EAB

Who Should Read

CIO

Chief Research Officer (Vice Provost, Vice Chancellor, Vice President for Research)

Chief Information Security Officer

Privacy and Research Compliance Officers

Proceduralizing Research Compliance

Streamlining Risk Discovery and Mitigation to Increase Research Data Security

Study in Brief

This report profiles the strategies that progressive institutions are deploying to encourage researchers to self-identify and mitigate risks to research data and to identify emerging research compliance risks.

5 Ways to Use This Research

- Identifying research data at risk
- Embedding security staff in research administration processes
- Introducing principal investigators to existing information security services
- Identifying emerging research methodologies that pose new security or compliance risks
- Familiarizing principal investigators with data classification policies

Ever-Increasing Needs for Research Data Security

Defined Compliance and Diversified Research Funding Will Drive Demand

Chief information security officers and security directors at high-research and aspiring research institutions already oversee a high volume of research compliance projects related to data security. These demands will expand, but the resources dedicated to these challenges will not increase at the same rate. CISOs expect additional requests in the future as grant awards increasingly contain more explicit security and compliance language regarding storage, access, and reporting.

- Universities must now meet a more detailed list of requirements because of new federal guidelines, chief among them NIST 800-171 (i.e., information security controls that will by applied to controlled unclassified information in select DoD contracts starting in December 2017).

- PIs must meet a different set of security requirements because of more proposals to corporate and philanthropic contract, due to relatively flat NIH and NSF funding that will force PIs to diversify their funding sources.

- Savvy PIs recognize that exemplary (and proactive) compliance can be a sometimes unspoken differentiator during grant proposal processes

A Need to Reform Ad Hoc Compliance Processes

Without changes to processes to increase researcher self-sufficiency and streamline access to research security-related service offerings, explicit security requirements and expanding funding sources will lead to unsustainable demands on information security resources. Even when only considering changes driven by NIST 800-171, the staff required to maintain ongoing security processes, let alone upfront investments in research security infrastructure, are beyond the projected resources of most institutions.

Anticipated Changes in Staffing Driven by NIST 800-171[1]

Probable Scenarios	**At a Minimum**	**Likely Scenario**	**Extreme Case**
Grantors Requiring NIST 800-171 or Similar Compliance	Department of Defense	NASA Department of Energy	Health and Human Services Department of Agriculture National Science Foundation
Percentage of Federally Funded HE R&D Expenditures Impacted (FY 2015)	13%	22%	91%
Information Security Staff Hours Annually for Ongoing Processes	.5 FTE	1 FTE	3.5 FTE

[1] "Higher Education Research and Development Survey (FY2015)", https://ncsesdata.nsf.gov/herd/2015/html/HERD2015_DST_21.html; EAB interviews

Closing the Gap Between Academic Research and Information Security

Promoting Risk Discovery and Self-Service Compliance Solutions

Three Barriers to Securing Research Data

Information security staff and researchers have difficulty identifying the data that needs protection. Challenges related to risk-discovery are two-fold: researchers are uninformed about the types of data that require additional security to ensure compliance with regulations, and CISOs are not aware of the data researchers access that could require additional support.

Information security staff spend time on simple data issues, which users could address themselves, rather than spending time securing restricted data, which they are uniquely qualified to address. When investigators realize the data they access has compliance requirements, their first step is frequently to contact the information security department, rather than accessing self-service security processes or tools. This means that information security staff spend time working with PIs to protect data that could be serviced through routine solutions, rather than spending their time on more complex restricted data that actually requires customized support.

Evolving research methodologies create new risks. New research methodologies may expose new risks, as researchers collect emerging types of data made available through new technologies and connect them in different ways. Identifying these changes as researchers develop them, and before they are executed, will limit institutional exposure to risk.

Increasing Awareness Without Increasing Demand

CISOs are caught between a desire to elevate researcher awareness of information security risks to research data and the IT security team's capacity to provide services to protect the newly discovered research data risks these initiatives would uncover. If the gaps between PI knowledge and compliance and between information security capacity and compliance go unaddressed, institutions are open to reputational risk if the data is exposed. Beyond that, they also put revenue at risk if granting organizations audit and identify areas of non-compliance, or if an increasing number of granting organizations include security requirements in RFPs that the IT security team cannot meet.

Looking for Frontier Practice

How can we enhance risk discovery for research data and streamline compliance?

Members asked the Forum to find promising, replicable approaches to address two problems: how to effectively identify research data at risk; how to expand IT's capacity to protect that data. From our interviews with CISOs, three scalable strategies emerged.

This study is based on understanding gained from diverse higher education IT leaders. We are grateful to interviewees for sharing institutional insights and benchmarking practice. We have abstracted the institutional insights to make them more generalizable for colleges and universities with different missions and budgets, but the Forum's work is as ever grounded in the proven innovations of progressive practitioners.

