INDIANA UNIVERSITY

18a – Basic Awareness for All IU Community Members

Action Item Template Response

General Action Item Information

Lead Division/Office: Information and Infrastructure Assurance (IIA)
Action Item Number: 18a
Action Item Short Name: Basic Awareness for All IU Community Members
Also supports other Action Items: 18, 18b, 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 to fully understand their responsibilities regarding privacy and should periodically receive updated training.

I. DESCRIBE YOUR PLANS FOR IMPLEMENTING THIS ACTION.

We envision:

Every employee receiving basic awareness on information security and privacy issues as part of the hiring process and at regular intervals throughout his or her tenure at Indiana University.

Every student receiving basic awareness on information security and privacy issues as part of the matriculation process and at regular intervals throughout his or her tenure at Indiana University.

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.

Action	Priority Category	Priority Number	Description
18a - 1	High (now)	3	To increase general awareness, cause the Use Agreement to be assented to by every employee upon employment, and then at intervals to be determined. Need method of handling expiry and notice, and procedure in the event of non-compliance. Need to identify existing employees who have not yet assented and ensure they assent. Use metrics to track adoption. PROGRESS: November 12, 2009 - Working through the CDS, all new employees now assent to the "Acceptable Use Agreement - Access to Technology and Information Resources - Employees" during the process to create their first IU computing accounts.
18a - 2	High (now)	1	To increase literacy for all new employees at all campuses - add to new employee/new faculty orientation session basic information on information security, privacy, and policy - 10-15 minutes. (Literacy is a level beyond awareness but less than training.) Prefer doing this via a high-quality video presentation in order to cover seven campuses and avoid monthly or bi-monthly travel to the campuses. If not included in formal HR/faculty orientation sessions, we propose to offer this in some other way that would reach all new employees at all campuses, for example, perhaps show the video in a separate, standalone orientation session monthly at each campus. Or put the video online and require all new employees to watch it, tracking that compliance through some method. Another possibility to increase literacy would be to add basic information on information security, privacy, and policy to all new supervisor training classes, which are required for all new supervisors. PROGRESS: September 2009 - Consulted with UITS Digital Media Production to estimate cost of producing a 10-minute, high-quality video.
18a - 3	Medium (soon)	-	To increase literacy for all current employees (method to be determined). (Literacy is a level beyond awareness but less than training). Goal is building an understanding that leads to a change of behavior, even when it means giving up some degree of convenience. This could be done through continuing the constant messages we send through existing outlets, having a booth presence at campus events, organizing presentations, increasing coverage by leveraging more of these outlets, etc. Employees should receive at least one printed reference item a year to keep the topic of information protection and privacy before them. This is crucial information, since it is now a crime to handle

			certain personal information incorrectly in Indiana. PROGRESS: April 2009 - Working through the CDS and the various compliance units, the "Protecting Red Hot Data flippy book" is designed, printed, and distributed to nearly 6,000 employees at all IU campuses who have access to central systems containing data classified as Critical.
18a - 4	High (now)	2	Create a structure and plan to provide systematic, regular, comprehensive communications to employees about data protection. This should cover all types of information, so it needs to be coordinated with medical, financial, student (FERPA), research, etc. This is an extension of 18a - 3, above, and could be envisioned as a shared newsletter with these other stakeholders on all aspects of information handling, privacy, and protection. A newsletter is a standard method, but we could modernize this approach to meet today's needs, still keeping in mind that a printed/physical item is very powerful.
18a - 5	High (now)	4	Update the Starter Kit for all students once the employee process is moved to the Use Agreement. PROGRESS: ACTION 18a - 5 COMPLETED. November 12, 2009 - All new students and affiliates now assent to the "Acceptable Use Agreement - Access to Technology and Information Resources - Students and Affiliates" during the process to create their first IU computing accounts.
18a - 6	Low (later)	-	Create a plan for delivery of information security and privacy messages to students throughout the year.

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
- UITS Communications (Chip Rondot)
- UITS IT Community Partnerships (Todd Herring and Bob Flynn)
- UITS IT Training and Education (Chris Payne)
- UITS Media Design and Production (Michael Jasiak)
- UITS Learning Technology Operations (David Donaldson)
- UITS Enterprise Services, Integration and Delivery (Brian McGough)