State of South Carolina – Policy Guidance and Training

Policy Workshop – All Agency

Access Control Policy

April 2014

Agenda

- Questions & Follow-Up
- Policy Overview: Access Control Policy
- Risk Assessment Framework & Access Control Policy
- Next Steps

Questions & Follow-Up

Policy Workshop Q&As

The following questions were raised during the **Data Protection and Privacy** policy workshop for **All Agencies**:

Question #1: Does each Agency need to develop an internal Master Policy? Or, are the Agencies to utilize the current State Master Policy and develop internal procedures to align with this policy?
Answer #1: DIS does not require agencies to develop a "Master Policy." As previously stated: Agencies may choose any method which documents and implements secure processes that align with DIS Policies. This should include the review of current process documentation for inclusion of security provisions, and potentially creation of additional process documentation where secure processes are not otherwise described. Replication of the entire DIS Policy framework at the agency level is not required.

Question #2: When will the Data Inventory tool be provided by DIS? Can additional training be provided to agencies in scope?
Answer #2: Data inventory tool will be ready by April 18, 2014. Additional training (open to all State Agencies) will be provided in late April-early May. Training dates and invitations will be communicated by DIS.

Policy Workshop Q&As (Cont'd)

The following questions were raised during the **Data Protection and Privacy** policy workshop for **All Agencies**:

Question #3 Would it be possible to get the draft procedures from the data inventory training before the inventory tool is finalized?
Answer #3: Procedures will be finalized by April 18, 2014 and communicated to the Agencies by DIS.

Policy Overview: Access Control Policy

Access Control: Key Requirements

Access Management - Account Management

- Agency shall establish, document and implement access control policy and related controls.

- Agency shall require that business/data owners
  - Approve user access requests
  - Perform periodic user access review of user accounts

- Agency shall identify account types (e.g., individual, group, system, application, guest/anonymous, and temporary) and establish group membership requirements.

Access Control: Key Requirements

Access Management - Account Management (Cont'd)

- Agency's relevant personnel (e.g. system administrators) shall remove/deactivate access due to transfer, termination or access rights changes.

- Agency shall review information system accounts every **180 days** and require annual certification.

- Agency privileged accounts shall be issued based on business need, approved by information security officer, controlled, monitored and reported periodically.

Access Control: Key Requirements

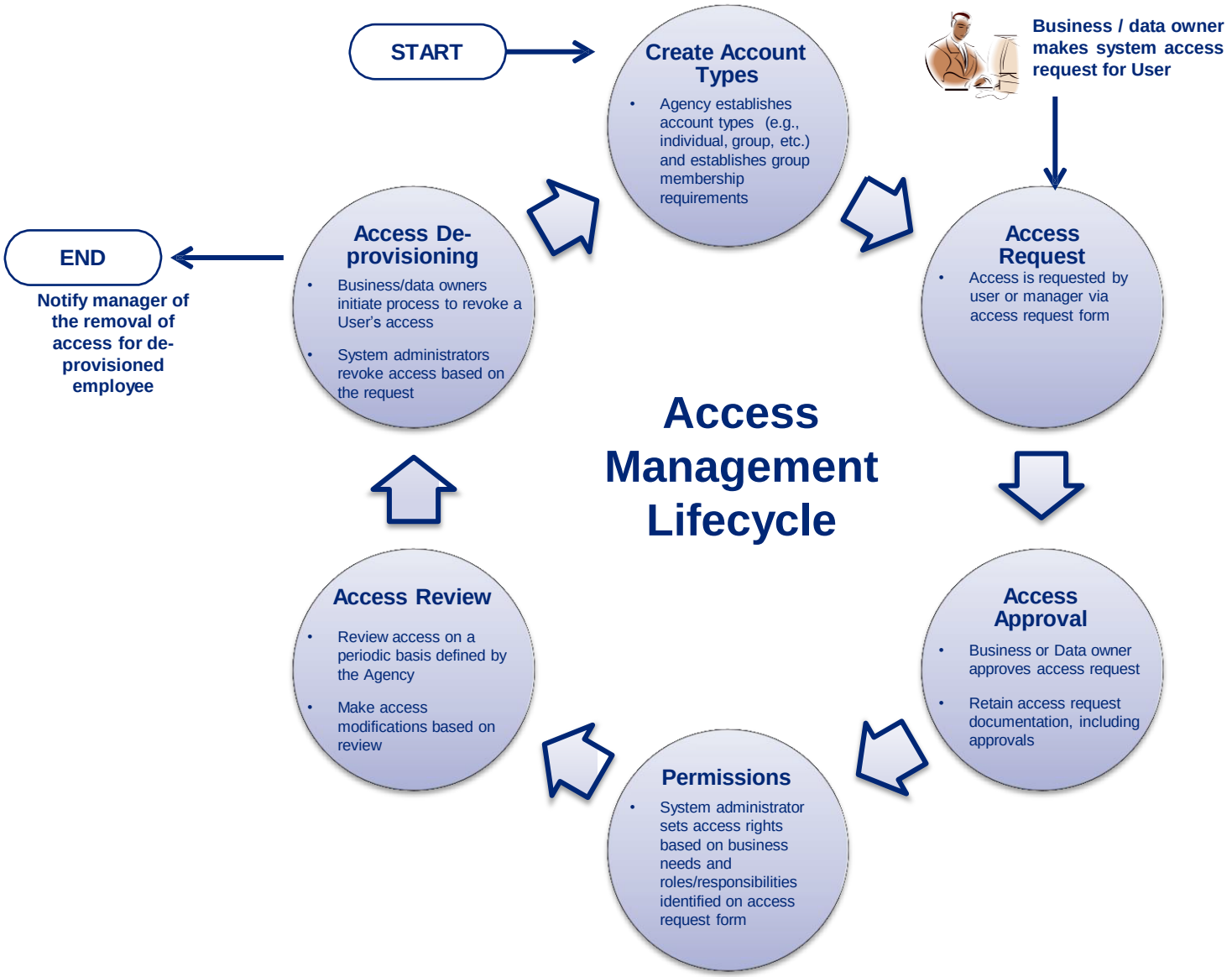
Access Management - Account Management (Cont'd)