Featured Institutions—With Sincere Appreciation

PennState

Don Welch
CISO

Joe Gridley
Privacy and Compliance Manager and HIPAA Security Officer

Stacey Bucha
Data Security Compliance Specialist

University of Delaware

Karl Hassler
Director, IT Security Policy and Compliance

UF University of Florida

Stephanie Gray
Assistant VP, Division of Sponsored Programs

Alicia Turner
Business Relationship Manager

Selected Research Participants

Purdue University
Mary Duarte Millsaps
Research Information Assurance Officer

Stony Brook University
Matthew Nappi
Interim CISO

University of British Columbia
Don Thompson
Deputy CIO, Information Security

University of Buffalo
Jeff Murphy
Information Security Officer

West Virginia University
Alex Jalso
CISPO

Embry Riddle Aeronautical University
Richard Davis
Executive Director of IT Security

SUNY Albany
Martin Manjak
Information Security Officer

Indiana University
Andrew Korty
University Information Security Officer

What the Best Are Doing

Foundations for research security self-service include self-identifying routine risks, expediting solution plans, and anticipating emerging risks.

Surfacing Research Data at Risk

Online Risk Diagnostic

Interactive Questions Pinpoint Applicable Data Restrictions

PIs can self-identify the level of risk related to their research data by accessing an online tool that takes them through nine questions pinpointing the data restrictions that apply to projects. If necessary, the Diagnostic will prompt the PI to contact the information security team for consultation.

Streamlining Access to Existing Solutions

Research Security Solutions Toolbox

Enabling Researchers to More Easily Find Security Solutions

To reduce security staff and PI effort to complete grant proposals, institutions are linking results of security needs diagnostics to a catalog of common, pre-approved security solutions related to different risks. These catalogs may even include language PIs can use in their grant proposals to articulate the steps they will take to protect their data. Extending these catalogs to includes costs associated with data security protocols provides PIs with an estimate of initial and ongoing costs.

Uncovering New Areas for Protection

IRB Security Advisor

Managing Previously "Invisible" Risks

A handful of universities are appointing a representative from information security to institutional review boards to spot check pre-award data management plans and identify emerging research methodologies and projects that require may additional security needs.

Online Risk Diagnostic

Interactive Questions Pinpoint Applicable Risk Restrictions

Practice in Brief

Information security team builds an online questionnaire that allows PIs to self-classify the level of risk their project poses and provides recommended security controls. Based on institutional data classification policy, the survey results guide researchers to existing processes or services or prompt researchers to contact staff members in the information security office.

Implementation Steps

- IT formalizes an institutional data classification system that helps IT staff prioritize what to secure, thereby decreasing the burden on researchers (and administrative end users) for understanding complex regulations. By standardizing risk identification, the institution moves from a system where each department defends their own network to a risk-based information defense (more targeted towards sensitive information). IT work with a standing advisory committee of faculty and staff dedicated to data organization for feedback during policy development.
- Information security staff developed a simple yes/no tool that queries researchers regarding the different types of data they may access in the course of their research. When researchers indicate they have a particular type of data as part of their research, the tool displays next steps to protect that data. This tool is on the website for the Office of Information Security, with links also available from the Office of Research Compliance.
- To elevate awareness and drive adoption of the online risk diagnostic, information security staff share information about the tool during faculty and graduate assistant onboarding. To increase the effectiveness of these presentations, IT security staff will ask audience members to briefly share their research, and then use a live example to walk through the tool as a group to demonstrate in real time.

