Prairie State College

Adoption Date: 11/17/2009

Revision Date: xx/xx/xx

Incident Response Plan

PURPOSE

This policy is designed to provide a rapid response to data security incidents, to improve incident reporting and related communications, to mitigate any damages caused by incidents, and to improve overall data security systems.

POLICY

Prairie State College 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 policy applies to all the information assets, information systems, and/or the networks that deliver the information at and/or owned by Prairie State College, regardless of location.

An ***incident*** is any event that threatens the security, confidentiality, integrity, and/or availability of the 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 College's Information Security Policy
- Networking system failure (widespread)
- Application or database failure (widespread)
- Others as defined by critical incident response teams

Incidents such as those listed above vary in their impact on the College community and in the degree of risk and vulnerability they pose.

A ***security breach*** is the unauthorized acquisition or access of data that compromises the security, confidentiality or integrity of personal information.

For the purpose of this policy, ***confidential information*** is an individual's first name or first initial and last name in combination with any one or more of the following: social security number, driver's license or ID number, bank or credit card account numbers or access codes. Personal information does not mean publicly available information that is lawfully made available to the general public from federal, state or local records.

Critical Incidents are defined as high impact and high risk; these include the known or suspected compromise of personal information or institutional proprietary information to entities outside the College or to entities inside the College for non-legitimate purposes. Critical incidents require the development and implementation of a formal incident response action plan by the critical incident response team.

Non-Critical Incidents are defined as low impact or low risk; these may include good faith but unauthorized acquisition or access of personal information by an employee for a legitimate business purpose, viruses, worms, compromised machines or other non-critical or minor issues. Non-critical incidents do not require a formal incident response action plan but must have an appropriate response, as determined by the Executive Director of Information Technology Resources (ITR) for system incidents or the College President/ designee for college incidents.

This table outlines response to the most frequent security incidents:

	Internal Communication (i.e. e-mail alert)	**Critical Incident Response Team**	**Press Release**	**Notification Letters**	**Incident Specific Web Site**
Data breach	X	X	X	X	X
Network breach	X	X			
Server emergency	X				
Network emergency	X				
Internet emergency	X				

Critical Incident Response Team (CIRT) membership will include:

- Chief Financial Officer (CFO)
- Executive Director, ITR
- Executive Director, Communications and Marketing
- Associate Director, ITR Administrative Computer Services
- Manager, ITR Operations & Client Support

- Director, Campus and Public Safety
- College Legal Counsel (if needed)

Participation by individual members may 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 executive leadership.

An incident is declared to be critical in one of the following ways:

- the College President, CFO, or VP Academic Affairs or designee, declares an incident to be critical.
- the Executive Director of ITR, in consultation with the CFO or VPAA or designee, declares an incident to be critical.

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. For more information, …

A ***Notification Letter*** will contain the following components:

a. What happened?
b. When did the breach occur and/or when was it detected?
c. How was it detected?
d. What data was potentially compromised?
e. How much data was compromised?
f. For whom was data compromised?
g. Why you are being notified.
h. What steps are/were being taken?
i. Is any data known to be fraudulently used or is notification precautionary?
j. What steps should individuals take?
k. Apology or statement of commitment to security
l. Anticipated next steps, if any.
m. Who to contact for additional information
n. Signature

An ***Incident Specific Web Site*** will contain the following components:

a. Most-Recent-Update section at top of page
b. 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
c. Actions taken by the unit/College to ensure more security in future/ongoing measures
d. What should I do to be sure I'm unaffected?
e. Link to Identity Theft website/credit agencies
f. FAQs
g. Press Releases
h. Toll-free Hotline contact information

For sample communications templates, see: https://wiki.internet2.edu/confluence/display/itsg2/Data+Incident+Notification+Toolkit

Procedures

1. Upon discovery or suspicion of an incident, College employees shall notify the ITR Department in a prompt and effective manner through a submission to the Help Desk, ext. 7999 or through a phone call directly to the ITR Executive Director, ext. 3579. After hours, contact the College Campus and Public Safety Office at ext. 3756.
2. Within four business hours of receipt of notification or suspicion of an incident, the ITR Executive Director (or her/ his designee in the case of absence) will consult with the President/designee; remove the risk, if possible; and begin an investigation of the incident, including notification to the critical incident response team. The ITR Executive Director 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, in consultation with the ITR Executive Director will determine whether the incident is critical or non-critical.
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 ITR Executive Director in conjunction with the critical incident response team; the response may include a change in policy or practice, required training, targeted communications or further inquiry. The ITR Executive Director or designee will submit to the President's Staff 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 remaining procedures. The team will review the incident, create an overall action plan and formulate an appropriate college 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 College website;
    - executing a remediation plan, possibly including repairing/ rebuilding any damaged systems and considering any additional remedies for affected constituents;
    - recommending any change in policy 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 President or designee, the critical incident response team will confirm with President's Staff a preliminary course of action. The Chair of the Board of Trustees will be notified of the incident and action plan.
7. In accordance with 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 President's Staff 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 College personnel policies, student handbook or employee collective bargaining agreement.

References:

- EDUCAUSE – Data Incident Notification Templates, **https://wiki.internet2.edu/confluence/display/itsg2/Data+Incident+Notification+Toolkit**