

State of South Carolina – Policy Guidance and Training

Policy Workshop – All Agencies

Human Resource (HR) and Security
Awareness



July 2014

Agenda

- Questions & Follow-Up
- Open Questions
- Policy Workshop Overview & Timeline
- Policy Overview: HR and Security Awareness Policy
- Risk Assessment Framework & HR and Security Awareness Policy
- Next Steps

Questions & Follow-Up

Policy Workshop Q&As

The following questions were raised during the **Mobile Security** policy workshop for **All Agencies**:

Question #1: Based on the requirements from the mobile security policy, does DIS have a recommendation for whether agencies can use a BYOD (Bring Your Own Device) approach?

Answer #1: Policy does not explicitly prohibit BYOD. Each agency should make a determination whether it can adequately protect business data on user devices through a combination of policy, awareness, and technical means.

Question #2: Building off the previous question, does DIS have a recommendation for whether agencies can use web mail, especially on personal devices?

Answer #2: Policy does not explicitly prohibit BYOD. Each agency should make a determination whether it can adequately protect business data on user devices through a combination of policy, awareness, and technical means.

Policy Workshop Q&As

The following questions were raised during the **Mobile Security** policy workshop for **All Agencies**:

Question #3: Can we (as an agency) have separate policies for mobile devices and removable media?

Answer #3: Agencies should apply security controls for removable electronic media (e.g. flash drives) similar to their controls for all magnetic or optical media (e.g. tapes, recorded CDs). Mobile devices will require additional protections due to their data processing and transmission capabilities. Protections for all of these types of devices may be documented together or separately, as the agency prefers.

Open Questions?

Policy Workshops Overview & Timeline

Policy Workshop: Timeline

Objective: Conduct bi-weekly policy workshops with selected agencies to review information security policies, address implementation challenges, risks and assist on gap analysis and action plans with the Agency-designated policy champions.

March	April	May	June	July	August
<p>Policy:</p> <ul style="list-style-type: none"> ❖ Asset Management 	<p>Policies:</p> <ul style="list-style-type: none"> ❖ Data Protection & Privacy ❖ Access Control 	<p>Policies:</p> <ul style="list-style-type: none"> ❖ Information System Acquisition, Development, Maintenance ❖ Threat and Vulnerability Management 	<p>Policies:</p> <ul style="list-style-type: none"> ❖ Business Continuity Management ❖ IT Risk Strategy 	<p>Policies:</p> <ul style="list-style-type: none"> ❖ Mobile Security ❖ HR & Security Awareness 	<p>Policy:</p> <ul style="list-style-type: none"> ❖ Physical & Environmental Security

Activities

- Facilitate bi-weekly Agency group workshops
- Review statewide policies
- Address key policy implementation challenges
- Conduct mini-gap analysis
- Discuss policy implementation plans

Agencies TO DOs

- Review Statewide policies and conduct mini-gap analysis
- Actively participate in breakout groups to discuss gaps and implementation challenges
- Identify remediation strategies and policy implementation plans

Policy Overview: HR and Security Awareness Policy

HR and Security Awareness: Key Requirements

Human Resource Compliance

Personnel Security Policy, Personnel Screening and Third-Party Personnel Security

- Agency shall define security roles and responsibilities for employees, contractors, and third party users.
- Agency shall conduct background verification checks on all candidates for employment, including contractors and third party users.

Personnel Termination and Transfer

- All agency documents, property and materials in a terminated or transferred employee's possession or control shall be returned to the agency.

HR and Security Awareness: **Key Requirements**

Security Awareness Training

Role-Based Security Training

- All updates in organizational policies and procedures shall be accompanied by appropriate awareness training for all employees, contractors and third party users related to their job function.
 - Training shall be accompanied by an assessment procedure to determine comprehension of key cyber security concepts and procedures.
- User access to information assets and systems will only be authorized to those who have passed their cyber security awareness training and are up to date with all subsequent learnings.

