

# COMMONWEALTH OF VIRGINIA



Information Technology Resource Management

## INFORMATION TECHNOLOGY LOGICAL ACCESS CONTROL GUIDELINE

Virginia Information Technologies Agency (VITA)

## ITRM Publication Version Control

ITRM Publication Version Control: It is the user's responsibility to ensure that he or she has the latest version of the ITRM publication. Questions should be directed to the Associate Director for Policy, Practice and Architecture (PPA) at VITA's IT Investment and Enterprise Solutions (ITIES) Directorate. ITIES will issue a Change Notice Alert when the publication is revised. The Alert will be posted on the VITA Web site. An email announcement of the Alert will be sent to the Agency Information Technology Resources (AITRs) at all state agencies and institutions, as well as other parties PPA considers interested in the publication's revision.

This chart contains a history of this ITRM publication's revisions:

Version	Date	Purpose of Revision
Original	04/18/2007	Base Document

1 **Publication Designation** 60  
 2 ITRM Guideline SEC509-00 61  
 3 **Subject** 62  
 4 Information Technology Logical Access Control 63  
 5 64  
 6 **Effective Date** 65  
 7 April 18, 2007 66  
 8 67  
 9 **Scheduled Review** 68  
 10 One (1) year from effective date 69  
 11 70  
 12 **Authority** 71  
 13 *Code of Virginia* § 2.2-603(F) 72  
 14 (Authority of Agency Directors) 73  
 15 74  
 16 *Code of Virginia*, §§ 2.2-2005 – 2.2-2032. 75  
 17 (Creation of the Virginia Information Technologies 76  
 18 Agency; “VITA;” Appointment of Chief Information 77  
 19 Officer (CIO)) 78  
 20 79  
 21 **Scope**  
 22 This *Guideline* is offered as guidance to all Executive 80  
 23 Branch State Agencies and institutions of higher 81  
 24 education (collectively referred to as “agency”) that 82  
 25 manage, develop, purchase, and use information 83  
 26 technology (IT) resources in the Commonwealth. 84  
 27 85  
 28 **Purpose**  
 29 To guide Agencies in the implementation of the 86  
 30 information technology logical access control 87  
 31 requirements defined by ITRM Standard SEC501-01.  
 32  
 33 **General Responsibilities** 88  
 34 (Italics indicate quote from the Code of Virginia) 89  
 35 **Chief Information Officer** 90  
 36 In accordance with *Code of Virginia* § 2.2-2009, the 91  
 37 CIO is assigned the following duties: “*the CIO shall* 92  
 38 *direct the development of policies, procedures and* 93  
 39 *standards for assessing security risks, determining the* 94  
 40 *appropriate security measures and performing* 95  
 41 *security audits of government databases and data* 96  
 42 *communications. At a minimum, these policies,* 97  
 43 *procedures, and standards shall address the scope of* 98  
 44 *security audits and which public bodies are authorized* 99  
 45 *to conduct security audits.”* 100  
 46  
 47 **Chief Information Security Officer**  
 48 The CIO has designated the Chief Information 101  
 49 Security Officer (CISO) to develop Information 102  
 50 Security policies, procedures, and standards to protect 103  
 51 the confidentiality, integrity, and availability of the 104  
 52 Commonwealth of Virginia’s IT systems and data.  
 53  
 54 **IT Investment and Enterprise Solutions**  
 55 **Directorate**  
 56 In accordance with the *Code of Virginia* § 2.2-2010, 105  
 57 the CIO has assigned the IT Investment and Enterprise 106  
 58 Solutions Directorate the following duties: *Develop* 107  
 59 *and adopt policies, standards, and guidelines for* 108

*managing information technology by state agencies and institutions.”*

**All State Agencies**

In accordance with § 2.2-603, § 2.2-2005, and §2.2-2009 of the *Code of Virginia*, all Executive Branch State Agencies are responsible for complying with all Commonwealth ITRM policies and standards, and considering Commonwealth ITRM guidelines issued by the Chief Information Officer of the Commonwealth.

**Definitions**

**Agency** All Executive Branch State Agencies and institutions of higher education that manage, develop, purchase, and use IT resources in the Commonwealth of Virginia (COV).

**BIA** - Business impact analysis – The process of determining the potential consequences of a disruption or degradation of business functions.

**Data** - Data consists of a series of facts or statements that may have been collected, stored, processed and/or manipulated but have not been organized or placed into context. When data is organized, it becomes information. Information can be processed and used to draw generalized conclusions or knowledge

**Database** - a collection of data organized into interrelated tables and specifications of data objects.

**Data Communications** - Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate COV data between and among computer systems, including the hardware, software, interfaces, and protocols required for the reliable movement of this information. As used in this Guideline, Data Communications is included in the definition of government database herein.

**Data Owner** - An agency manager responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data

**Information Security Officer (ISO)** - The individual who is responsible for the development, implementation, oversight, and maintenance of the agency’s IT security program.

