Top Information Security Concerns for Campus Executives & Data Stewards

Last reviewed: June 2017

Related Resources:

- **Top Information Security Concerns for HR Leaders & Process Participants - Protecting Your HR Assets**
- **Top Information Security Concerns for Researchers**

Do Campus Executives & Data Stewards know:

1. What/Where is my data?
2. How sensitive is it?
3. Who's responsible for it?
4. Who has access to it?
5. Do I need to keep it?
6. What if it gets into the wrong hands?

1. What/Where is my data?

What data are in my part of the organization and where are they located?

a. Do I know where paper records that contain sensitive data are located and used?
b. Do I know where electronic sensitive data are located and used?
c. Do I know the quantity of data?
d. Is it possible to store sensitive data on removable media or portable devices and is it part of regular business processes?
e. Is data stored on home computers, personally owned devices, or personally managed devices as part of approved workflows?
f. Do I know if a third party has access to or holds data from my organization?

RESOURCES

- Asset and Data Management - Information Security Guide chapter
- Confidential Data Handling Blueprint

Top of page

2. How sensitive is it?

How sensitive is the data in my part of the organization?

a. Do I know what data my institution considers sensitive? (Many institutions have established data classification policies outlining multiple levels of data sensitivity - e.g., University of Michigan.)
b. What are the consequences if sensitive data gets into the wrong hands? Do I understand the impacts should the data no longer be available or if the integrity of the data is compromised?

c. What are the federal, state, contractual and institutional requirements for data under my responsibility?
d. Do I know the legal and civil consequences of failing to protect the data or failing to follow the laws and policies regulating the data?
e. Does my institution have a data privacy and security policy and do I know what/where it is? Do I appropriately mitigate the risk level of data under my responsibility? Do I have a risk mitigation plan?
f. What are the risks of outsourcing data for which I am responsible to a third party?

RESOURCES

- Data Classification Toolkit
- Risk Management Framework
- Vendor and Third-Party Risk Management - Information Security Guide chapter

Top of page

3. Who's responsible for it?

Who's responsible for the security of information in my part of the organization?

a. Have I clearly outlined employee roles and responsibilities for securing information?
b. Have I made information (training, policies, procedures) available to employees so that they understand how to protect data?
c. What is my role and responsibility for information in my part of the organization and how do I communicate that to employees?
d. How do I ensure the data protection policies of my institution are being followed?
e. Have I identified who the information asset owners/data stewards are? Do they understand that they are accountable or responsible for making decisions on risks associated with that information/data?
e. Whom may I rely on for assistance outside of my part of the organization and how do I contact them?

i. Chief Information Security Officer?
ii. Chief Information Officer?
iii. Internal Audit?
iv. General Counsel?
v. Privacy/Compliance/Risk Officer?
vi. Chief Financial Officer?
vii. Others?

RESOURCES

- Security Program Development - Information Security Guide chapter

Top of page

4. Who has access to it?

a. Do only those with a business need have access to the data? How many people need to access the information? How often is the information accessed?
b. Are they authorized, documented and tracked?
c. Are authorization records periodically audited?
d. Do employee transition procedures (new employee, position changes, departure) include steps to update authorization records?
e. Have I made information (training, policies, procedures) available to users so that they understand how to protect data?
f. Do those with access to data know where to find information about how to protect it?

RESOURCES

- Identity and Access Management - Information Security Guide chapter

Top of page

5. Do I need to keep it?

a. How long is the institution required to keep each data type? Does my institution have a retention schedule?
b. What are the benefits of keeping the data and do the benefits outweigh the costs and risks?
c. Do I know the institutions procedures for secure disposal?

RESOURCES

- Electronic Records Management Toolkit
- Records Retention and Disposition Toolkit

Top of page

6. What if it gets into the wrong hands?

a. Do I know how to recognize a data breach?
b. Do I know what my institution's procedures are to address it?
c. Do I know whom to notify in the event of a data breach?
d. Does anyone working with the data know how to identify a possible breach and notify the appropriate institutional staff?

RESOURCES

- Data Incident Notification Toolkit
- Incident Checklist
- Incident Management and Response - Information Security Guide chapter

Top of page

Questions or comments? Contact us.