System-wide Incident Response Procedure to Data Breaches [1]

Date of last review: 09/30/2016

Purpose:

Any information security incident leads to a loss for the University, whether that is in the form of data, reputation, trust (employees, students, peers and public), finances in dollars or the indirect cost of valuable time. Some incidents may also pose significant risk to University services, resources, funding, and external relationships. Any incident, no matter how trivial it may seem initially, has the potential to cause harm to the University until thorough investigation proves the significance of impact. The level of impact from the incidents could vary; some incidents may represent minimal risk while others such as severe data breaches place people at risk of identity theft, financial loss, or other harmful consequences.

Clear and well-defined processes have proven to be very effective in minimizing the impact from security incidents. The primary purpose of this document is to define the communication and response channels in case of a data breach, and present a single, consistent and common message to the "outside world" by the University. An important objective of this document is to ensure that in the event of a data breach, resources are made available, regulatory requirements are met, and legal reporting requirements are fulfilled.

Definitions:

Information Security Incident: An Information Security Incident is any event that harms, or represents a serious threat to, the whole or part of University of Colorado (CU) information resources such that there is potential loss of data, absence of service or inhibition of functioning systems, including but not limited to:

- Theft
- Intrusion
- Misuse of data
- Computer and electronic communication-based violations
- Unauthorized changes to hardware, firmware, software and/or data
- Unauthorized exposure, change or deletion of (information assets) University Records
- Activities contrary to CU acceptable use policies

Highly Confidential information — Personal information about an individual for which the individual can reasonably expect will not be made available to the public. This type of information includes personally identifiable information (a category of personal information regulated by federal law), as well as other non-public personal information that would
adversely impact an individual if inappropriately used or disclosed. Examples of Highly Confidential information include Social Security numbers, Bank account information, Date of Birth, Protected Health Information, and educational records. In addition, the mishandling of Highly Confidential information may impact the University through financial and legal sanctions, loss of public confidence, and damage to University reputation.

**Reportable Incident:** An information security data breach incident involving any data, which falls under the category of “Highly confidential” type information as defined in this document is a reportable incident. For CU Covered Entities as defined under HIPAA, breach of protected health information owned by that entity will be reported in accordance with this procedure if it meets the criteria for media notification in accordance with the Omnibus Rule, breach notification regulations, issued on February 25th, 2013.

**Roles and Responsibilities:**

**Office of Information Security (OIS):** OIS is responsible for developing and maintaining the System-wide incident response process to data breaches. At least one and no more than two members of the OIS will be a part of the permanent members of the System-wide Data Breach Analysis Team (SDBAT). OIS will act as a central and the first point of contact in the event of data breaches. OIS will take the lead in coordinating the efforts of the SDBAT. After consulting with SDBAT and the affected campus designee, OIS may communicate with the President’s office, Colorado Department of Higher Education (CDHE) and the Board of Regents if and when necessary. OIS has the primary responsibility of submitting a final incident report, if necessary, to CDHE. OIS will also keep the Internal Audit informed of the SDBAT response activities.

**System University Relations (UR):** At least one and no more than two individuals from the System UR will form a part of permanent members of the SDBAT. System UR is the only entity allowed to talk to the media after consultations with the SDBAT and campus entities. System UR will communicate with the President’s office and the Board of Regents about the incident after consulting with SDBAT and the affected campus designee. System UR has the primary responsibility of submitting a final incident report, if necessary to the President and the Board of Regents.

**System Legal Counsel:** At least one and no more than two individuals from the System legal counsel will form a part of the permanent members of the SDBAT. Legal counsel is an initial required contact to provide advice during the investigation and advice as to the extent and timing disclosure as required by law, (e.g. HIPAA, state law, etc.).

**University Risk Management (URM):** At least one and no more than two individuals from University Risk Management will form a part of the permanent members of the SDBAT. URM should be included in initial conversations to assist in the determination whether to invoke cyber liability insurance.

**System-wide Data Breach Analysis Team (SDBAT):** SDBAT will consist of permanent and temporary members. Permanent members will consist of individuals from the following departments:

- OIS
- System UR
- System Legal counsel
- URM
- Appropriate campus ISO including the System ISO

The composition of the temporary members will depend on the type of incident (PCI, HIPAA, etc.) and the affected campus. The data owner(s) for the relevant business domains are to be included. Potential attendees may be from Internal Audit, Registrar’s office, Treasurer’s office (PCI compliance officer), UR, Legal, Human Resources, Office of Regulatory Compliance, etc. System Legal Counsel will be the approver of the SDBAT decisions.

SDBAT will assess the scope and the ramifications of the incident before deciding on the future course of action. SDBAT will also review the drafted incident alert document and any draft notification letters. SDBAT will provide inputs to the language and System Legal Counsel will approve the final documents, after which, they will be appropriately communicated to the necessary entities and individuals. There should be no communication with any external entity including the media until an approval is obtained from SDBAT.

**Designated Campus entity:** The designated campus entity will be the campus Information Security Officer. The designated campus entity will be a part of the SDBAT as a permanent member. This individual will be responsible for communicating the data breach incident to the OIS per the guidelines of this document. The following will be required for the First Information Report (FIR) submitted to the OIS:

- Brief summary of the incident:
  - a. Date and time detected
  - b. Campus, physical location, system and university services involved
  - c. Department responsible for the system/service
  - d. Type and scope of data compromised
  - e. Brief overview of the weakness exploited

- Potential impact to individuals, campus operations/resources, etc.
- Current status of response activities

If it is determined that an information security incident requires the President, Board, CDHE, media or affected individuals to be notified, the designee will work with the appropriate campus department (e.g., legal counsel, communications director, etc.) to draft an incident alert and forward it to SDBAT for review and edit.