**IT System** - An interconnected set of IT resources and data under the same direct management control.

**Least Privilege** - The minimum level of data, functions, and capabilities necessary to perform a

- 109 user's duties. Application of this principle limits the  
110 damage that can result from accident, error, or  
111 unauthorized use of an IT system.
- 112 **Role-based Security** – The assignment of security  
113 rights to IT systems and data based on role or job  
114 function.
- 115 **Sensitive Data** - Any data of which the compromise  
116 with respect to confidentiality, integrity, and/or  
117 availability could adversely affect COV interests, the  
118 conduct of agency programs, or the privacy to which  
119 individuals are entitled.
- 120 **Sensitive IT Systems** - COV IT systems that store,  
121 process, or transmit sensitive data.
- 122 **Separation of Duties:** Assignment of responsibilities  
123 such that no one individual or function has control of  
124 an entire process. Implied in this definition is the  
125 concept that no one person should have complete  
126 control. Separation of duties is a technique for  
127 maintaining and monitoring accountability and  
128 responsibility for IT systems and data.
- 129 **System Owner** -An agency manager responsible for  
130 the operation and maintenance of an agency IT  
131 system.
- 132 **Related ITRM Policy and Standards**  
133 ITRM Policy, SEC500-02, Information Technology  
134 Security Policy (Effective 07/01/2006)  
135 ITRM Standard SEC501-01: Information Technology  
136 Security Standard (Effective 07/01/2006)  
137 ITRM Standard SEC2003-02-1: Data Removal from  
138 State Electronic Equipment Standard (Effective  
139 03/08/2004)

**TABLE OF CONTENTS**

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	INFORMATION TECHNOLOGY SECURITY .....	1
1.2	LOGICAL ACCESS CONTROL.....	1
<b>2</b>	<b>ACCOUNT MANAGEMENT .....</b>	<b>2</b>
2.1	DEFINING IDENTIFICATION, AUTHORIZATION, AND AUTHENTICATION .....	3
2.2	ACCESS REQUESTS.....	8
2.2.1	<i>Least Privilege</i> .....	8
2.2.2	<i>Role-based Access Control</i> .....	9
2.2.3	<i>Approval</i> .....	9
2.2.4	<i>Prohibition of "Guest" or Shared Accounts</i> .....	9
2.3	ACCOUNT MAINTENANCE .....	9
<b>3</b>	<b>PASSWORD MANAGEMENT.....</b>	<b>10</b>
3.1	PASSWORD REQUIREMENTS .....	11
3.2	INITIAL AND REPLACEMENT PASSWORDS .....	12
3.3	USER MANAGEMENT OF PASSWORDS .....	12
3.4	PASSWORD MAINTENANCE .....	13
3.5	LOST, STOLEN, COMPROMISED PASSWORDS .....	14
3.6	PASSWORD RESET PROCESS.....	14
3.7	SESSION CONTROLS .....	14
3.8	DEFAULT VENDOR PASSWORDS.....	15
<b>4</b>	<b>REMOTE ACCESS.....</b>	<b>15</b>
4.1	ENCRYPTION OF REMOTE ACCESS SESSIONS.....	15
4.1.1	<i>Remote Access Encryption Techniques</i> .....	15
4.2	REMOTE ACCESS SERVICE HARDENING.....	17
4.3	REMOTE ACCESS RECORDS.....	17
4.4	TRAINING.....	17
<b>5</b>	<b>AGENCY POLICES, PROCEDURES, AND EXCEPTION PROCESS.....</b>	<b>17</b>
	<b>APPENDIX A – INFORMATION SECURITY ACCESS AGREEMENT TEMPLATE AND EXAMPLE ....</b>	<b>19</b>
	<b>APPENDIX B – ACCESS REQUEST / AUTHORIZATION FORM TEMPLATE AND EXAMPLE.....</b>	<b>21</b>

# 1 Introduction

## 1.1 Information Technology Security

This Guideline presents a methodology for Information Technology (IT) Logical Access Control suitable for supporting the requirements of the Commonwealth of Virginia (COV) Information Technology Security Policy (ITRM Policy SEC500-02) and the Information Technology Security Standard (ITRM Standard SEC501-01.) These documents are hereinafter referred to as the “Policy,” and “Standard,” respectively.

The function of the Policy is to define the overall COV IT security program, while the Standard defines high-level COV IT security requirements. This Guideline describes methodologies for agencies to use when implementing the logical access control requirements of the Policy and the Standard. Agencies are not required to use these methodologies however, and may use methodologies from other sources or develop their own methodologies, if these methodologies implement the requirements of the Policy and Standard.

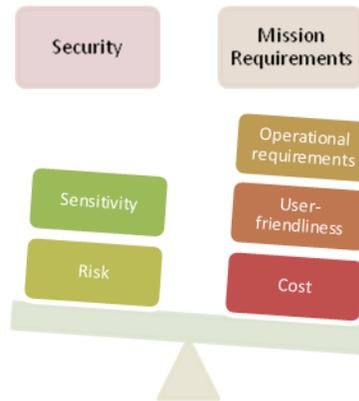
## 1.2 Logical Access Control

While physical access control protects IT systems through physical barriers (walls, locks, cameras, etc.), logical access control protects IT systems and data by verifying and validating authorized users, authorizing user access to IT systems and data, and restricting transactions (read, write, execute, delete) according to the user’s authorization level. The Standard defines logical access control requirements in the following three areas:

- Account Management
- Password Management
- Remote Access

Agencies should develop and document logical access control policies and processes that encompass all three elements.

Logical access controls are a technical means of implementing agency access policies. Development of the access policies should be directed by the Agency Head, with the assistance of the ISO, System Owners, and Data Owners. The access policies must provide protection of agency IT systems and data commensurate with sensitivity and risk. Development of such policies requires balancing the interests of security (sensitivity and risk) against what is needed to accomplish the agency’s mission (operational requirements, user-friendliness, and cost), as illustrated in Figure 1.

**Figure 1- Balance Mission Requirements Against Sensitivity and Risk**

Integrated identity and access management is a maturing domain of IT security. Agencies should consider solutions that provide automated and integrated management of:

- User identity;
- Access requests;
- Account creation and termination;
- Account privileges; and
- Passwords, including self-service password resets.

## 2 Account Management

Effective account management is central to providing Logical Access Control commensurate with sensitivity and risk. It consists of the processes of requesting, authorizing, administering, and terminating accounts which access IT systems and data, as illustrated in Figure 2. The remainder of this section discusses these processes.