- Agency shall define system access security requirements for vendors, contractors and partners.
- Agency shall implement access authorization controls to ensure separation of duties (e.g. divide information system testing and production functions).
- Agency shall ensure that authorized individuals have strictly controlled, audited access in accordance with the concept of 'least privilege'.

Access Enforcement

- Agency systems shall enforce a limit of unsuccessful logon attempts commensurate with type of data hosted, processed or transferred.

Access Control: Access Management



Access Control: Key Requirements

Access Management - Session Lock

- Agency shall time out sessions or require re-authentication process after **(30) minutes** of inactivity

System Use Notification

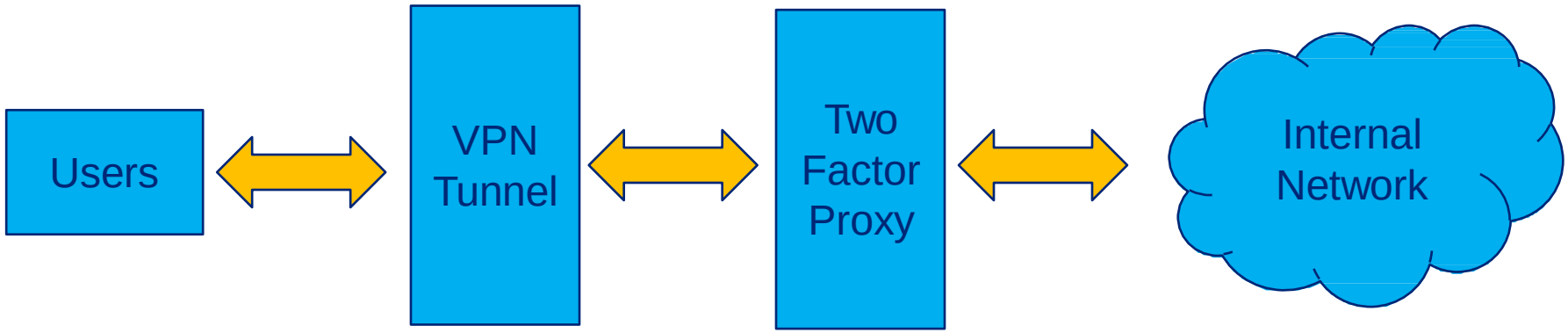
- Agency shall display a warning message before granting system access.

.

Access Control: Key Requirements

Network Access Management - Remote Access

- Agency shall document allowed methods, monitor and control remote access to the network and information systems.
- Agency shall use Virtual Private Network (VPN) or equivalent encryption technology to establish remote connections.
- *For Restricted Data and/or system admins:* Agency shall ensure employees and authorized third parties use two-factor authentication (2FA) technology for remote access.



For Restricted Data

Access Control: Key Requirements

Network Access Management - Wireless Access

- Agency shall establish usage restrictions, configuration / connection requirements, and implementation guidance for wireless access.
- Agency shall only use wireless networking technology that enforces user authentication.
- Agency shall not allow wireless access points to be installed independently by users.

