

State of South Carolina – Policy Guidance and Training

Policy Workshop – All Agencies

Physical & Environmental Security



August 2014

Agenda

- Questions & Follow-Up
- Policy Workshop Overview & Timeline
- Policy Overview: Physical & Environmental Security Policy
- Risk Assessment Framework & Physical & Environmental Security Policy
- Next Steps
- Thank You

Questions & Follow-Up

Policy Workshop Q&As

The following questions were raised during the **HR & Security Awareness** policy workshop for **All Agencies**:

Question #1: How thorough do background checks have to be in order to be compliant with the HR policy and subsequently, what type of users (new employees, existing employees, contractors, third-parties, etc.) require background checks?

Answer #1: Background check requirements are not strictly defined by DIS policy. The types of checks performed should align with the types of assets or data to which an employee or contractor will be granted access. For example, a criminal background check may be appropriate for those who will have unsupervised access to a building outside of business hours, and a credit check may be appropriate for those who will handle money or financial records.

Policy Workshop Q&As

The following questions were raised during the **HR & Security Awareness** policy workshop for **All Agencies**:

Question #2: What is the method agencies should use to upload implementations plans (and other complete templates) after Deloitte is completed, especially towards January 31, 2015 compliance?

Answer #2: DIS is in the process now of implementing a system for secure file exchange. We expect to have this solution in place before Deloitte e-room access is concluded.

Question #3: Is there a method for agencies to collaborate on common challenges, discuss solutions implemented and share information to help strengthen commonalities within the State towards compliance with the policies?

Answer #3: August through October of 2014, DIS is adding new personnel who will be specifically charged with helping agencies with their policy and compliance issues. These personnel will be positioned to facilitate collaboration among agencies.

Policy Workshop Q&As

The following questions were raised during the **HR & Security Awareness** policy workshop for **All Agencies**:

Question #2: What is the method agencies should use to upload implementations plans (and other complete templates) after Deloitte is completed, especially towards January 31, 2015 compliance?

Answer #2: DIS is in the process now of implementing a system for secure file exchange. We expect to have this solution in place before Deloitte e-room access is concluded.

Question #3: Is there a method for agencies to collaborate on common challenges, discuss solutions implemented and share information to help strengthen commonalities within the State towards compliance with the policies?

Answer #3: August through October of 2014, DIS is adding new personnel who will be specifically charged with helping agencies with their policy and compliance issues. These personnel will be positioned to facilitate collaboration among agencies.

DIS Announcement:

The Division of Technology (DT) is currently in the process of developing a questionnaire for agencies to use to respond to the Proviso 117.132 which calls for an "information technology plan" and an "information security plan" from each agency. These are not the same as the "IT Plan" that each agency submits for large procurements, nor the "information security plan" called for in DIS policy (e.g. Master policy).



DIVISION OF
INFORMATION SECURITY

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
Policy:	Policies:	Policies:	Policies:	Policies:	Policy:
❖ Asset Management	❖ Data Protection & Privacy ❖ Access Control	❖ Information System Acquisition, Development, Maintenance ❖ Threat and Vulnerability Management	❖ Business Continuity Management ❖ IT Risk Strategy	❖ Mobile Security ❖ HR & Security Awareness	❖ 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: Physical & Environmental Security Policy

Physical & Environmental Security: **Key Requirements**

Physical Access and Security

Physical Access Authorizations

- Agency shall develop a list of personnel with authorized access to a secure facility that houses information systems.
- Agency shall develop a process to review, approve, and issue credentials for facility access.
- Agency shall remove individuals from the facility access list when access is no longer required.

Physical & Environmental Security: **Key Requirements**

Physical Access and Security (cont'd)

Physical Access Control

- Agency shall control entry to/exit from the data center(s) or sensitive facilities using physical access control devices (e.g., key cards) and/or security guards.
- Agency shall maintain physical access audit logs for data center/sensitive facility entry/exit points.
- Agency shall escort visitors and monitor their activity within the sensitive facilities.

Physical & Environmental Security: **Key Requirements**

Physical Access and Security

Access Control for Transmission Medium

- Agency shall control physical access to information system distribution and transmission lines within the data center(s) using physical access control devices.

