SACRAMENTO STATE

Introduction

Sensitive Data Inventory Survey

Working together to protect sensitive data

Data security and privacy is a critical campus-wide responsibility.

Per the Asset Management Policy in the CSU Information Security Policy and Standards. "Campuses must maintain an inventory of Information Assets containing **Level 1 or Level 2 Data** as defined in the CSU Data Classification Standard. These assets must be categorized and protected throughout their entire life cycle, from origination to destruction."

This survey helps us meet the inventory requirement and helps our campus be more secure by knowing where the data is located and who has access to the data. Campus is able to focus information security efforts based on the information you provide.

What you will be asked to do

Each business unit, program, college, or department administrator is

responsible for designating **one or more** knowledgeable individual(s) to complete a **single** survey to report on what sensitive data your area accesses or stores, where the records containing sensitive data elements are stored, and who has access to the data. If this is not you, delegate this responsibility to the individual who will complete the inventory for the area you manage.

Are you the individual responsible for completing this survey for your business unit, program, college, or department?

- ○ Yes
- ○ No

Delegate an individual to complete the Sensitive Data Inventory Survey on your behalf.

We will contact your delegate using the information you provide and give them the survey information and a link to the survey.

Your First Name:

Your Last Name:

Your Division:

Business Unit/Program/College/Department Under Your Purview for Reporting Sensitive Data Inventory:

Delegate First Name:

Delegate Last Name:

Delegate Job Title:

Delegate Phone:

Delegate Email:

Scope

Depending upon your answers, the survey can take anywhere from 20 minutes to over an hour. If you need to exit the survey due to time constraints or to gather information, **use the same computer and web browser you started with** so you will see your saved progress.

Our thanks in advance! Your IRT Information Security Office Team

Responder Information

Are you completing this for yourself or are you a delegate?

- ○ Myself
- ○ I am a delegate

Please provide the First Name of the person who delegated the survey response to you:

Please provide the Last Name of the person who

delegated the survey response to you:

Division:

Business Unit/Program/College/Department You Are Reporting On Behalf Of:

First Name:

Last Name:

Job Title:

Phone:

Email:

Personal Information

Do you or the unit you are reporting on behalf of keep records that include Personally Identifiable Information (PII) or Private/Internal Use Data?

Examples below:

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 license/California identification card number
- Health insurance or medical information
- Financial account number (such as a credit card in combination with any required security code, access code, or password that would permit access to their financial account)
- A user name or email address **in combination** with a password or security question/answer that permits access to an online account:
- Birthdate(s)
- Home Address(es)
- Home Phone number(s)
- Personal email address(es)

○ Yes
○ No

Please select the contents of these records (select all that apply):

- [ ] Name + Social Security Number (Protected Information)
- [ ] Name + Driver license/California identification card number (Protected Information)
- [ ] Name + Health Insurance information (Protected Information)
- [ ] Name + Medical information (Protected Information)
- [ ] Name + Financial account number (Protected Information)
- [ ] User name or email address, in combination with a password or security question and answer that would permit access to an online account (Protected Information)
- [ ] Birthdate(s)
- [ ] Home address(es)
- [ ] Home Phone number(s)
- [ ] Personal email address(es)
- [ ] Other

For other, please describe the contents of these records:

Where are the PII records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the PII records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Biometric information

Do you or the unit you are reporting on behalf of have records that include Biometric Information such as the following?
Note: This does not include your own biometric information such as fingerprints or facial recognition to access a device.

- Facial recognition
- Fingerprints
- Hand geometry
- Earlobe geometry
- Retina and iris patterns
- Voice waves
- DNA

- ○ Yes
- ○ No

Please select the contents of these records (select all that apply):

- [ ] Facial recognition
- [ ] Fingerprints
- [ ] Hand geometry
- [ ] Earlobe geometry
- [ ] Retina and iris patterns
- [ ] Voice waves
- [ ] DNA
- [ ] Other

For other, please describe the contents of these records:

Where are the Biometric records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**

- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Biometric records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Electronic or digitized signatures

Do you or the unit you are reporting on behalf of keep records that include Electronic Signatures (excluding

files signed with Adobe Sign)?

Electronic Signature = an electronic image or symbol of someone's handwritten signature for use to electronically sign or approve a record. Example of risk: A copy of someone's electronic signature can be used to provide "fake" approvals on forms.