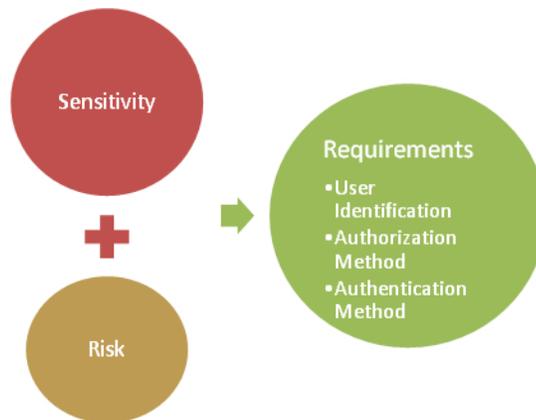
**Figure 2 - Account Management Cycle**



**2.1 Defining Identification, Authorization, and Authentication**

As shown in Figure 3, System and Data Owners develop the requirements for identification, authorization, and authentication to access an IT system according to the sensitivity and risk of the IT system and the data it processes.

**Figure 3 - Defining Requirements**



The Standard requires that agencies classify IT systems and the data they process as sensitive and non-sensitive. Agencies should further differentiate the sensitivity of IT systems and data as recommended in Tables 1 and 2 and document and enforce identification, authorization, and authentication requirements accordingly. Table 1 delineates recommended requirements for internal COV IT systems; Table 2 lists these requirements for customer-facing COV IT systems.

Passwords are specifically required by the Standard for access to all sensitive IT systems and are recommended for all IT systems. Agencies should document policies and procedures that require User IDs and passwords to be delivered to users separately.

Other authentication methods should be considered according to risk and sensitivity. In determining sensitivity level for customer-facing systems, agencies should consider:

- Whether allowing customer access to the data raises the sensitivity level of the data.
- Whether customers have access only to data regarding themselves, or whether they have access to data regarding others, and the appropriate corresponding sensitivity level.

In addition, agencies should document policies and procedures that require user acknowledgement of an Information Security Access Agreement prior to receiving access to an IT system. The nature of this agreement will vary depending on the type of user.

For internal IT systems, and for customer-facing IT systems where customers have access only to data regarding themselves, the Information Security Access Agreement should document requirements that users:

- Safeguard access control mechanisms such as user IDs and passwords and to use only those access control mechanisms specifically assigned to them;
- Receive specific authorization for any additional access required;
- Abide with all applicable COV and agency security policies, procedures, and standards; and
- Report any violation of the agreement that they observe to the agency Information Security Officer and to the Office of the Chief Information Security Officer of the Commonwealth.

The agreement should also document any limitations on the use of data to which access is authorized. Appendix B contains an example and template for an Information Security Access Agreement appropriate for this use.<sup>1</sup>

---

<sup>1</sup> Agencies may obtain user acknowledgement of an Information Security Access Agreement for customer-facing IT systems where customer users have access only to data regarding themselves by presenting the agreement to the user on-line at first logon, and requiring an affirmative action on the part of the user to acknowledge the agreement.

For customer-facing IT systems where customers have access to data regarding others, the Information Security Access Agreement should document, in addition:

- Permitted uses and disclosure of the data to which the customer user is granted access.
- Responsibilities for protection of the data to which the customer user is granted access.
- Terms and termination of the agreement; and
- Legal liabilities under the agreement.

Agencies should consult the Office of the Attorney General regarding additional requirements for such agreements.

**Table 1 – Recommended Authorization and Authentication Requirements for Internal COV IT Systems**

Sensitivity	Sensitivity Criteria	Identification	Authorization	Authentication
Low	All data handled by the IT System is of low sensitivity for compromise of confidentiality, integrity, and availability	<ul style="list-style-type: none"> <li>• Documented request from user</li> </ul>	<ul style="list-style-type: none"> <li>• Credentials mailed or emailed to user</li> </ul>	<ul style="list-style-type: none"> <li>• Password meets minimum COV requirements (initial password must be changed on first use)</li> </ul>
Medium	All data handled by the IT system is of low or moderate sensitivity for a compromise of the criteria of confidentiality, integrity, and availability	<ul style="list-style-type: none"> <li>• Documented request authorized by user’s supervisor &amp; approved by System Owner</li> <li>• Confirmation of request sent to user’s supervisor</li> </ul>	<ul style="list-style-type: none"> <li>• Credentials delivered to user only after user’s identity is verified via government-issued photo ID</li> <li>• Criminal background check successfully completed</li> </ul>	<ul style="list-style-type: none"> <li>• Password meets minimum COV requirements (initial password must be changed on first use)</li> </ul>
High	Data handled by the IT system is of high sensitivity for a compromise of one of the criteria of confidentiality, integrity, or availability	<ul style="list-style-type: none"> <li>• Documented request authorized by user’s supervisor &amp; approved by System Owner</li> <li>• Confirmation of request sent to user’s supervisor</li> <li>• User’s identity verified via government-issued photo ID</li> </ul>	<ul style="list-style-type: none"> <li>• Credentials delivered to user only after user’s identity is verified via government-issued photo ID</li> <li>• Delivery logged</li> <li>• Fingerprint criminal background check successfully completed</li> </ul>	<ul style="list-style-type: none"> <li>• Password meets minimum COV requirements (initial password must be changed on first use)</li> <li>• Second-factor identification (e.g. token) required where appropriate relative to risk</li> </ul>
Extreme	Data handled by the IT system is of high sensitivity for a compromise two or more of the criteria of confidentiality, integrity, or availability	<ul style="list-style-type: none"> <li>• Documented request authorized by user’s supervisor &amp; approved by System Owner</li> <li>• Confirmation of request sent to user’s supervisor</li> <li>• Both user’s &amp; supervisor’s identity verified via government-issued photo ID</li> </ul>	<ul style="list-style-type: none"> <li>• Credentials delivered to user in the presence of user’s supervisor</li> <li>• Both user’s &amp; supervisor’s identity verified via government-issued ID</li> <li>• Delivery logged</li> <li>• Fingerprint criminal background check successfully completed</li> </ul>	<ul style="list-style-type: none"> <li>• Password meets minimum COV requirements (initial password must be changed on first use)</li> <li>• Second-factor identification (e.g. token) and/or Biometric authentication (e.g. fingerprint, hand-span, retinal scan, etc.) required</li> </ul>

