

State of South Carolina – Policy Guidance and Training

Policy Workshop – All Agency

Mobile Security



July 2014

Agenda

- Questions & Follow-Up
- Policy Workshop Overview & Timeline
- Policy Overview: Mobile Security Policy
- Risk Assessment Framework & Mobile Security Policy
- Deliverable Template Tips
- Next Steps

Questions & Follow-Up

Policy Workshop Q&As

The following was discussed during the **IT Risk Strategy** policy workshop:

Information Security Metrics

- *Develop, Monitor and Report* on key performance metrics:
 - Adoption of security controls
 - Adoption of policies/procedures
 - Effectiveness of information security program
- Use S.M.A.R.T. metrics

Third-Party Risk Management

- Conduct risk assessments
- Interconnection Security Agreements
- Information sharing with third parties

DIS Deliverable Dates:

The following dates were established by DIS for compliance with the 13 State policies:

June 30, 2014 – Roles & Responsibilities Chart

January 31, 2015 – Policy Implementation Plan of Actions (all 13 policies)

July 1, 2016 – End compliance date



**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: Mobile Security Policy

Mobile Security: **Key Requirements**

Mobile Security

Device Identification

- Agency shall only allow portable media devices that are procured and assigned by the authorized Agency department.
- Agency shall only use portable media devices that can be sanitized and remotely wiped / erased.

Access Control for Mobile Devices

- Agency shall develop the following for mobile devices sanctioned by it:
 - Usage restrictions;
 - Configuration requirements;
 - Connection requirements; and
 - Implementation guidance



Mobile Security: Key Requirements

Mobile Security

Access Control for Mobile Devices (continued)

- Agency shall establish and maintain a list of approved mobile devices.
- Agency shall utilize an approved encryption mechanism for mobile devices.
- Agency shall secure all mobile devices by enabling passwords or Personal Identification Number (PIN) and also enable timeout/ locking features.
- Agency shall develop a process for users to notify designated personnel when mobile devices are lost or stolen.
- Agency shall maintain the capability to remotely wipe mobile devices in the event of their theft

Mobile Security: Key Requirements

Mobile Security

Access Control for Mobile Devices (continued)

- Agency shall centrally manage (e.g. maintain an admin group) the installation of updates to operating systems, (mobile) applications, and security patches.
 - In addition, the agency shall test the vendor recommended patches and update system firmware, OS and applications based on test results.
- Agency shall establish guidelines for the storage and transmission of information on portable media devices (e.g. scanning for malicious code)
- Agency shall delete sensitive and confidential information from the mobile devices prior to disposal



Mobile Security: **Key Requirements**

Mobile Security

Access Agreements

- Agency personnel shall sign appropriate access agreements prior to receiving the device.
- The physical security of the device shall be the responsibility of the individual receiving the device.

Media Protection Procedures

- Agency shall protect information system media until the media is destroyed or sanitized.

Media Storage

- Agency shall ensure that only secure portable storage devices (e.g., encrypted flash drives) are utilized as removable media.

Mobile Security: Key Requirements

Removable Media Security

Media Transport

- Agency shall utilize encryption mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Media Sanitization

- Agency shall sanitize removable digital and non-digital media prior to disposal.



Mobile Security: **Key Requirements**

Portable Computing Devices

Access Control for Mobile Devices

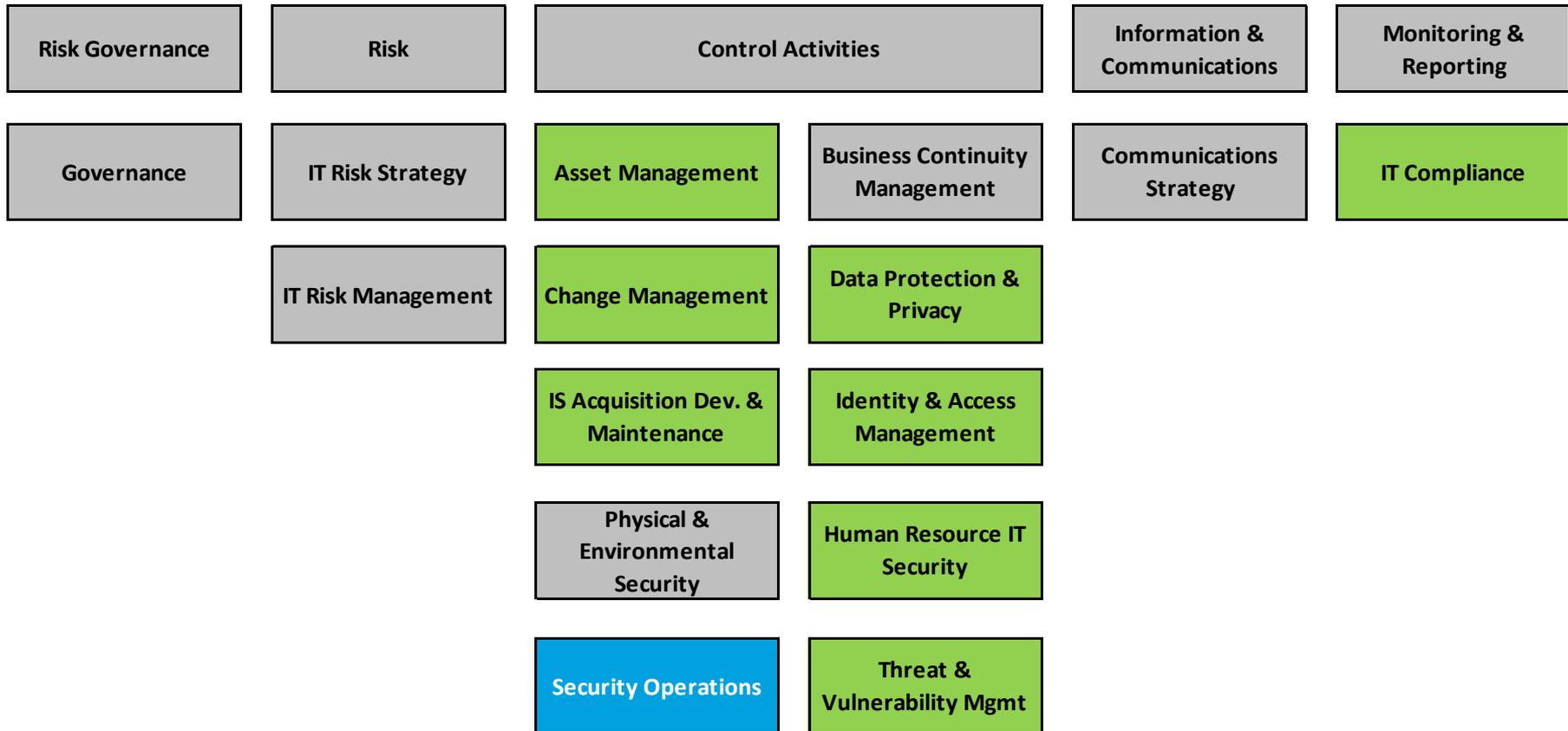
- Agency shall maintain mechanisms (e.g. tools) to automatically update and prevent viruses on portable computing devices.
- Unauthorized software shall not be installed on laptops and/or other portable computing devices without receiving authorized business case approval.
- Agency shall place asset tags on portable computing devices.
- Agency shall disable peer-to-peer wireless connections on all portable computing devices, including laptops.