Benefits to Institution

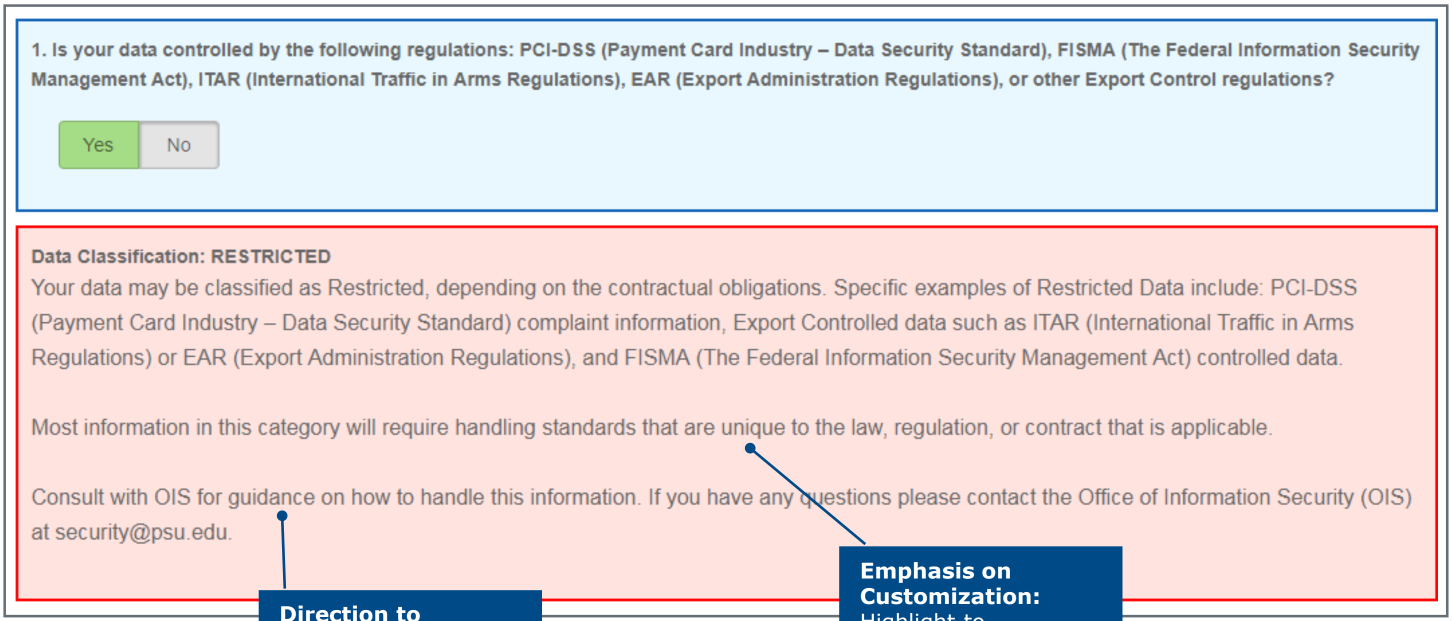
- » Increased likelihood of identifying research data at risk
- » Tiered direction for researchers based on risk, with prompts to existing security resources or staff contacts

> This tool is an easy way for researchers to identify what level of security protocols they need to provide for their data, and it directs them to the appropriate policy outlining next steps. We estimate about 80 percent of our researchers know what data they are supposed to protect and try to follow appropriate protocols. This is an opportunity to increase that number without additional staff effort.

Joe Gridley, Privacy and
Compliance Manager and HIPAA
Security Officer,
Pennsylvania State University

Spotlight Practice

Pennsylvania State University



1. Is your data controlled by the following regulations: PCI-DSS (Payment Card Industry – Data Security Standard), FISMA (The Federal Information Security Management Act), ITAR (International Traffic in Arms Regulations), EAR (Export Administration Regulations), or other Export Control regulations?

[✓ Yes] No

Data Classification: RESTRICTED

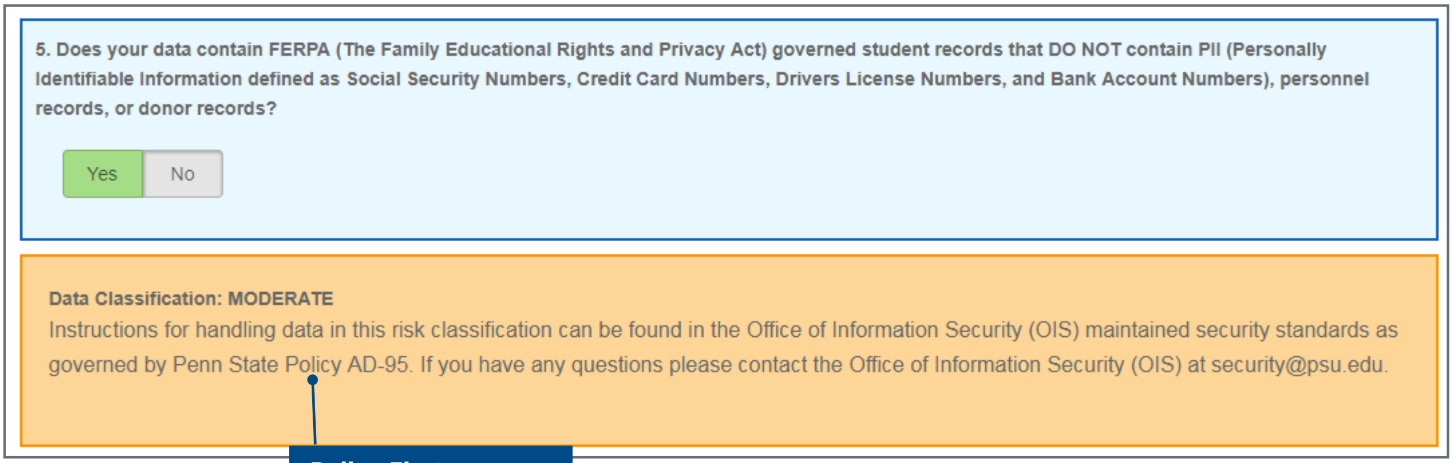
Your data may be classified as Restricted, depending on the contractual obligations. Specific examples of Restricted Data include: PCI-DSS (Payment Card Industry – Data Security Standard) complaint information, Export Controlled data such as ITAR (International Traffic in Arms Regulations) or EAR (Export Administration Regulations), and FISMA (The Federal Information Security Management Act) controlled data.