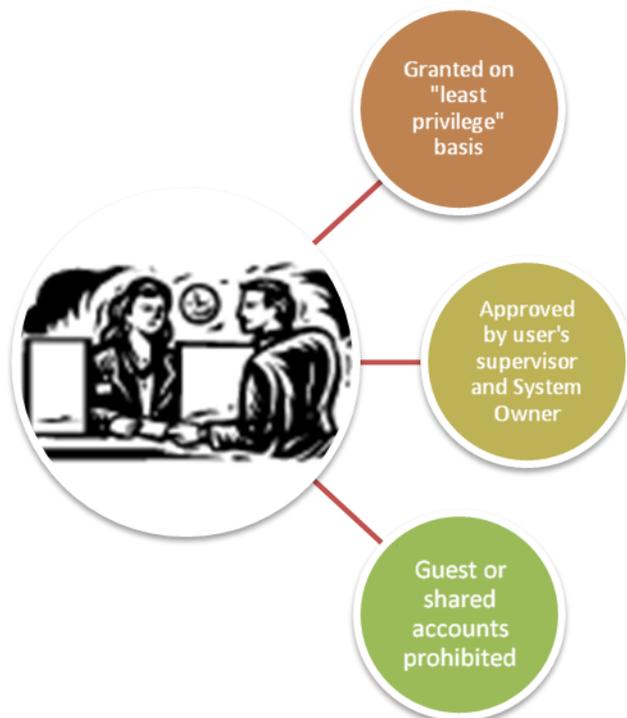
**Table 2 – Recommended Authorization and Authentication Requirements for Customer-Facing COV IT Systems**

Sensitivity	Sensitivity Criteria	Identification	Authorization	Authentication
Low	All data handled by the IT System is of low sensitivity for compromise of confidentiality, integrity, and availability	<ul style="list-style-type: none"> <li>• Documented request from customer user</li> </ul>	<ul style="list-style-type: none"> <li>• Credentials mailed or emailed to user</li> </ul>	<ul style="list-style-type: none"> <li>• Password meets minimum COV requirements (initial password must be changed on first use)</li> </ul>
Medium	All data handled by the IT system is of low or moderate sensitivity for a compromise of the criteria of confidentiality, integrity, or availability	<ul style="list-style-type: none"> <li>• Documented request from customer user approved by System Owner</li> <li>• Confirmation of request sent to customer user</li> <li>• Customer user’s identity verified based on information on file with agency regarding the customer user (i.e. Driver’s License No.)</li> </ul>	<ul style="list-style-type: none"> <li>• Credentials delivered to customer user only after customer user confirmation of request</li> </ul>	<ul style="list-style-type: none"> <li>• Password meets minimum COV requirements (initial password must be changed on first use)</li> </ul>
High	Data handled by the IT system is of high sensitivity for a compromise of one of the criteria of confidentiality, integrity, or availability	<ul style="list-style-type: none"> <li>• Documented request from customer user approved by System Owner</li> <li>• Confirmation of request sent to customer user.</li> <li>• Customer user’s identity verified based on information on file with agency regarding the customer user (i.e. Driver’s License No.)</li> </ul>	<ul style="list-style-type: none"> <li>• Credentials delivered to customer user only after customer/ user confirmation of request</li> <li>• Credentials delivered to customer user by alternate channel (i.e., US Mail)</li> <li>• Delivery logged</li> </ul>	<ul style="list-style-type: none"> <li>• Password meets minimum COV requirements (initial password must be changed on first use)</li> <li>• Second-factor identification (e.g. token) or additional identification required where appropriate relative to risk</li> </ul>
Extreme	Data handled by the IT system is of high sensitivity for a compromise two or more of the criteria of confidentiality, integrity, or availability	<ul style="list-style-type: none"> <li>• Documented request from customer user approved by System Owner</li> <li>• Request confirmed with customer user</li> <li>• Customer user’s identity verified based on information on file with agency regarding the customer user (i.e. Driver’s License No.)</li> </ul>	<ul style="list-style-type: none"> <li>• Credentials delivered to customer user only after customer/ user confirmation of request</li> <li>• Credentials delivered to customer user by alternate channel (i.e., US Mail)</li> <li>• Delivery logged</li> </ul>	<ul style="list-style-type: none"> <li>• Password meets minimum COV requirements (initial password must be changed on first use)</li> <li>• Second-factor identification (e.g. token), additional identification and/or Biometric authentication (e.g. fingerprint, hand-span, retinal scan, etc.) required</li> </ul>

## 2.2 Access Requests

Agencies must establish policies and procedures for requests and authorization for access to agency IT systems and data. The policy and procedures must require that access is authorized using the principle of least privilege. In addition, access to IT systems and data may only be granted with the approval of the user's supervisor and the System Owner; "guest" or shared accounts are prohibited. These requirements of the Standard for internal COV IT systems are illustrated in Figure 4.

