SPIA 2.0

Security and Privacy Impact Assessment

UNIVERSITY of PENNSYLVANIA

INTRODUCTION TO THE SPIA PROGRAM

As a complex and dynamic organization, Penn regularly creates and deploys new IT applications, databases and reports that enable faculty, staff and students to achieve new learning more efficiently and effectively.

With all of the advantages new systems bring, it is also important to address the risks that come with them – in particular threats to confidential, personal or proprietary data that, if compromised, could cause significant harm to individuals or to Penn. Consider some of the types of harm that can result from failure to adequately protect confidential data.

- Identity Theft
- Stalking / Harassment
- Damage to University Reputation
- Disruption of Operations/ Services
- Legal Liability
- Regulatory Fines

Federal and state laws, industry practices, and principles of data stewardship have all driven home the fact that individuals who create, use, or maintain Confidential University Data are responsible for adequate protection of that data. The Security and Privacy Impact Assessment (SPIA) program is a resource to help each School/Center better understand frameworks for protecting data with a focus on safeguards that can be implemented to mitigate unacceptable risks.

It is important to note that SPIA does not require that all available safeguards be implemented. Rather, it is a roadmap to help organizations self-identify areas of unacceptable risk and select appropriate strategies to address them.

How does SPIA work?

SPIA currently operates through a Web-based application, where School/Center SPIA Administrators and their designated Inventory Managers will be asked to:

1. Inventory all applications and databases with Confidential University Data or "CUD" (referred to as "Assets" in the SPIA Web Application) and optionally inventory other business processes and record sets involving CUD.

2. For each Asset (i.e., application and databases with CUD) in the Inventory, answer basic questions about the data involved to help prioritize which Assets should be addressed first.

3. Utilize an educational framework to identify controls in place and areas of residual risk relating to that Asset and choose strategies to address that risk.

4. The School/Center Administrator may complete an Executive Summary designed to highlight Assets that are of greatest concern or that represent successes in how information is currently being managed for the School/Center. The Executive Summary helps capture the findings of the School/Center's assessment at a high-level. Executive Summaries are completed on an annual basis by the School/Center Administrator.

5. Submit the Inventory and risk assessment as well as an Executive Summary through the SPIA Web application to ISC Information Security and OACP's Privacy Office at the end of each fiscal year.

How do I Get Started?

School/Center SPIA Administrators and designated Inventory Managers may access the SPIA Web Application here: https://spia.apps.upenn.edu.

Other resources including the SPIA Web Application User's Guide can be found at the following site: https://www.isc.upenn.edu/security/spia

IT IS IMPORTANT TO REVIEW MODULE 1 OF THE USER'S GUIDE AT THE OUTSET TO GAIN AN UNDERSTANDING OF THE OVERALL STRUCTURE OF THE SPIA WEB APPLICATION.

The User's Guide will provide you with detailed instructions on how to complete various activities associated with the SPIA Web Application

What if I need help?

The Office of Audit, Compliance, and Privacy, and Information Systems and Computing (ISC)'s Security Office are available to assist you with the use of the tools and in applying them to any areas within your School/Center.