Most information in this category will require handling standards that are unique to the law, regulation, or contract that is applicable.

Consult with OIS for guidance on how to handle this information. If you have any questions please contact the Office of Information Security (OIS) at security@psu.edu.

Direction to Contact: For restricted data, recommend a consultation and provide an email contact for easy follow up

Emphasis on Customization: Highlight to researchers that this will require a potentially unique solution that information security will help them identify and develop



5. Does your data contain FERPA (The Family Educational Rights and Privacy Act) governed student records that DO NOT contain PII (Personally Identifiable Information defined as Social Security Numbers, Credit Card Numbers, Drivers License Numbers, and Bank Account Numbers), personnel records, or donor records?

[✓ Yes] No

Data Classification: MODERATE

Instructions for handling data in this risk classification can be found in the Office of Information Security (OIS) maintained security standards as governed by Penn State Policy AD-95. If you have any questions please contact the Office of Information Security (OIS) at security@psu.edu.

Policy First: Refer simple projects to existing resources to limit staff involvement in protecting less sensitive information

Research Security Solutions Toolbox

Enabling Researchers to More Easily Find Security Solutions

Practice in Brief

Some universities are developing research security service catalogs designed to educate users about risks and connect them with security services. The most sophisticated of these catalogs include sample data management plan language that researchers can incorporate into their proposals, as well as costs to access services both from the central IT unit and from other sources.

Implementation Steps

- **Conduct an audit of security services available to users.** Identify which services are most applicable to different levels of data classification as outlined by institutional policy.
- **Organize services using groups and labels that end users understand.** Include links to internal and external definitions when appropriate to clarify technical or ambiguous terms. Also provide links to existing institutional pages on specific tools and protocols.
- **Collaborate with the Office of Research Administration** to identify exemplary language for inclusion in data management plans related to different levels of data classification; include this language in the research security service catalog.
- When applicable, **calculate the cost** to offer services listed in the security service catalog and publish that information so that researchers can understand the costs during the proposal process and increase the likelihood of cost recovery from granting organizations.

Benefits to Institution

- » IT resources redirected away from responding to simple problems to more strategic security initiatives
- » Greater utilization of existing IT research security investments
- » Researchers can submit proposals with clarity regarding research compliance costs

> “
>
> With a robust online catalog for research security services, researchers can self-identify the steps they need to take to protect their research data without interacting with information security staff. Of course we’re available to answer questions and help with more complex compliance issues, but this allows us to target our services to those specific users that need more help.
>
> Karl Hassler, Director IT Security
> Policy and Compliance
> *University of Delaware*