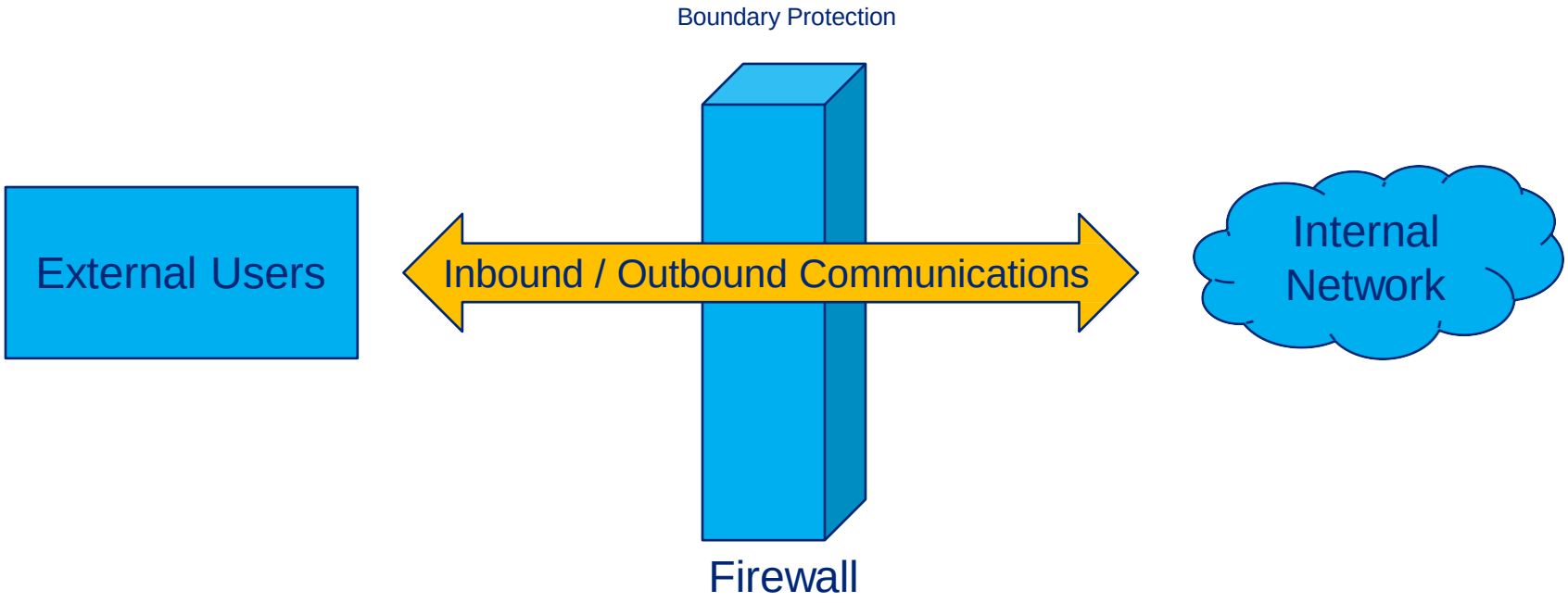
Use of External Information Systems

- Agency shall establish terms and conditions for use of the authorized external information systems

Access Control: Key Requirements

Network Access Management - Boundary Protection

- Agency shall physically or logically segregate critical information from publicly available networks.
- Agency shall minimize the network access points.



Access Control: Key Requirements

Identity Management - Identification and Authentication

- Agency shall implement unique user IDs for all employees regardless of role.

- Agency shall allow group IDs for business or operational reasons only.
  - If group IDs are permitted, Agency must have user authenticate using their unique user account *before* using the group ID.

- Agency shall minimize the use of a system, application and service accounts
  - Document, approve and designate an owner for each account used within the Agency.
  - Verify identification and location of each authorized user.

Access Control: Key Requirements

Authentication

- Agency shall use multifactor authentication for external / remote, vendor, VPN, and administrative access.

- Agency shall track unsuccessful and failed login attempts.

- Agency shall define and implement the following elements:
  - Maximum number of invalid attempts
  - Disable users exceeding the number of invalid attempts allowed
  - Keep user locked out for predetermined amount of time

Access Control: Key Requirements

Emergency Access

- Agency shall implement the following emergency procedures:
  - Only authorized personnel can receive access to the system and data
  - All actions are explicitly documented / recorded
  - Emergency action is reported and reviewed by management
  - Access granted shall be terminated within **24 hours**.