Access Control for Output Devices

- Agency shall place output devices (e.g., printers, scanners, copiers, etc.) in secured areas to authorized individuals only where they can be monitored by authorized personnel.
- Agency shall control access to information system output devices to prevent unauthorized individuals from obtaining sensitive data.

Physical & Environmental Security: **Key Requirements**

Physical Access and Security

Visitor Access Records

- Agency shall maintain visitor access records to the data center(s) and/or sensitive facilities for a minimum period of **one (1) year**.

Delivery and Removal

- Agency shall establish the processes to authorize, monitor, and control items entering and exiting the data center(s) and maintain records of those items.

Physical & Environmental Security: **Key Requirements**

Environmental Security

Emergency Shutoff

- Agency shall establish the capacity of shutting off power to data center(s) during an incident.
- Agency shall implement physical and logical controls to protect emergency power shutoff capability from unauthorized activation.

Data Center Emergency Power

- Agency shall establish uninterruptible power supply to facilitate transition to long-term alternate power in the event of a primary power source loss.

Physical & Environmental Security: **Key Requirements**

Environmental Security

Data Center Fire Protection

- Agency shall install and maintain fire detection and suppression devices that are supported by an independent power source.
- Agency shall establish an automatic fire suppression system for data center(s) that are not staffed on a continuous basis.

Data Center Temperature and Humidity Controls

- Agency shall employ automatic temperature and humidity controls in the data center(s) to prevent fluctuations potentially harmful to processing equipment.
- Agency shall employ temperature and humidity monitoring tools that have an in-built alarm and notification system.