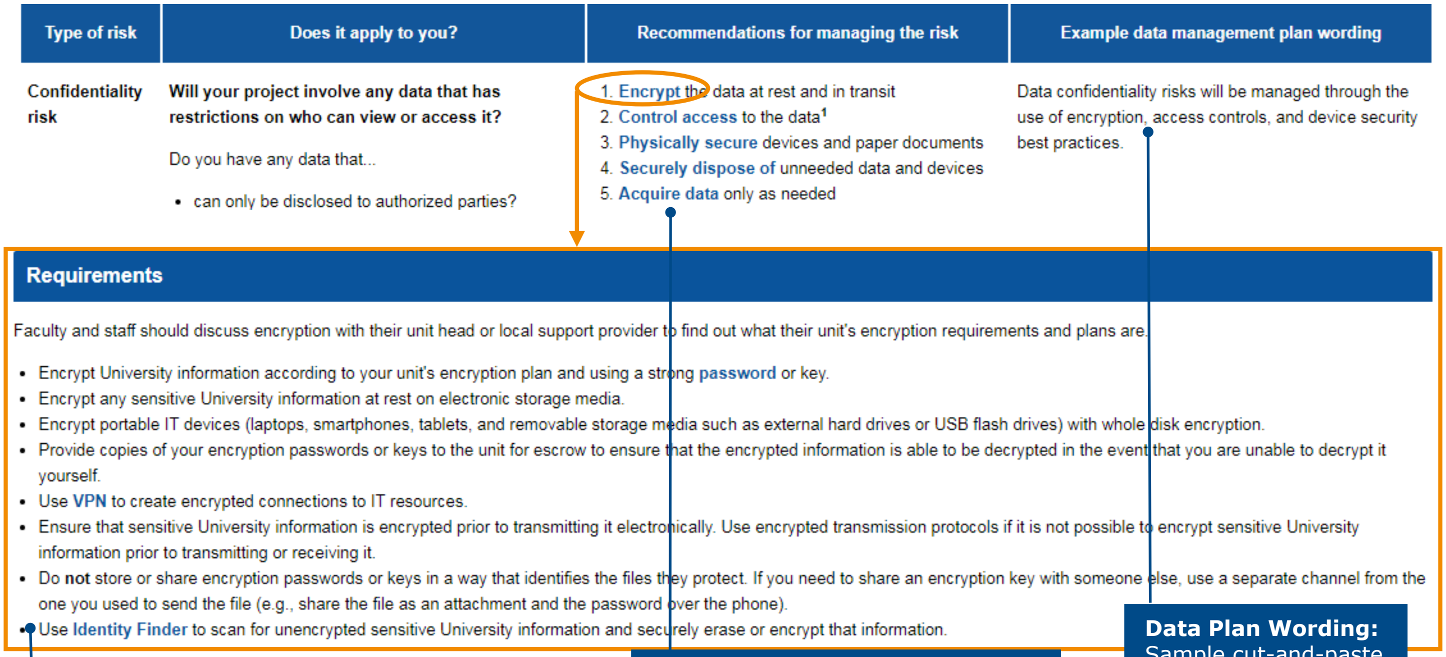
Spotlight Practice

University of Delaware

University of Florida

Research Security Service Catalogs Encourage Self-Service

University of Delaware



Type of risk	Does it apply to you?	Recommendations for managing the risk	Example data management plan wording
Confidentiality risk	**Will your project involve any data that has restrictions on who can view or access it?** Do you have any data that... • can only be disclosed to authorized parties?	1. Encrypt the data at rest and in transit 2. Control access to the data[1] 3. Physically secure devices and paper documents 4. Securely dispose of unneeded data and devices 5. Acquire data only as needed	Data confidentiality risks will be managed through the use of encryption, access controls, and device security best practices.

Requirements

Faculty and staff should discuss encryption with their unit head or local support provider to find out what their unit's encryption requirements and plans are.

- Encrypt University information according to your unit's encryption plan and using a strong password or key.
- Encrypt any sensitive University information at rest on electronic storage media.
- Encrypt portable IT devices (laptops, smartphones, tablets, and removable storage media such as external hard drives or USB flash drives) with whole disk encryption.
- Provide copies of your encryption passwords or keys to the unit for escrow to ensure that the encrypted information is able to be decrypted in the event that you are unable to decrypt it yourself.
- Use VPN to create encrypted connections to IT resources.
- Ensure that sensitive University information is encrypted prior to transmitting it electronically. Use encrypted transmission protocols if it is not possible to encrypt sensitive University information prior to transmitting or receiving it.
- Do **not** store or share encryption passwords or keys in a way that identifies the files they protect. If you need to share an encryption key with someone else, use a separate channel from the one you used to send the file (e.g., share the file as an attachment and the password over the phone).
- Use Identity Finder to scan for unencrypted sensitive University information and securely erase or encrypt that information.

Requirements Checklist: Cross-walk to IT-approved policies and pre-existing services for fast re-use

Solution Recommendations: A menu of options appropriate for self-diagnosed risk introduces researchers to possible solutions without additional IT staff time

Data Plan Wording: Sample cut-and-paste language for data management plans to include with grant proposals eases submission processes

Including Cost of Services Promotes Utilization and Cost Recovery

Modified from a University of Florida Practice

Research Security Service	Cost to University of Florida Researcher	Fully Loaded Cost to Deliver Service	Discounted Price
1 Processor Core (Normalized Compute Unit (NCU))	$200 / NCU	$530 / NCU	$230

Supporting Grant Submissions: Including information on full cost recovery allows researchers to more accurately estimate cost for compliance and increase the likelihood they receive funding to cover those costs

Demonstrating Value: Cost information about the difference between the amount researchers pay to access the service through central IT and the amount they would pay to receive the same service elsewhere creates incentive for them to use central IT services.

Institutional Research Board Security Advisor

Managing Previously “Invisible” Risks

Practice in Brief

Through representation on institutional review boards, which approve research involving humans subjects, security staff can more quickly identify “invisible” risks. In particular, an Institutional Research Board (IRB) Security Advisor can identify emerging research methodologies or approaches that may expose the institution to risk and evaluate data management plans for non-sponsored research. A formal role as an IRB Security Advisor can provide early detection of areas where additional data classification policies are necessary to mitigate risk

Implementation Steps

- Gather support and approval for information security staff IRB participation through consultation with the CIO and a representative from research administration (e.g., Vice President for Research or Director of the IRB). Determine whether information security staff are better suited as a permanent member of the IRB or as a consultant available to discuss one-off requests.
- As a newly appointed member of the IRB, complete the formal training for all new IRB members prior to attending the first meeting.
- Participate in monthly IRB meetings and review assigned proposals in the interim. Provide consultation to researchers referred to information security staff prior to proposal submission.
- Identify trends in new research methodologies that pose research compliance risks; when necessary elevate these risks to the CISO, CIO, or Privacy Office to recommend the creation of new institution-wide policies.

