INDIANA UNIVERSITY

18b - Specialized Awareness and/or Training by

Employee Role

Action Item Template Response

General Action Item Information

Lead Division/Office: Information and Infrastructure Assurance (IIA)
Action Item Number: 18b
Action Item Short Name: Specialized Awareness and/or Training by Employee Role
Also supports other Action Items: 18a, 18c Implementation leader (name & email): Merri Beth Lavagnino (mbl@iu.edu); Scott Wilson (szw@iu.edu)

Description:

IU should continue its program of outreach and education to increase the awareness and understanding of security and privacy issues among all members of the university community. Individuals who interact with sensitive, important and/or private resources should have appropriate training so they can fully understand their responsibilities regarding privacy, and should periodically receive updated training.

I. DESCRIBE YOUR PLANS FOR IMPLEMENTING THIS ACTION.

We envision:

An Awareness and Training Registry that records which information security and privacy awareness and/or training activities - both basic and specialized - an employee has participated in (i.e. attended or completed) or received (i.e. mailed or emailed) and on what date.

An Online Training Tool that houses high-quality training modules addressing specialized awareness and/or training related to information security and privacy.

Supervisors, Data Stewards and Data Managers, and Compliance staff able to efficiently indicate which employees are required or desired to achieve what level of mastery in which awareness or training module or activity.

Supervisors, Data Stewards and Data Managers, and Compliance staff able to efficiently identify which awareness or training modules an employee is required to complete but has not yet completed, and to easily prompt the individual to do so by a certain date.

Effective corrective measures taken when an employee, especially one who interacts with sensitive, important and/or private resources, does not complete required awareness and/or training activities.

Based on the management information made available in the above tools (especially the Online

Training Tool), the ability to tailor awareness and training materials to the identified needs of targeted segments of the university community, depending on changing risks and identified knowledge misunderstandings and gaps.

Activities will be planned to meet the specialized awareness and/or training needs of individuals in the following high-risk roles:

Action	Priority Category	Priority Number	Description
A	Medium (soon)	-	Employee with access to information classified as critical at IU
B	High (now)	1	Employee with access to an "institutional data system" or other systems that have specialized awareness or training requirements. Could include Research, Medical, FERPA, Financial, etc.
C	High (now)	2	Data Manager
D	High (now)	3	LSP Training on security fundamentals, policy fundamentals, baseline level on security, policy, and privacy Provides level of assurance of knowledge - award certificate or record on a list
E	Medium (soon)	-	System Administrator / DBA
F	Medium (soon)	-	Application Developer (includes Web)
G	Medium (soon)	-	UITS/OVPIT employee
H	Low (later)	-	Security SAT (Systems, Applications, and Theory) Seminars Three-part focus, twice a year. One of each (S, A, T) in fall and spring. Focused on security in different areas each time. Chosen according to current hot topics, feedback on needs, current vulnerabilities or threats, etc. Open to anyone in community. Presented by experts throughout IU and externally. Good way to showcase and share edge expertise.

II. WHAT ARE THE POLICY AND PRACTICE IMPLICATIONS OF YOUR PLANS?

In order for this action to be successful, all members of the university community, especially faculty and staff, will need to allocate time and effort to this action.

The successful implementation of this action is furthered by active participation by:

- Human Resources, to ensure that all employees assent to and regularly re-assent to user agreements, and fulfill user awareness and training requirements. Corrective measures will be necessary in cases where employees, especially those who interact with sensitive, important and/or private resources, do not fulfill their identified assent, awareness, and training requirements.

- the Committee of Data Stewards and associated data managers, to ensure that all employees

who interact with sensitive, important and/or private resources assent to and regularly re-assent to user agreements, and fulfill user awareness and training requirements. Procedures will be necessary for removal of access to resources in cases where these employees do not fulfill their identified assent, awareness, and training requirements.

- the various Compliance Offices, to ensure that all employees who interact with sensitive, important and/or private resources assent to and regularly re-assent to user agreements, and fulfill user awareness and training requirements. Procedures will be necessary for removal of access to resources in cases where these employees do not fulfill their identified assent, awareness, and training requirements.

- Student Affairs, to ensure that all students assent to and regularly re-assent to user agreements, and have the opportunity for additional awareness and training activities as appropriate.

- University Counsel, to ensure that all user agreements, and awareness and training activities conform to generally acceptable practices that result in the reduction of risk to the institution and to individuals.

- UITS, to ensure that tools and resources are developed or obtained and appropriately provided in a production environment to support recurring user agreement, awareness and training activities. Coordination specifically with IT Training and with enterprise-wide systems that can record user fulfillment of awareness and training requirements is anticipated.

III. IDENTIFY STAKEHOLDERS.

Once we know which specific project proposals are accepted as part of *Empowering People*, we will bring together implementation teams consisting of members from various UITS offices and other stakeholders such as HR, SES, Student Affairs, Academic Affairs, Financial, Research, HIPAA Compliance, University Counsel, IT Training, and the CDS Awareness & Training Subcommittee. These teams will formalize actual goals and plans.

In order to prepare estimated budgets and to better clarify initial project proposals for this action, we have consulted with the following individuals, units, or committees:

- Committee of Data Stewards (CDS) (in particular, the Awareness & Training Subcommittee)
- Research Compliance Committee
- Human Resources (Deb Dunbar)
- UITS Communications (Chip Rondot)
- UITS IT Community Partnerships (Todd Herring and Bob Flynn)
- UITS IT Training and Education (Chris Payne)
- UITS Learning Technology Operations (David Donaldson)
- UITS Enterprise Services, Integration and Delivery (Brian McGough)