- ○ Yes
- ○ No

Where are the Electronic Signatures located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Electronic Signatures?

Please list the names of personnel who have access to the Electronic Signatures, include yourself if applicable.

Private Key (digital certificate)

Do you or the unit you are reporting on behalf of keep records that include Digital Certificates or Private Keys
***(i.e., Used to allow a user to encrypt or decrypt an electronic message or file. Or used for server certificates.)*?**

- ○ Yes
- ○ No

Please identify the type of file (select all that apply):

- [ ] PGP
- [ ] Adobe
- [ ] SSL Server Certificate (Private Key)
- [ ] PKI / SMIME Signing Certificate (Private Key)
- [ ] InCommon Digital Certificate (Private Key)
- [ ] Other

If other, please describe the type of file:

Where are the Digital Certificates or Private Keys located?

- Enter the server name (s) and/or file location(s).
- If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include this information.

Who has access to the Digital Certificates or Private Keys?

Please list the names of personnel who have access, include yourself if applicable.

Psychological counsel records

Do you or the unit you are reporting on behalf of keep records that include Psychological Counseling Records?

- ○ Yes
- ○ No

Where are the Psychological Counseling records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Psychological Counseling records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Forms of national and international identification

Do you or the unit you are reporting on behalf of keep records that include National and International Identifications such as the following?

- Passports
- Visas
- I-9
- I-20
- I-94

- ○ Yes
- ○ No

Please select the contents of these records (select all that apply):

- ☐ Passports
- ☐ Visas

- [ ] I-9
- [ ] I-20
- [ ] I-94
- [ ] Other

For other, please describe the contents of these records:

Where are the National and International Identifications records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the National and International Identifications records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Passwords or Credentials

Do you or the unit you are reporting on behalf of keep records that include Passwords or Codes used to access device(s) or account(s) that store or access Level 1 or Level 2 data (excluding passwords stored in encrypted password managers)?

- ○ Yes
- ○ No

Where are the Passwords or Codes located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Passwords or Codes?

Please list the names of personnel who have access, include yourself if applicable.

Credit or Debit Cardholder Data

Do you or the unit you are reporting on behalf of keep records that include Credit or Debit Cardholder Data such as the following?

- Cardholder name
- Primary account number (PAN)
- Service code
- Expiration date

This includes if the department takes credit card information over the phone (even if they are only typing this information into a web payment processing page) or collects credit card information via paper documents sent through the mail, or other forms of payment collection methods using credit or debit cards.

- ○ Yes
- ○ No

Please select the contents of these records (select all that apply):

- ☐ Credit or debit cardholder data + Cardholder name
- ☐ Credit or debit cardholder data + Primary account number (PAN)
- ☐ Credit or debit cardholder data + Service code
- ☐ Credit or debit cardholder data + Expiration date
- ☐ Other

For other, please describe the contents of these records:

Where are the Credit or Debit Cardholder Data records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Credit of Debit Cardholder Data records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Financial Information

Do you or the unit you are reporting on behalf of keep records that include Financial Information such as the following?

- An individual's number of tax exemptions
- Amount of taxes or OASDI withheld
- Amount and type of voluntary/involuntary deductions/reductions
- Survivor amounts
- Net pay
- Designee for payroll warrants

- ○ Yes
- ○ No

Please select the contents of these records (select all that apply):

- [ ] An individual's number of tax exemptions
- [ ] Amount of taxes or OASDI withheld
- [ ] Amount and type of voluntary/involuntary deductions/reductions
- [ ] Survivor amounts
- [ ] Net pay
- [ ] Designee for payroll warrants
- [ ] Other

For other, please describe the contents of these records:

Where are the Financial Information records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Financial Information records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Healthcare Information

Do you or the unit you are reporting on behalf of keep records that include Protected Health Information (PHI) that link an individual to health care such as the following?