**Process:**

The following is the System-wide Incident Response to data breach process:

- Potential “Reportable Incident” occurs
- The campus ISO determines if the incident is indeed a “Reportable Incident”. If so, the incident is “declared” and the campus provides initial response to the incident according to the Campus Incident Response Plan
Incident reported to the OIS by the campus ISO within 72 hours of the declaration or by an external entity (anyone other than the campus SP) including students, media or other institutions. If the incident is reported by an external entity (other than the campus designee), OIS will contact the campus ISO and the process starts from “Potential Reportable Incident occurs” step as above.

- “First Information Report” (FIR) document submitted to OIS
- The campus ISO and/or CISO convene the SDBAT meeting with the FIR as the leading document.
- For a quorum to be established for the SDBAT meeting, at least one member from the OIS, System UR, Legal counsel and the affected campus ISO must be present. Additionally, in case of a payment card data breach, a PCI compliance representative from the Treasurer’s office must be present. The appropriate data owner(s) of affected data should also be included in this meeting.
- If necessary, OIS will provide an initial update to the Vice President, Employee Information Systems, and the Campus ISO or IT Resource oversight authority will provide an initial update to the Campus leadership.
  - The OIS team is responsible for updating System leadership for campus incidents.
- SDBAT works closely with the affected campus to gather more information and understand the concerns.
- At the end of 30 days, if necessary, OIS will provide additional details to the Vice President, Employee Information Systems. Campus ISO or Chief Information Officer/Chief Technology Officer will provide an update to the Campus leadership.
- If it is determined that an information security incident requires the President, Board of Regents, CDHE, media or affected individuals to be notified, OIS will work with the appropriate campus department (e.g., attorney, communications director, etc.) to draft an incident alert and forward it to SDBAT for review and edit.
- If the incident so requires, the individual departments represented on the SDBAT will start contacting the external entities. E.g. Treasurer’s office contacting the financial institutions in case of a payment card information breach.
- After assessing the additional information from the campus, the SDBAT will determine if a notification needs to be sent to the individuals affected and if a press release is required. OIS will work with the appropriate campus/business unit to draft the notification letters.
- In case of press releases, notifications are reviewed by System UR and approved by the campus. System UR will inform the BOR before releasing them.
- System UR will work with the campuses to send out notifications and inform the media if necessary.
- When necessary, OIS will submit a report to the CDHE.
- Law enforcement agencies will be involved and updated if deemed pertinent to the incident and investigation.

The campus will prepare and submit a detailed incident report to the OIS including but not limited to the cause, remediation and future controls.

**Reporting Actions and Responsibilities:**
Testing the System-wide Incident Response Plan to data breaches:

Any plan, no matter how well thought-out or efficiently written can be successful if not appropriately tested. In the case of data breaches, chances of there being anxious moments and stressful situations are very high. In such a scenario, it is critical that a response plan is executed smoothly and all the involved members know exactly what has to be done and when. A good testing mechanism ensures that when an incident occurs, there will be a consistent, coherent and effective response. Tests also offer a great opportunity to observe and rectify any overlooked flaws or ambiguities in a plan.

To ensure that the University of Colorado System-wide Incident Response to data breaches is swift and smooth, the following testing steps will be taken:

- The Incident Response plan shall be regularly tested and a test summary shall be provided to the Security Advisory Committee (SAC).
- OIS will have as an objective, testing and reviewing the plan annually. However, should it not be feasible, notice shall be provided to the SAC.
• Campuses and the SDBAT will be tested through a “real life” incident, which essentially will be a mock real life scenario.

• The first time that the plan is tested, the date, time, type of the incident and the campus will be known in advance. All the relevant parties shall be informed of the same. Such a plan shall be referred to as a “Planned test”

• If a campus faces an actual incident and the System-wide Incident response plan is followed, then that incident would count as a surprise test for the campus.

• The following planned tests will occur outside of the regular testing cycle:
  - When a new campus Information Security Officer (ISO) is appointed by a campus, or
  - When a department comprising the permanent members of the SDBAT (e.g., Legal, OIS) replace more than one representative.

• After every test, the members of the SDBAT shall assess the effectiveness of the plan and recommend changes to the SAC, if necessary.

• The Office of Information Security will be responsible for initiating the test, documenting its results, and making changes to the Incident Response Plan.

**Testing Mechanism:**

Both the surprise and planned tests will follow a structured walk-through mechanism. This approach will present a fictional scenario to the campus, after which the campus ISO will follow the System wide Incident Response procedure. The SDBAT will be convened and the members will go through the elements of the response plans verbally. There will be a strong effort made to respond to the fictional incident with the intensity of responding to an actual incident. There won’t be any formal reporting of these tests to the President’s Chief of Staff, Board of Regents or the Colorado Department of Higher Education, rather these tests will serve as learning tools to ensure that the plan is effective at all times and all the members are adequately trained.

**Groups audience:**
Office of Information Security

**Source URL:** https://www.cu.edu/ois/system-wide-incident-response-procedure-data-breaches

**Links**