**Figure 4 - IT System Access Request Requirements for Internal COV IT Systems**



Agencies should document policies and procedures for requests and authorization for access to agency IT systems and data that reflect the differentiation of sensitivity described in Tables 1 and 2. In particular, agencies should document appropriate access requests and authorization requirements for customer-facing COV IT systems, since customers do not have a supervisor to approve the request. In addition, agencies may wish to allow blanket approval of access requests for low sensitivity systems by the System Owner in order to reduce the administrative burden of these low sensitivity systems on the System Owner.

### 2.2.1 Least Privilege

Access to IT systems and data must be granted on the basis of least privilege. The principle of least privilege requires that agencies provide access only to those systems that users require to complete their functions. In addition, least privilege requires that agencies must

authorize the most restrictive access level necessary for users to perform these functions. Adhering to least privilege principle enhances protection of IT systems and data.

### **2.2.2 Role-based Access Control**

Role-based access control grants access to IT systems and data to users based on their roles within the organization or as customers of the organization, rather than on individual users. Agencies should adopt role-based access control as part of their account management policies.

Adopting role-based access control is recommended because it simplifies the administration of user access rights by associating these rights with a limited number of standardized roles. This association of access rights with standardized roles also assists in maintaining the principle of least privilege. In addition, agencies should adopt access control policies that prohibit assignment of multiple roles to a single user that can combine to violate separation of duties requirements.

### **2.2.3 Approval**

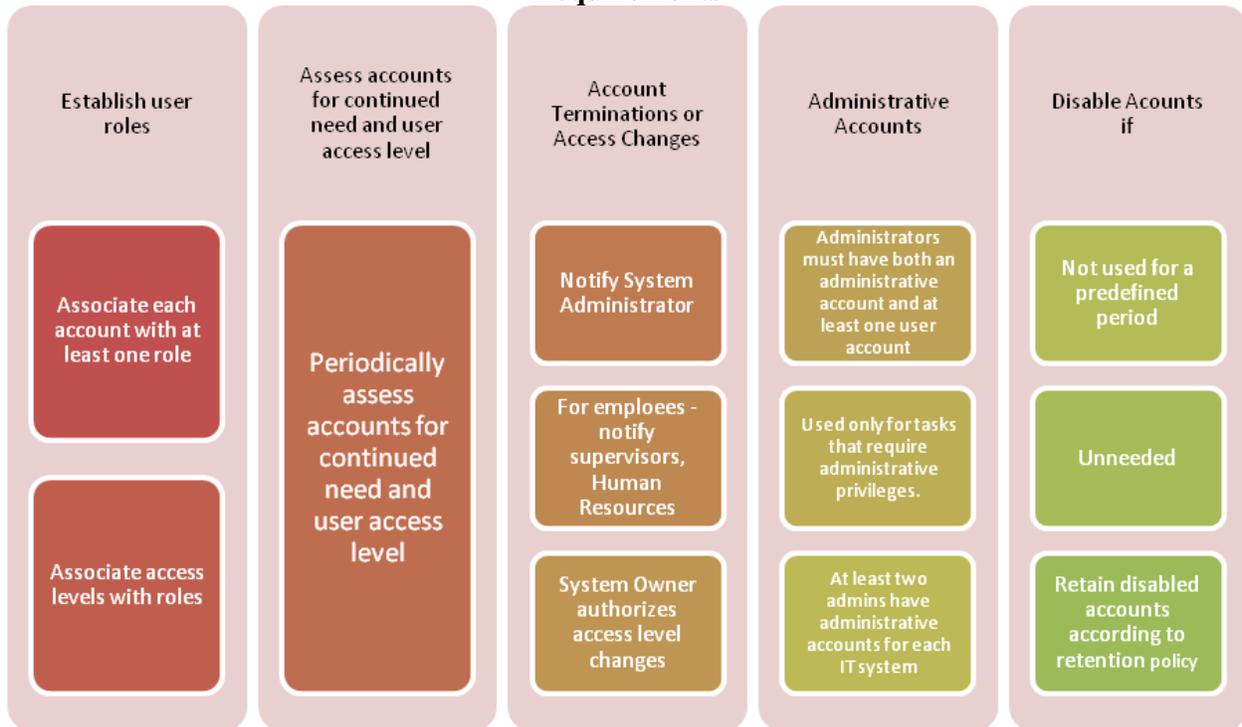
Before granting access to agency IT systems and data, agencies must have documentation of the access request. For IT systems with sensitivity of medium and higher, the request must be approved by the System Owner, and, for internal systems, by the user's supervisor. While the System Owner approves the request based on need to know relative to the data, the user's supervisor approves the request based on job requirements. Appendix B contains an example and template for an Access Request / Authorization.

### **2.2.4 Prohibition of "Guest" or Shared Accounts**

Individual accountability is essential for IT systems security. Agencies must not authorize the creation of accounts that can be used anonymously or by more than one person. A guest account enables anonymous access to an IT system, while a shared account (or shared password) hides individual accountability within a group. Both types of accounts, and the sharing of passwords or other logical access methods, are prohibited.

## **2.3 Account Maintenance**

Established accounts require maintenance on a continuous basis to strengthen IT security. Accounts must be validated periodically to determine if the access is still necessary and meets the requirements of least privilege. If not, the access level must be changed or the account disabled / deleted. Agencies should document policies and procedures for the account maintenance activities and requirements described in Figure 5.