HR and Security Awareness: Key Requirements

Security Awareness Training

Testing, Training, and Monitoring

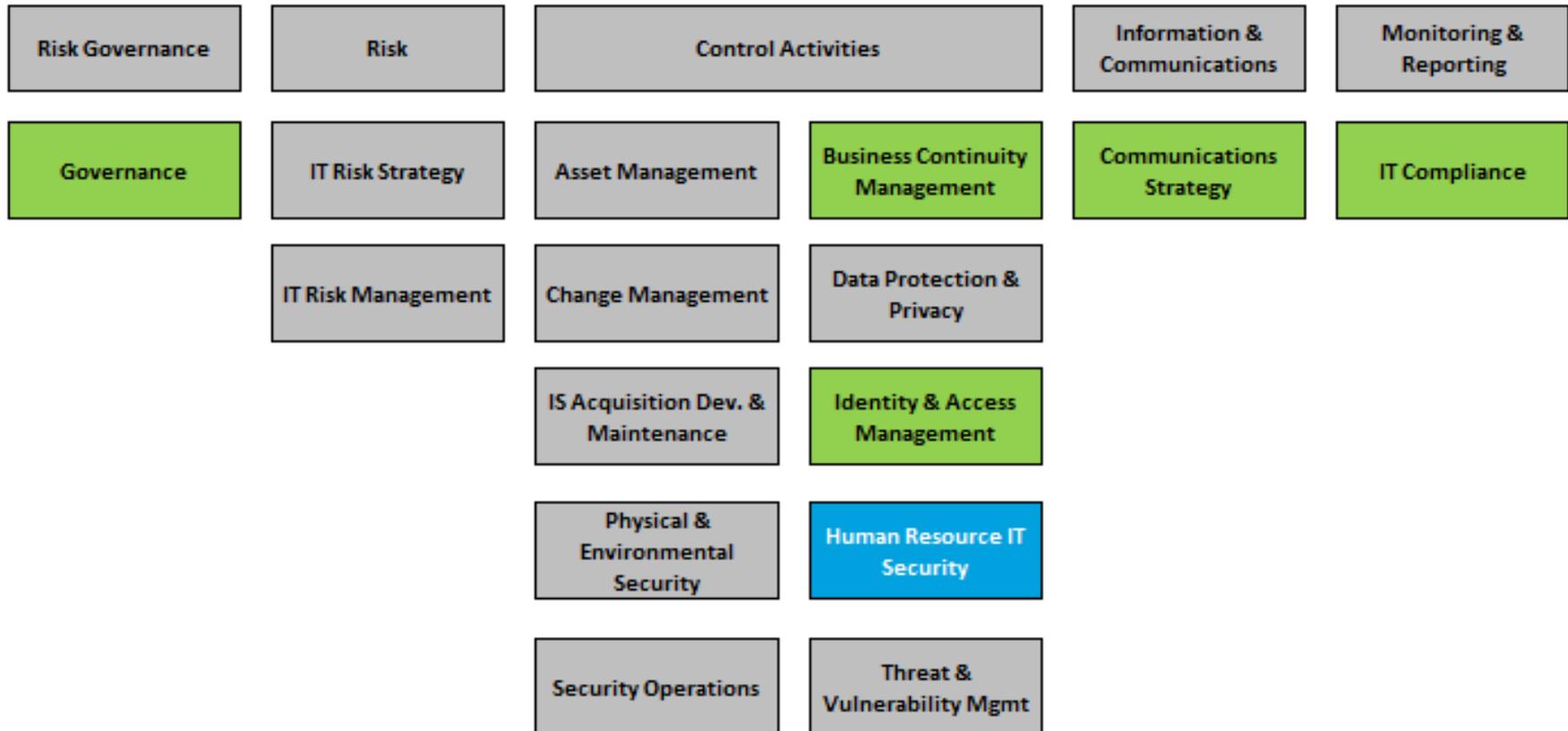
- Agency shall appoint a cyber-security awareness training coordinator, responsible for managing training content, schedules and user training completion status.
- The training coordinator, along with the Agency CISO/security manager role shall review training content on an **annual** basis such that it aligns with the State of South Carolina policies.

Risk Assessment Framework & HR and Security Awareness Policy

Risk Assessment Framework

The Risk Assessment Framework, based on the National Institute of Standards and Technology (NIST 800-53), was used as the basis to assess risk across the State Agencies using the fifteen (15) security domains (noted below):

Information Security Risk Dashboard



HR and Security Awareness Policy: Risks & Remediation Strategies

Risk assessments conducted with State Agencies uncovered a number of risks in environments with inadequately implemented Access Control Policy and procedures. Remediation strategies were created to help Agencies address gaps and implement necessary safeguards.

Examples

Overall Risks	Identified Gaps	Remediation Strategies
<ul style="list-style-type: none"> Lack of information security training Inappropriate access to information systems for terminated employees 	An ongoing information security awareness and training program does not exist within many agencies to train employees on the proper methods to protect sensitive data.	Expand scope and frequency of the existing information security awareness and training program. Provide focused security training for employees based on role/ responsibility.
	Agencies do not provide risk designation for the positions/ designations.	Expand scope and measurement of the existing information security awareness and training program
	Many agencies do not have a defined process for terminations of contractors/ third parties.	Develop a streamlined procedure to ensure contractors/ third party terminations occur in a timely manner.
	Many agencies have not established a formalized security training curriculum.	Develop a formalized information security training program for users which includes courses on information security and privacy.

HR and Security Awareness Policy: Challenges & Remediation Strategies for All Agencies

Examples	
Sample Challenges	Potential Solutions
Role based security training	<ul style="list-style-type: none"> • Generic and Role Specific Trainings: Provide generic security training to all employees (like SANS trainings etc.) • Provide on-the-job trainings and role-specific trainings to the employees based on the role of the employee during recruitment, promotion or transfer. • Certification requirements based on the level or designation of the employee (like CISSP for ISO, CCNA for Network Managers etc.,)
Changing the security culture	<ul style="list-style-type: none"> • Provide generic security awareness training to all employees, security seminars and conferences to change the security culture. • Develop multiple methods used to drive the same security topic (e.g. trainings, posters, slogans, newsletters, email, etc.) • Provide tangible examples for employees to relate new security requirements to daily tasks (e.g. hard-paper with PII/FTI data).

Next Steps

Next Steps

1. Develop or update Agency's InfoSec policies to align with published State policies
2. Conduct Policy Gap Analysis
3. Develop Policy Implementation Plan of Action
4. Develop processes to enable the implementation of InfoSec Policies
5. Promote Agency-wide InfoSec policies awareness
6. Coordinate with DIS on training and guidance