- Patient Name(s)
- Patient Address(es)
- Patient Email address(es)
- Patient Social security number(s)
- Medical record numbers
- Health insurance beneficiary numbers
- Medical information combined with Student ID or Medical account numbers
- Health status
- Payment for health care
- Medical history records
- Mental or physical health conditions
- Medical or mental health diagnosis and treatment records
- Health insurance policy number
- Patient consent and authorization forms
- Records release for mental and physical health

- ○ Yes
- ○ No

Please select the contents of these records (select all that apply):

- [ ] Patient Name(s)
- [ ] Patient Address(es)
- [ ] Patient Email address(es)
- [ ] Patient Social security number(s)
- [ ] Medical record number(s)
- [ ] Health insurance beneficiary number(s)
- [ ] Medical account number(s)
- [ ] Health status
- [ ] Provision of health care
- [ ] Payment for health care
- [ ] Medical history records
- [ ] Mental or physical conditions
- [ ] Medical treatment or diagnosis
- [ ] Health insurance policy number(s)
- [ ] Subscriber ID number(s)
- [ ] Unique ID used by health insurer to identify an individual
- [ ] Patient application and claims history including appeals records
- [ ] Other

For other, please describe the contents of these records:

Where are the Personal Health Information records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Personal Health Information records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Technical Security Information

Do you or the unit you are reporting on behalf of keep records that include Technical Security Information such as the following?

- Firewall configurations
- Network diagrams
- Systems configurations
- System vulnerability reports
- Locations of critical or protected assets
- Inventory of licensed software

- ○ Yes
- ○ No

Please select the contents of these records (select all that apply):

- [ ] Firewall configurations
- [ ] Network diagrams
- [ ] Systems configurations
- [ ] System vulnerability reports
- [ ] Locations of critical or protected assets
- [ ] Inventory of licensed software
- [ ] Other

For other, please describe the contents of these records:

Where are the Technical Security Information records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Technical Security Information records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Law Enforcement Information

Do you or the unit you are reporting on behalf of keep records that include Law Enforcement Information which may contain the following?

- Law enforcement records
- Names
- Home addresses
- Phone numbers
- Incident reports
- License plate numbers

- ○ Yes
- ○ No

Please select the contents of these records (select all that apply):

- ☐ Law enforcement records
- ☐ Names
- ☐ Home addresses
- ☐ Phone numbers
- ☐ Incident reports

- [ ] License plate numbers
- [ ] Other

For other, please describe the contents of these records:

Where are the Law Enforcement Information records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Law Enforcement Information records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Library Patron Information

Do you or the unit you are reporting on behalf of keep records that include Library Patron Information which may contain the following?

- Names of patrons
- Addresses
- Phone

- Social Security Numbers
- Information that links a patron with subject matter accessed or requested

- ○ Yes
- ○ No

Please select the contents of these records (select all that apply):

- ☐ Names of patrons
- ☐ Addresses
- ☐ Phone
- ☐ Social Security Numbers
- ☐ Information that links a patron with subject matter accessed or requested
- ☐ Other

For other, please describe the contents of these records:

Where are the Library Patron Information records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Library Patron Information records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Legal Information

Do you or the unit you are reporting on behalf of keep records that include Legal Information related to investigations conducted by University counsel, including client privilege communications?

- ○ Yes
- ○ No

Where are the Legal Information records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**

- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Legal Information records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Contract Information

Do you or the unit you are reporting on behalf of keep records that include Contract Information deemed confidential by the University or a third party (e.g., the vendor) which may contain the following?

- Vendor/contractor sealed bids
- Third party proprietary information per contractual agreement

- ○ Yes
- ○ No

Please select the contents of these records (select all that apply):

- ☐ Vendor/contractor sealed bids
- ☐ Third party proprietary information per contractual agreement
- ☐ Other

For other, please describe the contents of these records:

Where are the Contract Information records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Contract Information records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Employee/Student/Alumni/Job Applicant/University Donor Information

Do you or the unit you are reporting on behalf of keep records that include Employee / Student / Student Applicant / Alumni / Job Applicant / University Donor Information such as the following?

- Net salary
- Employment history
- Home address
- Personal phone numbers
- Personal email addresses
- Parents and other family member names
- Payment history
- Performance evaluations
- Background checks/investigations
- Mother's maiden name
- Birthplace (City, State, Country)
- Race and ethnicity
- Gender
- Marital status
- Physical description
- Grades
- Courses taken
- Schedules

- Test Scores
- Advisement records
- University services received
- Disciplinary actions
- Photo image database for identity validation

- ○ Yes
- ○ No

Please select the contents of these records (select all that apply):

- ☐ Net salary
- ☐ Employment history
- ☐ Home address
- ☐ Personal phone numbers
- ☐ Personal email addresses
- ☐ Parents and other family member names
- ☐ Payment history
- ☐ Performance evaluations
- ☐ Background checks/investigations
- ☐ Mother's maiden name
- ☐ Birthplace (City, State, Country)
- ☐ Race and ethnicity
- ☐ Gender
- ☐ Marital status

- [ ] Physical description
- [ ] Grades
- [ ] Courses taken
- [ ] Schedules
- [ ] Test Scores
- [ ] Advisement records
- [ ] University services received
- [ ] Disciplinary actions
- [ ] Photo image database for identity validation
- [ ] Other

For other, please describe the contents of these records:

Where are the Other Personal Information records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**

- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the Other Personal Information records?