**Figure 5 - Account Maintenance Activities and Requirements**

### 3 Password Management

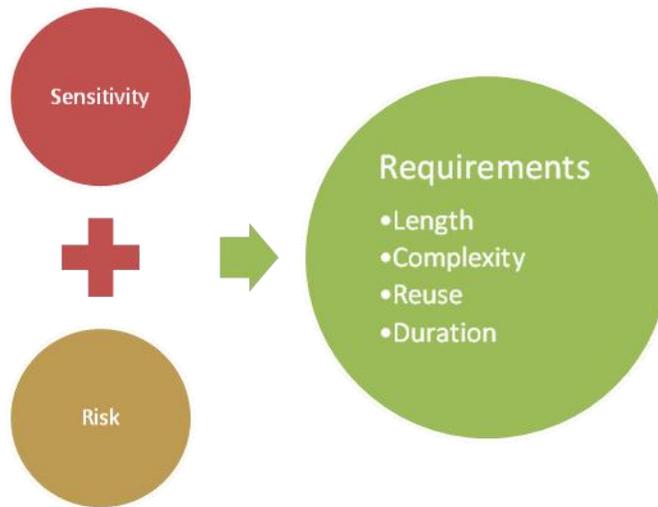
Passwords are required for accounts on sensitive COV IT systems and recommended for access to all COV IT systems. Agencies must document their password management policies and procedures. These policies and procedures must include requirements for:

- Password complexity;
- Secure delivery of new passwords to users;
- User activities to keep passwords secure;
- Password administration;
- Responding to lost, stolen or compromised passwords;
- Resetting passwords;
- Session controls; and,
- Changing vendor default passwords.

### 3.1 Password Requirements

Agencies must document password length, complexity, duration, and reuse requirements according to risk and sensitivity. Agency-wide password requirements should be documented in agency policies and procedures; password requirements for each IT system should be documented in policies and procedures for the IT system. These password characteristics are defined in Table 2.

**Figure 6 - Password Requirements**



In accordance with IT security best practice, agencies should require passwords that:

- Are at least eight characters long;
- Contain letters, numbers, and special characters;
- Are forced to be changed at least every 90 days<sup>2</sup>;
- Are not reusable for at least 12 months<sup>3</sup>; and
- Are masked during entry and encrypted during transmission and storage.<sup>4</sup>

Most operating systems have configurable password generators that will enable the IT system to generate passwords that conform to these requirements in accordance with the System Owner's

<sup>2</sup> Each agency should set password expiration frequency policy for each IT system based on the sensitivity and risk of the system, which may require password changes more often than every 90 days.

<sup>3</sup> Each agency should set password reuse policy for each IT system based on the sensitivity and risk of the system, which may require prohibiting and preventing password reuse for more than 12 months.

<sup>4</sup> All IT security frameworks require the use of passwords; these password complexity requirements are based on review of the requirements of numerous public and private sector organizations.

password policy for each IT system. Table 2 below explains password requirement terms in more detail.

**Table 3 - Password Requirement Terms**

Length:	The minimum and maximum number of characters allowed in the password
Complexity:	The variety of characters required or allowed in the password. Character variety includes letters, numbers, and symbols (e.g. %, \$, _). A password containing upper and lower-case letters, numbers, and symbols is the most complex.
Reuse:	The amount of time that must pass before a previous password may be reused. Limiting reuse reduces risk by preventing users from repeatedly using the same one, two or three passwords.
Duration:	The maximum amount of time that may pass before a user is required to establish a new password.

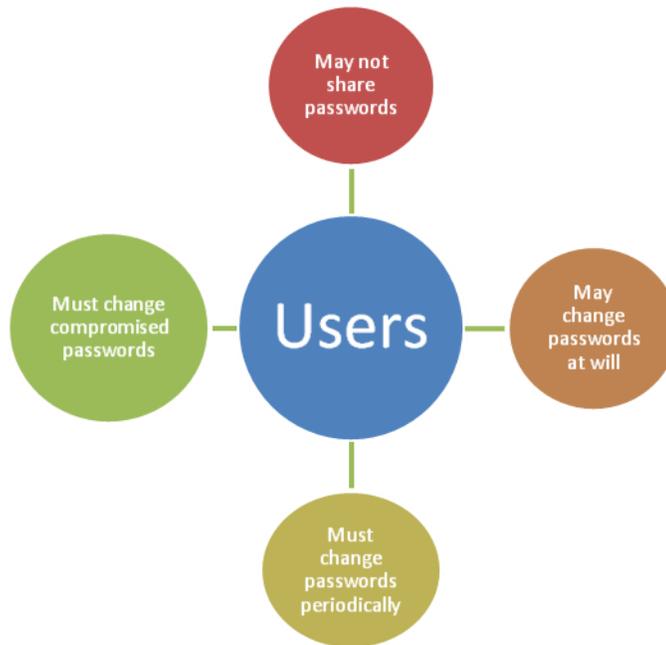
### 3.2 Initial and Replacement Passwords

Agencies should document policies and procedures for delivery of initial and replacement passwords. Any new password administratively provided to a user (either for initial use or as a replacement) must be unique. In this context “unique” means the password cannot be common to any two or more new users (e.g. the agency or IT system name, or “abc123”), nor can it be derived from public information (e.g. the user’s last name and phone extension.) The best practice is to use a password generator configured to the password policy of the IT system. Initial or replacement passwords must be securely delivered to the user and the user must be required to change the initial or replacement password immediately upon its first use.

### 3.3 User Management of Passwords

Agencies must document the responsibilities that users of IT systems have for the management of passwords. In particular, agency policy must reflect the characteristics shown in Figure 7. Users must agree to the responsibilities prior to being granted access.