Benefits to Institution

» Ability to identify risks from emerging research methodologies or approaches

» Scrutiny of research without external funding by security professionals

» Improved relationships between faculty members and information security staff

“

Between increased discussion of security in the media and security awareness efforts on campus, we are seeing much stronger security plans in initial proposals from researchers. It is very rare now to see protocols that say 'data will be held in a secure environment’ as the entirety of their data management plan.

Senior Director of Computing Services
Private Research University

Spotlight Practice

Private Research University

Typical Monthly Time Commitment

Research Staff
Department Chair
PI
Security

» Attends monthly IRB meetings	2 hours
» Provides consultations to faculty prior to submission or resubmission	1 hour
» Reviews proposals and communicates recommendations	~3 hours
Total	6 hours

Responsibilities as an IRB Security Advisor

Inform IRB Members of Security Risks

Information security staff on the IRB raise awareness among other members of research protocols that introduce security risk.

Review Submissions

Information security staff evaluate proposals as a full participant on the IRB, assessing the entirety of the proposal against federal, state, and local regulations and institutional policy.

Consult Researchers

When other IRB members identify submissions with insufficient security protocols, they may recommend a meeting with the IRB member from information security for further discussion prior to resubmission.

Update Existing Policies

When information security staff identify recurring security gaps they recommend policy updates to clarify those processes.

Potential "Invisible" Risks Revealed by an IRB Security Advisor

1

Studies Include Direct Quotes from Participants' Social Media Websites

Entering the quotation in a search engine can lead to a specific web link and identify the participant

2

Research Protocols Break the Terms of Use of a Web Service

The IRB must determine whether to approve a research protocol that collects data from a website where that act violates the terms of use

3

Consent from Subjects is Difficult to Gather Through Social Media Websites

Researchers seek guidance for strategies to receive informed consent from subjects of research conducted on social media websites

DISCUSSION GUIDE

Proceduralizing Research Compliance

Using this Report to Speed Consensus for Change

Many Forum members use our research as an occasion to convene IT and campus leaders. Together, they review best-practice lessons from innovative higher education institutions and deliberate about the need to revisit policies, implement new processes, or reallocate staff and budget dollars.

Forum reports now feature self-evaluation diagnostics and discussion guides that IT leaders can use as a backbone for focused working sessions. We recommend that members distribute this report to the relevant stakeholders as pre-reading to establish a common vocabulary and fact base. Then, spend 60-90 minutes going through the diagnostics and discussion questions to decide whether policy course-corrections or resource re-allocations make sense. Forum staff would be delighted to facilitate such discussions live on your campus or on a private webconference as helpful.

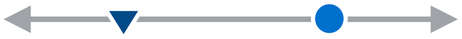
Creating a One-Hour IT Team Working Session

- Send report to IT leadership or procurement task force and committees for pre-reading
- Convene group to discuss diagnostic questions and assess need for adopting profiled practices
- Contact IT Forum for implementation support:
  - Unmetered consultation with Forum researchers
  - Networking contact with profiled institutions
  - Model policy and process templates

Online Risk Diagnostic

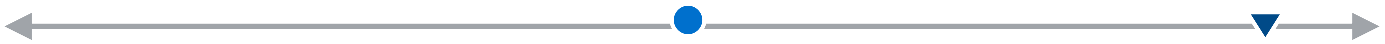
PIs can self-identify the level of risk related to their research data by accessing an online tool that takes them through nine questions pinpointing the data restrictions that apply to projects. If necessary, the Diagnostic will prompt the PI to contact the information security team for consultation.

Found in Forum Research



Typical Practice **Frontier Practice**

1. When in the grant application process do researchers learn about research data risk?

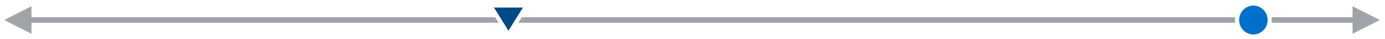


After an audit exposes insecure practices

Prior to internal propsoal review processes

During internal review processes prior to proprosal submission

2. How proactive are efforts to identify research data at risk?

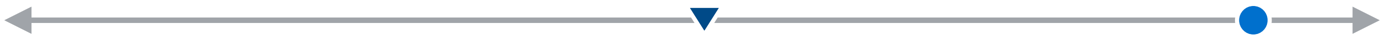


Information security staff support researchers who approach them

Staff in the research administration process identify data that requires additional security precautions