Please list the names of personnel who have access to the data, include yourself if applicable.

University Research

Do you or the unit you are reporting on behalf of keep records that include University Research information such as trade secrets or intellectual property?

- ○ Yes
- ○ No

Where are the University Research Information records located?

- **Enter the system name(s) and/or file location(s). For example OneDrive, SharePoint, OnBase, CMS, N: drive, SacFiles Secure, etc.**
- **If you have paper records, include the building and room number, if available, or a description of the physical location if not.**
- **If this is stored on a desktop, laptop, mobile device, or USB/external hard drive, include the device type.**

Who has access to the University Research Information records?

Please list the names of personnel who have access to the data, include yourself if applicable.

Data Sanitization and Records Retention

Data Management Information and Responsibilities

Data your area manages and stores must be properly controlled and must follow the Records Retention and Disposition Schedule for both paper and electronic records. Please access and bookmark the Data Security and Records Retention site.

Please acknowledge you understand this responsibility by initialing in the box that follows.

☐

Devices/equipment **(such as printers, hard drives, computers, flash drives)** in your area that are not managed by Information Resources & Technology (IRT) need to be properly sanitized of data before being given to someone else or disposed. Please consult with IRT Desktop Support for information on proper sanitation.

Please acknowledge you understand this responsibility by initialing in the box that follows.

☐

Non-electronic Level 1 or Level 2 data (physical data records) need to follow handling guidelines. Please access and bookmark the Data Classification and Protection Standards and see section 6.0 Handling Guidelines for paper records.

Please acknowledge you understand this responsibility by initialing in the box that follows.

☐

For Data Systems or Cloud Services that your area manages or utilizes, your unit needs to review user accounts/access and security at least annually according to the CSU Access Control Standard and document the review.

Please acknowledge you understand this responsibility by initialing in the box that follows.

☐

To find out more about the Data Privacy Policies and Standards required to protect sensitive data under your purview visit and bookmark the IRT Information Security Office Data Privacy Policies and Standards website. You can contact the IRT Information Security Office for additional information or consultation.

Encryption and Physical Inventory

Additional Data Management Information and Responsibilities

All Level 1 electronic records need to be encrypted. If you are unsure if your electronic records are encrypted, consult with the IRT Information Security Office. Please note: If the records are stored in a secure system such as PeopleSoft (CMS) or on SacFiles Secure, then they are encrypted.

Please acknowledge you understand this responsibility by initialing in the box that follows.

☐

If Level 1 data is stored on a device such as a mobile phone, tablet or electronic storage device, the the device must be encrypted and also locked or secured by a method such as Touch ID, Passcode Lock, or Pattern.

Please acknowledge you understand this responsibility by initialing in the box that follows.

Personally owned computers cannot be used to store or access Level 1 data. Please ensure that personnel under your purview are aware of this restriction. If you are aware of Level 1 data being stored or accessed on a personal computer, please consult with the IRT Information Security Office to mitigate the current risk and to establish a timeline to end the practice for personnel in your area.

See sections 2.0 and 6.0 of the Sacramento State Data Classification and Protection Standards.

Please acknowledge you understand this responsibility by initialing in the box that follows.

Visit and bookmark the IRT Information Security Office website for information on reporting potential unauthorized access, compromises, and data loss.

File Upload

If you made one or more lists for the following categories as part of your survey preparation (great work!), please upload them as a helpful supplement to your survey response:

A) Computers that store or manage Level 1 data
Please include: 1) user's name, 2) computer name, 3) property tag, and 4) device location
B) Cloud applications that store or manage Level 1 data
Please include: 1) cloud application name(s), 2) name(s) of the functional administrator(s) for the app(s)
C) Locations that store or manage Level 1 data
Please include: 1) description of storage type, and 2) office/room number

If you do not have any lists to upload, simply click “next” to complete your survey.