Access Control: Key Requirements

Password Policy

- Agency shall implement password-based authentication for the following:
  - All users shall change passwords every **ninety (90)** days; **sixty (60)** days if the user handles restricted data or is a system administrator; **one hundred eighty (180)** days for system accounts.
  - Password complexity shall consist of at least **eight (8)** alphanumeric (i.e., upper and lowercase letters and numbers) and/or special characters.
  - A minimum number of character shall be enforced when changing passwords (for restricted data, a minimum of **four (4)** characters is suggested).
  - Passwords shall not be the same as the last **six (6)** generations.
  - For FTI data, change or refresh authenticators every **90** days; **60** days for privileged users

Access Control: Password Management

Password Requirements	
Policy	**Policy Setting**
Enforce Password History	6 passwords remembered
Maximum Password Age	60 days – administrator accounts 90 days – user accounts 180 days – service/system accounts
Minimum Password Age	1 days
Minimum Password Length	8 characters
Complexity	Enabled - (i.e., upper and lowercase letters, and numbers) and/or special characters)
Account Lockout Threshold	Agency Dependent (i.e., 3 failed logon attempts)
Reset Account Lockout Counter After	Agency Dependent (i.e., 30 minutes)

Access Control: Key Requirements

Password Policy

- Agency users shall not share passwords.
- Agency shall not allow use of common words as passwords.
- Agency shall change system passwords immediately upon termination and resignation of a privileged user.
- Agency shall suspend user accounts after a specified number of days of inactivity.

Access Control: Key Requirements

Password Administration

- Agency users shall sign an acknowledgement of understanding password requirements and responsibilities prior to allowing access to network or information systems.

- Agency shall establish a process to assign unique user IDs and enforce authentication for non-Agency users (e.g., vendors, third parties, and contractors.

- Agency shall establish a procedure to manage new or removed privileged account passwords.