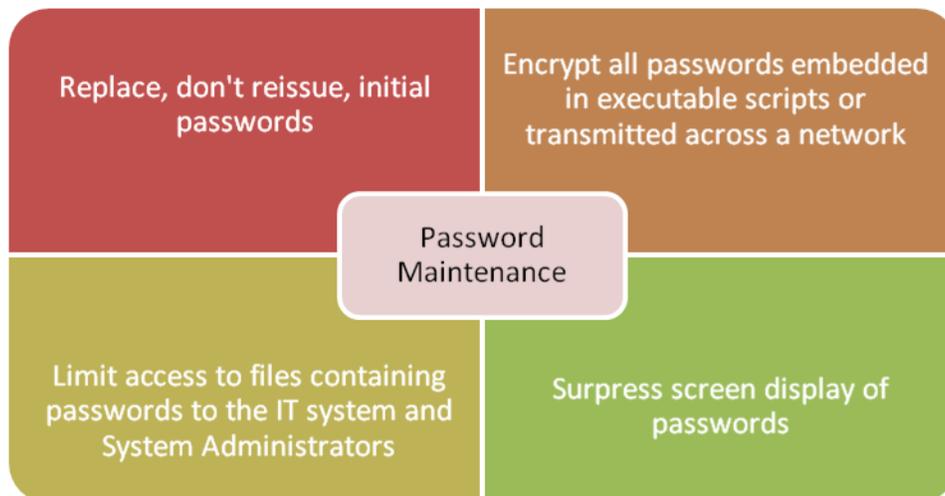
**Figure 7 - User Password Management Responsibilities**



### 3.4 Password Maintenance

System Owners must document password maintenance practices to be followed by System Administrators for each IT system. At a minimum, these practices must encompass those listed in Figure 8.

**Figure 8 - Password Maintenance Requirements**



### 3.5 Lost, Stolen, Compromised Passwords

Agencies must document procedures for dealing with lost, stolen, or otherwise compromised passwords. At a minimum these procedures must require users to:

- Immediately report, to the ISO, the loss, theft, or compromise of passwords; and
- Immediately change their password, if compromised.

Agencies should establish and adhere to consistent, secure processes for verifying user identity before providing a replacement password.

### 3.6 Password Reset Process

Agencies should document policies and procedures for resetting user passwords. These policies and procedures should require that users authenticate their identities before having their passwords reset. Where possible and where required by IT system or data sensitivity, agencies should document policies that require:

- Verification of the user's identity prior to delivery of the reset password to the user;
- Logging delivery of the reset password; and
- The user to change the reset password on first use.

In many cases, agency requirements will require that users be able to request and receive password resets by means of a telephone call to a help desk. In such cases, hand delivery of the reset password to the user may not be practicable. In these cases, agencies should document policies that require verification of the user's identity via information known only to the help desk and the user, in addition to the other requirements described above.<sup>5</sup>

### 3.7 Session Controls

Agencies should document session controls to prevent the compromise of passwords and the unauthorized use of established accounts. Agencies should adopt session controls commensurate with sensitivity and risk; at a minimum these controls should:

- Lock user accounts after no more than three unsuccessful login attempts in a row and delay login for no less than 30 minutes, or require an administrator to reset the account before allowing login<sup>6</sup>.

---

<sup>5</sup> A "secret" question and answer, defined by the user, recorded in the user's profile by the help desk are often used for this purpose.

<sup>6</sup> Agencies should consider the potential for denial-of-service attacks that intentionally lock many user accounts before determining whether to delay login or require administrator account reset after a series of unsuccessful login attempts.

- Lock user sessions after inactivity of no more than 10 minutes until the user reestablishes access using appropriate identification and authorization procedures (i.e. user ID and password); and
- Terminate user sessions after inactivity of no more than 60 minutes.

### **3.8 Default Vendor Passwords**

IT hardware and software products are often supplied with default passwords that are set by the vendor. To protect against compromise of IT systems and data by means of these passwords, agencies should document policies and procedures that require default vendor passwords to be changed before IT hardware and software is placed into production.

## **4 Remote Access**

Remote Access to sensitive IT systems and data may present serious risks to the agency. Agencies must document the policies and procedures to manage these risks.

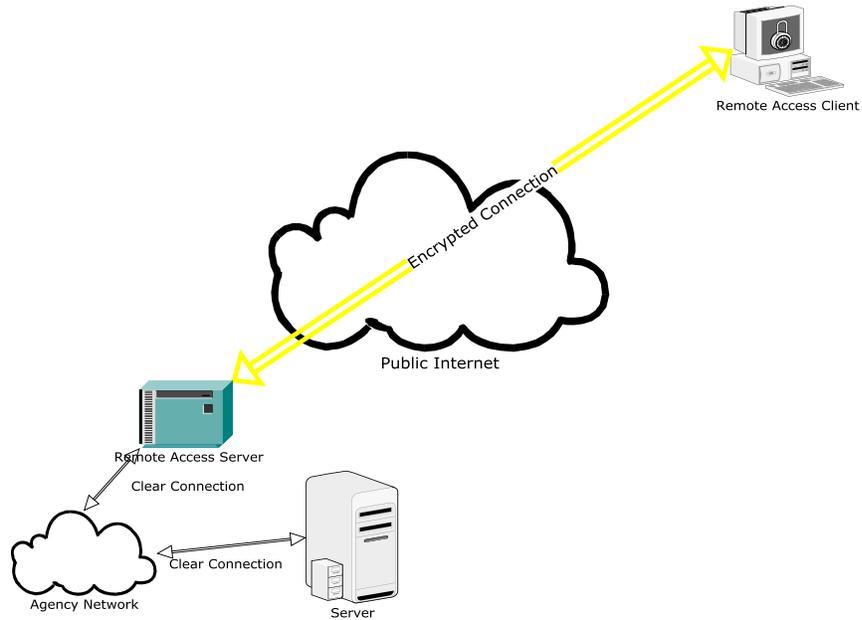
### **4.1 Encryption of Remote Access Sessions**

All remote access to sensitive IT systems and data must be encrypted. The encryption must begin with the initiation of the session, include all user identification and authentication, and not end until the session is terminated.

