity, or availability of UCSB information assets, information systems, and/or the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident. Incidents may include:

- Unauthorized entry
- Security breach
- Unauthorized scan or probe
- Denial of service
- Malicious code or virus
- Other violations of the District’s Computer and Network policies
- Networking system failure (widespread)
- Application or database failure (widespread)
- Others as defined by critical incident response teams

For the purpose of this procedure, Security Breach is used as defined in Florida Statute 817.5681(4):

"[B]reach" and "breach of the security of the system" mean unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person. Good faith acquisition of personal information by an employee or agent of the person is not a breach or breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

For the purpose of this procedure, Personal Information is used as defined in Florida Statute 817.5681(5):

"[P]Personal information" means an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:

(a) Social security number.
(b) Driver's license number or Florida Identification Card number.
(c) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

For purposes of this section, the term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

Critical Incident Response Team (CIRT) membership will include:

Director of Personnel - Chair
• Technology Coordinator
• Finance Director
• MIS Coordinator
• Food Services Specialist
• Network Specialist

Participation by individual members and other employees will vary by incident as appropriate. Members of the critical incident response team are expected to respond immediately and fully when called upon. Responding to a critical incident, in general, takes precedence over all other work. If a member is unavailable at the time the team is assembled, a substitute member may be named by the chair or a majority of the members of the CIRT who are available or the Superintendent or designee.

An incident is deemed critical when so declared by the Superintendent, Director of Personnel, Technology Coordinator or MIs Coordinator.

Procedures

1. Upon discovery or suspicion of an incident, UCSB employees shall notify the Director of Personnel in a prompt and effective manner through direct contact or telephone call to 386-496-2045 ext. 229.

2. Within four business hours of receipt of notification or suspicion of an incident, the Director of Personnel (or designee in the case of absence) will consult with the Superintendent/designee; remove the risk, if possible; and begin an investigation of the incident, including notification to the critical incident response team. The Director of Personnel will keep a log of all activity related to the investigation.

3. Within three business days of receipt of notification, the critical incident response team will formulate a recommendation of whether the incident is critical or non-critical. Factors to be considered in this recommendation include, but are not limited to, whether data was inappropriately accessed, the nature and type of data accessed, and the extent of the data accessed. The CIRT will advise the Superintendent of the recommendation.

4. If the incident is determined to be non-critical, public notice of the incident is not required, but an

appropriate response will be determined by the Director of Personnel in conjunction with the critical incident response team; the response may include a change in procedure or practice, required training, targeted communications or further inquiry. The Director of PERSONNEL will submit to the Superintendent a brief description of the incident and the rationale for determining it to be non-critical. The procedures for a non-critical incident end at this step.

5. If the incident is determined to be critical, the critical incident response team will follow all the below procedures. The team will review the incident, create an overall action plan and formulate an appropriate district or system response; this response may include but is not limited to:

• Selecting which CIRT members should respond;
• Assuming control of and containing the incident; involving appropriate personnel, as conditions require;
• conducting a thorough investigation of the incident, including establishing controls for the proper collection and handling of evidence, and keeping a log of all communications and actions related to the incident;
• protecting the rights of students, employees and others as established by law, regulations, and policies;
• determining whether or not to involve outside personnel, such as legal advice, law enforcement or computer forensic experts;
• drafting statements and materials for public notice as required by State law, including posting an incident report on the UCSB website (www.union.k12.fl.us);
• executing a remediation plan, possibly including repairing/rebuilding any damaged systems and considering any additional remedies for affected constituents;
• recommending any change in procedure or practice, required training, targeted communications or further inquiry;
• monitoring and revising the action plan as needed in the period directly following the incident;
• discussing, reviewing and documenting all actions and results, and particularly any lessons learned from the security breach.

6. Within four business days of receipt of notification, unless authorized for extended review by the Superintendent or designee, the critical incident response team will confirm with the Superintendent a preliminary course of action.

7. In accordance with Florida state law, the critical incident response team will send a Notification Letter to affected constituents without unreasonable delay. The Notification may be provided by one of the following methods:
• Direct notice to the constituent's residence,
• Telephonic notice directly with the constituent and not through a prerecorded message, or
• Electronic notice if address or phone information is not available; electronic notice cannot request personal information and must conspicuously warn constituents not to provide personal information in response to electronic communications regarding security breaches.

8. The critical incident response team will conduct a post-incident critique and submit a summary report to the Superintendent including:

• A description of the incident
• A summary of lessons learned
• Any suggested changes to existing policies or procedures
• Any recommendations to protect against future incidents
9. Any disciplinary action considered in association with a critical incident shall follow procedures set forth in the appropriate UCSB Board Rules and the District Student Code of Conduct Handbook.

If determined appropriate and necessary, the notification methods may include the following:

1. A Press Release will contain the following information:

a. What are you doing?
• Announcing a breach? A theft?
• Announcing that the case has been resolved? That notification has occurred?
b. Who is affected/not affected? What specific types of personal information are involved?
c. What are the (brief) details of the incident?
d. No evidence to indicate data has been misused or what the evidence points to.
e. Expression of regret and concrete steps the institution is taking to prevent this from happening again.
f. Major (re)actions taken.
g. Contact information for the District spokesperson for the incident.

2. A Notification Letter will contain the following components:

• What happened?
• When did the breach occur and/or when was it detected?
• How was it detected?
• What data was potentially compromised?
• How much data was compromised?
• For whom was data compromised?
• Why you are being notified?
• What steps are/were being taken?
• Is any data known to be fraudulently used or is notification precautionary?
• What steps should individuals take?
• Apology or statement of commitment to security.
• Anticipated next steps, if any.
• Who to contact for additional information.
• Signature

3. An Incident Specific Web Site will contain the following components:
• Most-Recent-Update section at top of page
• Basic facts (similar to what might appear in a notification letter):
Who was impacted?
What data may have been involved?
When compromise or discovery occurred?

Where compromise occurred?
Whether anyone believed to be negatively affected or not?

Actions taken by the District to ensure more secure in Future/Ongoing measures
What should I do to be sure I'm unaffected?
Link to Identity Theft website/credit agencies
FAQs
Press Releases

References:

• Vermont State Colleges - Data Security Incident Response Procedure, October 5, 2006
• PASCO-HERNANDO Community College – Information Security Incident Response Plan, May 18, 2009
• The College of St. Scholastica - Information Technologies Incident Response Plan, July 17, 2007
EDUCAUSE – Data Incident Notification Templates