Privacy and Security Incident Response Plan - Banner

Scope:

Any incidents that originate from or are directed towards, or transit University controlled computer or network resources associated with Banner fall under the purview of this Incident Response Plan.

Definitions:

Incident: An event that has actual or potential adverse effects on computer or network resources such as misuse or abuse; compromise of information; or loss or damage of property or information.

Incident types include, but are not limited to, deliberate or incidental unauthorized access, disclosure or modification of University data, denial of service attacks, port scans, system break-ins, email abuse, copyright infringement, and violations of the campus acceptable use policy.

The "Data Classification and Protection Level" tables below will guide what University data is classified as private or secure data.

A violation of any Data Class above **Protection Level 0 (General)** is a reportable incident.

Examples include unauthorized disclosure or modification of:

- FERPA Student Data
    - student transcripts (grades)
    - Test scores
    - Evaluations
    - Financial aid records
    - Loan collection records
- Personally Identifiable Information (PII)

  First name, or first initial, and last name in combination with one or more of:

    - Social Security Number
    - Driver's license number
    - California identification number

Incident Response Team (IRT): The IRT is an ad hoc group of technical and functional specialists. The actual team consists of a core team of technical specialists who are assisted by functional specialists, depending on the nature of a particular incident under investigation.

Reporting New Incident

Any Banner community member or anyone affected by a campus computing security incident should report the suspected incident by email (abuse@ucdavis.edu) per policy:

UCD Security Incident Response Plan

Security Incident reports received by the Banner Help Desk will also be reported by email (abuse@ucdavis.edu).

In addition the Banner Program Directory and Banner Security Office will also be notified:

Banner Security Officer
Vijay Mudumbe
vrmudumbe@ucdavis.edu
Office # (530) 754-5564

SIS (Banner) Program Director
Tim Olesen
tlolesen@udavis.edu
Office # (530) 754-5196 Cell # (530) 979-7022

The following information should be provided by individuals reporting incidents:

- Contact information
- Brief description of the incident
- Log information including date, time
- Address of the source of the attack
- Target network information, if available

The IRT will acknowledge receipt of the reported incident. All user reports will be analyzed and prioritized in order to generate an appropriate response plan. The scope of the IRT response will be determined by the incident priority rating, or as directed by senior campus administrators.

Report Exceptions
Incidents meeting certain criteria with regard to confidential or personal information, criminal activity or misuse will be handled in the manner prescribed below:

Confidential subject matter -Incidents involving restricted data will be directly reported to the IT Security Coordinator or Vice Provost, Information and Educational Technology.
Restricted data is defined in BFB-IS3, Electronic Information Security (http://www.ucop.edu/ucophome/policies/bfb/is3.pdf). Incidents involving restricted personal information (personal name in combination with Social Security number, driver license number and/or

financial account information) must follow the process described in http://security.ucdavis.edu/idtheft_docs/id_doc_full.pdf. Such reports will be coordinated with the campus police department.

Possible Crime - Incidents relating to the report of a possible crime should be reported directly to the campus police department.

Misuse of University Resources - Incidents pertaining to improper governmental actions (see PPM 330-095) and/or research integrity (PPM 240-01) should be reported via procedures contained in the respective policy. At the request of the Offices of the Chancellor and Provost, the IRT may assist investigations under the purview of the UC Investigations Coordination Workgroup.

Data Classification Summary Table

Data Class	Adverse Business Impact*	Sample Data Types
Protection Level 3	Extreme	CAS credential database
Protection Level 2	High	California state law "notice-triggering data"
Protection Level 1	Moderate	Personally identifiable information (unless otherwise classified as Level 0, 2 or 3). Includes: FERPA student data Staff and academic personnel records Data protected by contract, depending on terms of agreement (e.g., trade secrets, licensed software, software license keys, library paid subscription electronic resources)
Protection Level 0 (General)	Limited or none	Public directory data

Data Classes and Sample Data Type Descriptions

Protection Level 3 -- Extreme Impact

- The CAS credential database

Protection Level 2 -- High Impact

(for purposes of data classification, applies to data about California residents and non-residents)

Personally Identifiable Information (PII)

First name or first initial, and last name in combination with one or more of the following:

- Social Security Number
- Driver's license number
- California identification number

- Financial account number, credit 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

- Medical information
- Health insurance information

PCI Data (Payment Card Industry Security Council)

Credit Card number (primary account number or PAN) and one or more of the following:

- Cardholder name
- Service code
- Expiration date

PHI Data (Protected Health Information)

(e.g., information about patients of the Tang Center, the Optometry Clinic, or the Psychology Clinic)

Protection Level 1 -- Moderate Impact

All personally identifiable information that is not otherwise classified as Level 0, 2, or 3; includes, but is not limited to:

Student Records, including, but not limited to:

- Transcripts (grades)
- Exam papers
- Test scores
- Evaluations
- Financial aid records
- Loan collection records
- All records for students who have opted out of inclusion in the public directory

Academic Personnel Records as Defined in Section 160 of the Academic Personnel Manual

Including, but not limited to, confidential and non-confidential academic review records and personal information.

- Home telephone number and home address
- Spouse's or other relatives' names
- Birth date
- Citizenship
- Income tax withholdings
- Information relating to evaluation of performance

Non-Personally Identifiable Confidential Information

e.g., Confidential contract terms, information subject to a non-disclosure agreement. Depending on the financial risk or consequences to the campus, this type of information may warrant a higher impact classification.

Protection Level 0 (General) -- Limited or No Impact

Staff Information

- Name
- Date of hire or separation
- Current position title
- Current rate of pay
- Organizational unit assignment including office address and telephone number
- Full-time, part-time, or other employment status

Public Staff Records

- Name
- Date of hire
- Current position title
- Current salary
- Organizational unit assignment
- Date of separation

- Office address and office telephone number
- Current job description
- Full-time or part-time, and appointment type

Student Directory Data (unless marked directory confidential)

- Name of student
- Address, telephone, e-mail
- Dates of attendance
- Number of course units in which enrolled
- Class level
- Major field of study
- Last school attended
- Degrees and honors received
- Participation in official student activities
- Name/weight/height (intercollegiate athletic team members only)

Public Information

e.g., Course listings and prerequisites

References:

UCOP Security Incident Response Plan

UCD Security Incident Response Plan

IET Security Incident Response Plan