Access Control: Key Requirements

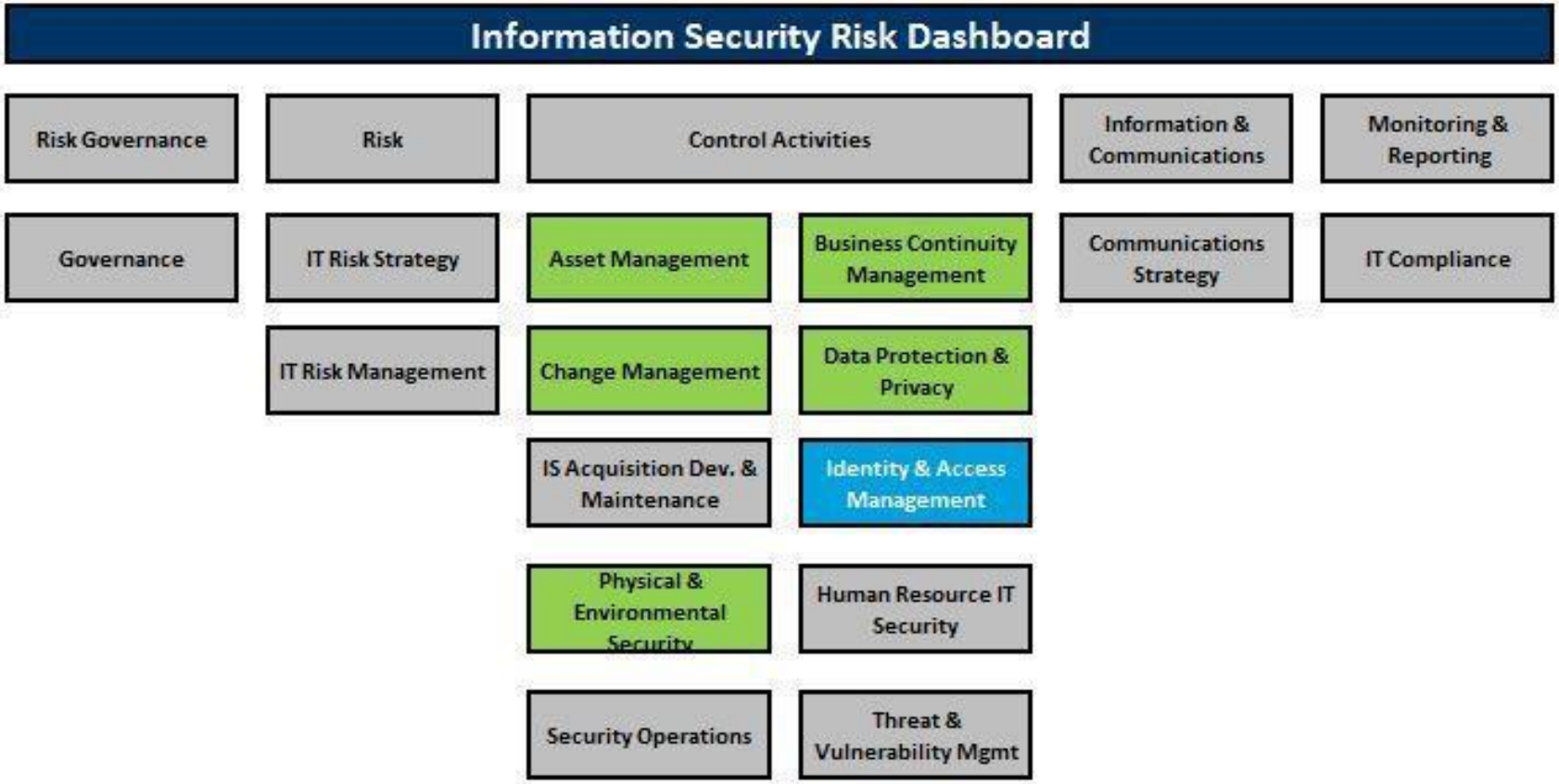
Password Administration

- Agency shall set first-time passwords to a unique value per user and changed immediately after first use.
- Agency shall not allow default passwords for network and remote applications.
- Agency shall obscure feedback of authentication information to protect exploitation and unauthorized access.

Risk Assessment Framework & Access Control 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):



Access Control 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
• Misuse of IT resources • Loss of reputation/ public image • Lack of accountability with improper access provisioning	Agencies lack the presence of a two-factor authentication solution for remote access	Deploy a two-factor authentication for users authenticating through the Virtual Private Network (VPN)
	Group administrative accounts have been established for administrator groups	Establish individual user accounts for administrator access
	Periodic user access reviews are not performed	Define and implement a procedure to perform periodic user access reviews
	Many Agencies have not established a Role Based Access Control (RBAC) framework	Develop an RBAC framework to be used for user provisioning

Access Control Policy: Risks & Remediation Strategies (Cont'd)

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
• Absence of Segregation of Duties to prevent fraud or error • Lack of remote access controls (e.g. VPN, 2FA, etc.)	Agencies have not established privileged access policy and procedures	Develop formalized privileged access policy and procedures for assigning privileged access rights.
	Agencies have not established a formal process around the lifecycle management of privileged access	Define a process for the lifecycle management of privileged access
	Agencies do not undertake Segregation of Duties (SoD) reviews or assessments for critical applications	Implement a review and assessment process around SoD for critical applications and systems

Access Control Policy: Challenges & Remediation Strategies for All Agencies

Examples	
Sample Challenges	**Potential Solutions**
Access level assignment and approval	• Implement a process for system access request and approval within the Agency • Utilize the data inventory tool to identify critical business processes, critical systems and business/data owners • Implement a Role Based Access Control (RBAC) framework • Manager will assign and approve proper application/information system/data level of access to employees, vendors, partners utilizing the • System administrator grant access following authorization from the manager • *If necessary, assign read-only access to confidential or restricted data*
Managing access for transferred employees within Agency	• Establish process for access removal for the employee/contractor • Obtain necessary approvals from employee's manager to remove application/system access • Obtain new access request and approvals from the employee's new manager • Determine if access removal is immediate and affects all application/systems • If necessary, perform data wiping and sanitization on employee's equipment

Access Control Policy: Challenges & Remediation Strategies for All Agencies (Cont'd)

Examples	
Sample Challenges	**Potential Solutions**
Managing file shared drives	• Document the data inventory tool showcasing critical business processes, business process owners and critical data residing within applications, systems and files • Scan the file shared drive and keep an inventory of sensitive data residing in that location • Determine whether data should remain on the shared drive • Determine if access should be altered to restrict users and assign appropriate users and levels of access • Provide awareness and training to employees for what can be uploaded and how to maintain proper levels of security around confidential or restricted data.
Controls over Remote Users	• Establish remote access policies and procedures • Provide guidance to managers and employees on remote access requirements • Deploy tools (i.e. VPN, 2FA) to protect inbound and outbound flow of sensitive data • Train personnel on proper usage of remote access to the Agency's network and information systems (e.g. avoid saving critical information locally (i.e. personal PC), unless remotely accessing the desktop) • Limit remote access to users based on business need

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