Physical & Environmental Security: **Key Requirements**

Disposal of Equipment

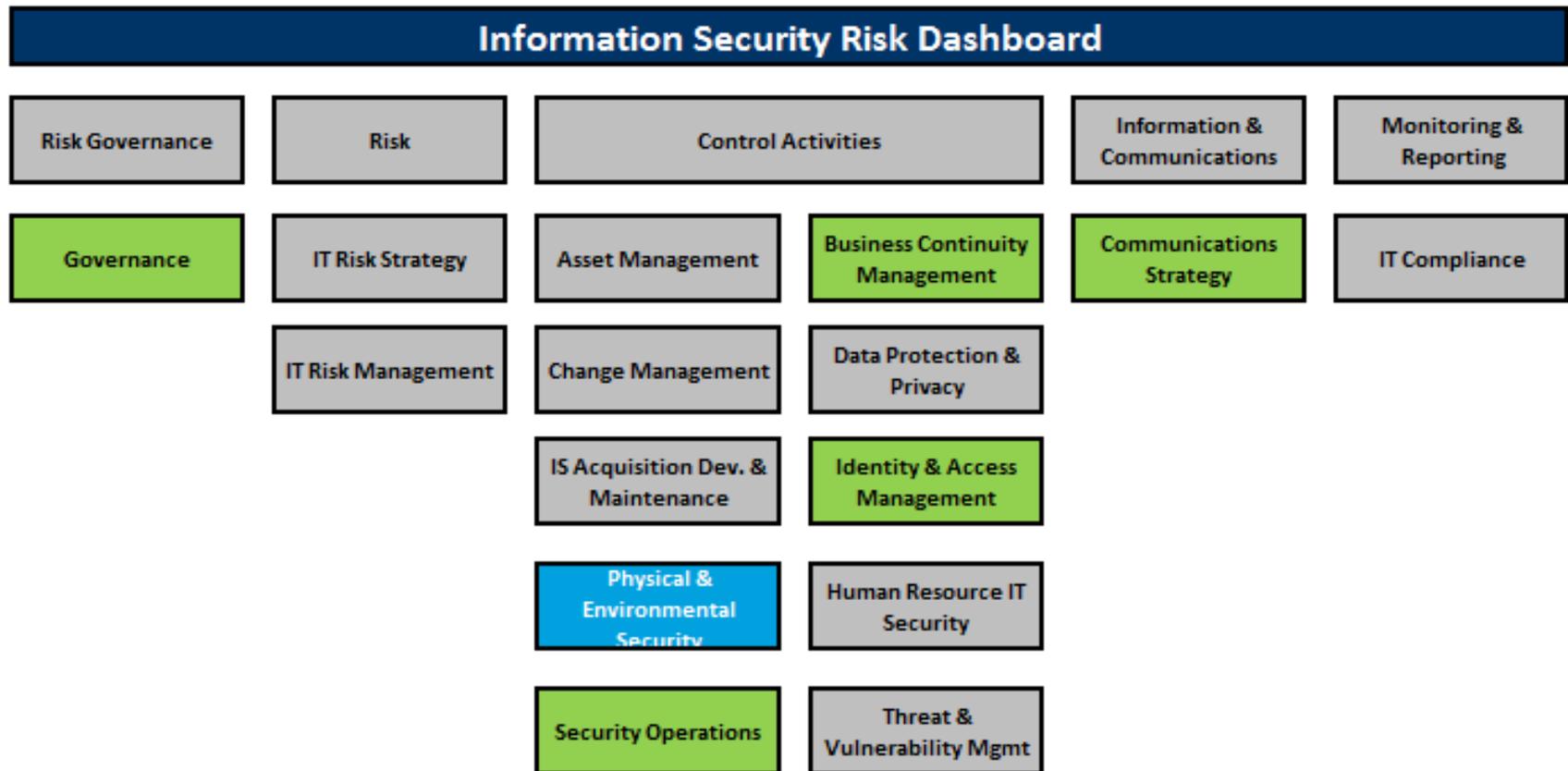
Media Sanitization

- Agency establish mechanisms for disposal of digital media and data storage devices.
- Agency shall establish processes for cleansing and disposal of computers, hard drives, and other output devices (e.g., printers, scanners, copiers, and fax machines).
- Agency shall establish controls to track and verify sanitization of devices prior to disposal.

Risk Assessment Framework & Physical and Environmental 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):



Physical & Environmental Security 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"> Unauthorized access by untrusted individuals Disruption of services due to environmental threats Loss of data due to inadequate protection of the data center 	Physical security site assessments are not performed on an ongoing basis.	Conduct physical site assessments at least annually .
	User access reviews of personnel with access to sensitive areas are not performed.	Develop a must develop a process to approve and monitor the removal of equipment from its premises.
	Lack of protection (e.g., water sprinklers, Very Early Smoke Detection Apparatus (VESDA) system not functioning) against environmental threats and hazards.	Enhance the protection (e.g., fire prevention) from environmental threats and hazards.
	Lack of identity verification, prior to issuing of visitor pass or gaining building access	Perform identity verification (e.g., driver license, passport), prior to issuing of visitor pass or gaining building access

Physical & Environmental Security Policy: Challenges & Remediation Strategies for All Agencies

Examples	
Sample Challenges	Potential Solutions
Securing the Datacenter	<ul style="list-style-type: none"> • Restrict physical access of employees or visitors to the Datacenter • Provide access based on need to know basis (as opposed to generic access) • Segregate the Datacenter into different portions depending up on the devices and sensitivity of the data present on them and provide access based on that (stricter access to devices and assets hosting highly sensitive data). • Implement protection mechanisms for fire protection, humidity and temperature controls as well as emergency power back up for the entire data center
Securing servers and assets outside the Datacenter	<ul style="list-style-type: none"> • Restrict physical access of employees to the servers and assets by having them behind closed doors with proper access control mechanism • Provide access based on need to know basis (as opposed to generic access) • Implement protection mechanisms for fire protection, humidity and temperature controls as well as emergency power back up in the form of a power inverter or UPS
Third party Physical & Environmental Security	<ul style="list-style-type: none"> • Have Physical & Environmental Security as part of the SLA with the third party and conduct risk assessments for compliance. • Perform data center visits to assess the physical and environmental security controls

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

Further Questions & Comments

For any further questions or comments on the DIS information security policies, please email the following account:

informationsecurity@bcb.sc.gov

Thank you for your time and participation in this effort, and for your continued support in helping to strengthen information security in South Carolina