Researchers self-identify data requiring security protocols

3. What percentage of staff time is dedicated to securing low-sensitivity data?

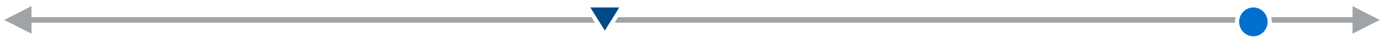


More than 80%

50%

30%

4. What percentage of PIs can self-diagnose their data classification?



50%

65%

80%

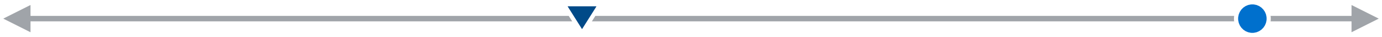
Research Security Solutions Toolbox

To reduce security staff and PI effort to complete grant proposals, institutions are linking results of security needs diagnostics to a catalog of common, pre-approved security solutions related to different risks. These catalogs may even include language PIs can use in their grant proposals to articulate the steps they will take to protect their data. Extending these catalogs to includes costs associated with data security protocols provides PIs with an estimate of initial and ongoing costs.

Found in Forum Research

Typical Practice **Frontier Practice**

1. Do we have a service catalog specifically for research security services?

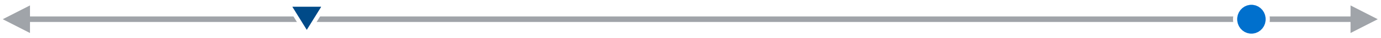


No

Yes, for internal IS purposes only

Yes, and it is published for PI access

2. How easy to navigate is the research security services catalog?

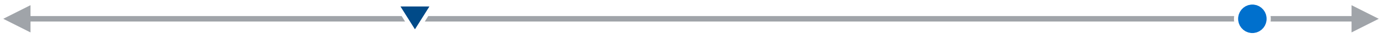


Users must click through multiple pages to access

Users can access with a single click from IT home page or drop down menu

Users can access top-level categories directly on IT's homepage

3. How user-friendly is the research security services catalog's language?

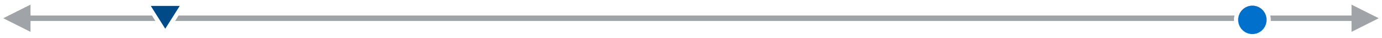


Reads as if written by an IT professional, with technical jargon

Reads as if written for a generic university, lacking local terms or names

Reads as if written by a local (articulate) student or staff member

4.What information about costs does the research security services catalog provide?

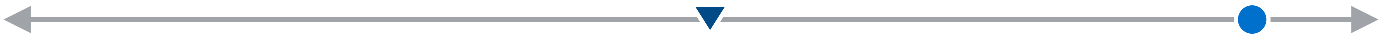


No information is available about the cost to access services

When appropriate, the cost to access a service is listed

Cost includes comparative costs for discounted rate and full cost recovery

5. How easy is it to find additional support if needed via the research security services catalog?



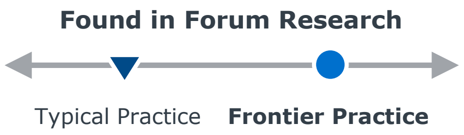
Does not reliably include contact details for service owners

Directs users to a general IT help desk

Connects users to the specific service owner

IRB Security Advisor

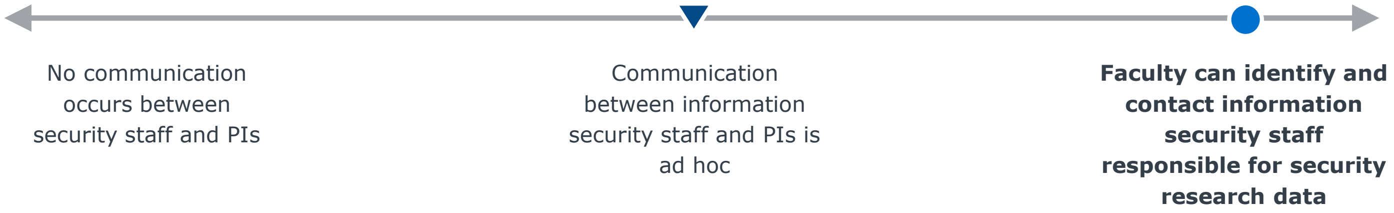
A handful of universities are appointing a representative from information to institutional review boards, to spot check pre-award data management plans and identify emerging research methodologies and projects that require may additional security needs.