Risk Assessment Framework & Mobile Security 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



Mobile 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"> • Data breach due to loss of devices • Misuse of agency mobile devices • Data leaks through removable media 	Formal documented mobile device policies and procedures do not exist.	Establish a formalized policy and procedures for mobile devices.
	Lack of controls over mobile devices such as laptops, mobile phones (for remote wipe, Data encryption, authentication, data storage etc.)	Establish formal technical controls around lap tops and mobile phones (for remote wipe, data encryption, authentication, data storage, etc.
	Inadequate protection against removable media devices such as USBs, CDs, DVDs, external hard disks etc.	Disable the use of generic removable media by disabling USB ports, CD/DVD drives on agency devices.
	Lack of encryption in the portable devices used to transfer agency data such as unencrypted disk drives (including hard disks), USBs etc.	Employ disk encryption mechanisms for laptops and other portable devices. Restrict use of portable media devices such as USBs, CDs, DVDs to only agency permitted encrypted devices.

Mobile Security Policy: Challenges & Remediation Strategies for All Agencies

Examples	
Sample Challenges	Potential Solutions
Control of Mobile Devices	<ul style="list-style-type: none"> • Implementation of a Mobile Device Management (MDM) solution to any mobile device handling agency data including email. • Use of agency issued devices only as opposed to BYOD (Bring Your Own Device) • Restriction on the device type or model or operating system (such as restricting agency devices to iOS as opposed to any generic systems) • Security awareness and training for employees
Misuse of agency devices	<ul style="list-style-type: none"> • Security awareness and training for employees • Use of MDM with Data Loss Prevention (DLP) capabilities to detect misuse or loss of data from devices • Sandboxing of agency applications and agency data present in mobile devices
Control of Removable Media	<ul style="list-style-type: none"> • Disable the use portable/removable media devices on agency endpoints and servers • Promote the use of encrypted disk drives such as encrypted USB keys, CDs, DVDs etc. • Use of whole/full disk encryption on the agency portable devices such as laptops, mobile devices etc.

Deliverable Template Tips

Gap Analysis: Tips & Guidance

Policy Requirement	Questions	YES , NO or N/A	Gap	Comments
InfoSec Policy has been reviewed and approved	Has the InfoSec Policy been reviewed and			

- Be DETAILED!!
- Consider using *'Partial'* to answer questions
- The *'Comments'* column should be used to document current environment and notes
- For identifying and finalizing gaps:
 - Consider both **process** and **documentation** gaps separately (and document both types)
 - Gaps should be detailed enough to read and understand independently when transferred to the implementation plans
 - You can have multiple gaps per question
- Consider using Gap Analyses as a process improvement exercise as well
- The Gap Analyses are meant to be filled out once as a point in time exercise
- Not all gaps will be identified with a 'No' response

Policy Implementation Plan of Action: Tips & Guidance

Action Plan						
Related Policy Clause	Current Gaps	Implementation Challenges	Implementation Strategy	Lead	Status	Due Date
SAMPLE ENTRY 1.1	SAMPLE ENTRY Asset inventory is not updated	SAMPLE ENTRY Process has not been	SAMPLE ENTRY <ul style="list-style-type: none"> Define process for 	SAMPLE ENTRY John Doe	SAMPLE ENTRY IP	SAMPLE ENTRY 3/30/2014

- Implementation Plans are meant to be living, breathing documents (even through the July 1, 2016 implementation date).
- Copy finalized gaps from Gap Analyses directly to ‘*Current Gaps*’ column
- Consider using long, medium and short-term implementation strategies
- There should be multiple, detailed bullets once an implementation strategy is finalized.
- Recommendations:
 - *Documentation* gaps should be separated (different lines) from *process* gaps.
 - Merge rows (where applicable) or transfer implementation plan to Excel
 - Identify unique ‘*due dates*’ for each bullet of the strategy
- A sample, short-term strategy could be as simple as ‘Waiting for State solution for Patch Management’ (your detailed strategy to close the gap would be identified after the DIS/DTO has announced the available solution).

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