Found in Forum Research

Typical Practice **Frontier Practice**

1. What processes are currently in place to encourage communication between information security staff and PIs?

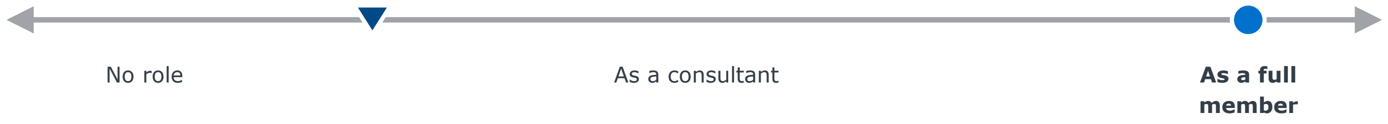


No communication occurs between security staff and PIs

Communication between information security staff and PIs is ad hoc

Faculty can identify and contact information security staff responsible for security research data

2. What role do information security staff have in relation to the IRB?

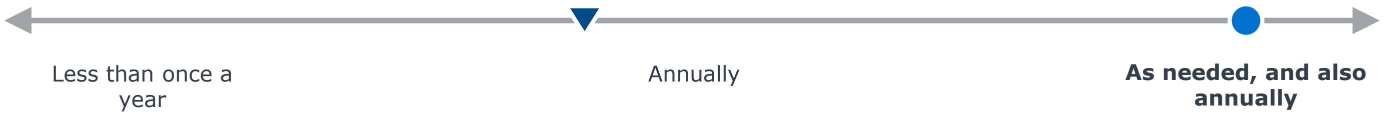


No role

As a consultant

As a full member

3. How often are data security policies reviewed based on emerging data collection methodologies and available data?



Less than once a year

Annually

As needed, and also annually

IT Forum

Project Director

Scott Winslow

Contributing Consultants

Anna Krenkel

Design Consultant

Kevin Matovich

Senior Vice President

Chris Miller

LEGAL CAVEAT

EAB is a division of The Advisory Board Company ("EAB"). EAB has made efforts to verify the accuracy of the information it provides to members. This report relies on data obtained from many sources, however, and EAB cannot guarantee the accuracy of the information provided or any analysis based thereon. In addition, neither EAB nor any of its affiliates (each, an "EAB Organization") is in the business of giving legal, medical, accounting, or other professional advice, and its reports should not be construed as professional advice. In particular, members should not rely on any legal commentary in this report as a basis for action, or assume that any tactics described herein would be permitted by applicable law or appropriate for a given member's situation. Members are advised to consult with appropriate professionals concerning legal, medical, tax, or accounting issues, before implementing any of these tactics. No EAB Organization or any of its respective officers, directors, employees, or agents shall be liable for any claims, liabilities, or expenses relating to (a) any errors or omissions in this report, whether caused by any EAB organization, or any of their respective employees or agents, or sources or other third parties, (b) any recommendation or graded ranking by any EAB Organization, or (c) failure of member and its employees and agents to abide by the terms set forth herein.

EAB, Education Advisory Board, The Advisory Board Company, Royall, and Royall & Company are registered trademarks of The Advisory Board Company in the United States and other countries. Members are not permitted to use these trademarks, or any other trademark, product name, service name, trade name, and logo of any EAB Organization without prior written consent of EAB. Other trademarks, product names, service names, trade names, and logos used within these pages are the property of their respective holders. Use of other company trademarks, product names, service names, trade names, and logos or images of the same does not necessarily constitute (a) an endorsement by such company of an EAB Organization and its products and services, or (b) an endorsement of the company or its products or services by an EAB Organization. No EAB Organization is affiliated with any such company.

IMPORTANT: Please read the following.

EAB has prepared this report for the exclusive use of its members. Each member acknowledges and agrees that this report and the information contained herein (collectively, the "Report") are confidential and proprietary to EAB. By accepting delivery of this Report, each member agrees to abide by the terms as stated herein, including the following:

1. All right, title, and interest in and to this Report is owned by an EAB Organization. Except as stated herein, no right, license, permission, or interest of any kind in this Report is intended to be given, transferred to, or acquired by a member. Each member is authorized to use this Report only to the extent expressly authorized herein.

2. Each member shall not sell, license, republish, or post online or otherwise this Report, in part or in whole. Each member shall not disseminate or permit the use of, and shall take reasonable precautions to prevent such dissemination or use of, this Report by (a) any of its employees and agents (except as stated below), or (b) any third party.

3. Each member may make this Report available solely to those of its employees and agents who (a) are registered for the workshop or membership program of which this Report is a part, (b) require access to this Report in order to learn from the information described herein, and (c) agree not to disclose this Report to other employees or agents or any third party. Each member shall use, and shall ensure that its employees and agents use, this Report for its internal use only. Each member may make a limited number of copies, solely as adequate for use by its employees and agents in accordance with the terms herein.

4. Each member shall not remove from this Report any confidential markings, copyright notices, and/or other similar indicia herein.

5. Each member is responsible for any breach of its obligations as stated herein by any of its employees or agents.

6. If a member is unwilling to abide by any of the foregoing obligations, then such member shall promptly return this Report and all copies thereof to EAB.

The best practices are the ones that work for **you.**SM

EAB

2445 M Street NW, Washington DC 20037
P 202.266.6400 | **F** 202.266.5700 | eab.com