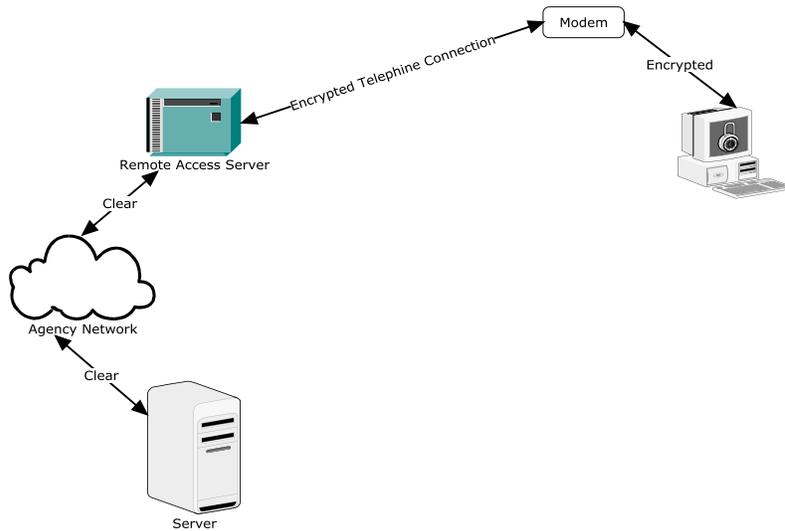
#### **4.1.1 Remote Access Encryption Techniques**

The two most widely used remote access encryption techniques are Virtual Private Networks (VPNs) and link encryption. VPNs are primarily used when the remote access occurs through an open network, such as the Internet, while link encryption is used primarily when the remote access occurs through a closed network, such as a dial-up connection. Figures 9 and 10 illustrate these two remote access methods.

**Figure 9 - VPN Remote Access**



**Figure 10 - Link Encryption**



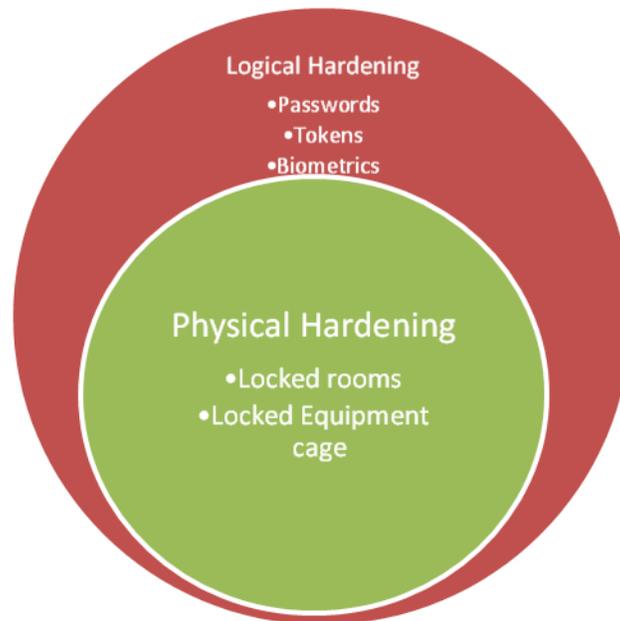
The administration of specific remote access technologies is beyond the scope of this guideline. Agencies are advised to seek detailed guidance on securing remote access from third-party remote access providers or vendors of the remote access solutions. Additional general information regarding remote access encryption is available from CERT ([www.cert.org](http://www.cert.org)), the

SANS Institute ([www.sans.org](http://www.sans.org)), and the National Institute of Standards and Technology ([www.nist.gov](http://www.nist.gov)), among others.<sup>7</sup>

## 4.2 Remote Access Service Hardening

Equipment providing remote access services must be hardened physically (e.g. stored in lockable spaces) and logically (e.g. access protected with passwords, tokens, etc.), as depicted in Figure 11. These protections increase the security of the implemented remote access solutions.

**Figure 11 - Remote Access Equipment Hardening**



## 4.3 Remote Access Records

Agencies must maintain auditable records of remote access attempts and sessions. Because of transaction volumes, these logs should be automatically generated; most remote access solutions provide this capability. Agencies must protect these logs as sensitive information.

## 4.4 Training

Users must be trained on the agency remote access policies and procedures prior to receiving remote access authorization.

## 5 Agency Policies, Procedures, and Exception Process

Agencies must develop policies and procedures to meet the logical access control requirements of the Policy and Standard. Agencies should develop policies and procedures

---

<sup>7</sup> These hyperlinks are current as of December 2006.

to implement the recommendations of this Guideline and to document a process for exceptions to agency policies and procedures. This process should document Agency Head approval and periodic review of all exceptions.

## **Appendix A – Information Security Access Agreement Template and Example Example**

### **Information Security Access Agreement**

As a user of the computer systems which are operated by the Virginia Department of Regulatory Management (DRM), I understand and agree to abide by the following terms which govern my access to and use of the processing services of DRM:

Access has been granted to me by DRM as a necessary privilege in order to perform authorized job functions. I am prohibited from using or knowingly permitting use of any assigned or entrusted access control mechanisms (such as log-in IDs, passwords, terminal IDs, user IDs, file protection keys or production read/write keys) for any purpose other than those required to perform my authorized employment functions;

If, due to my authorized job functions, I require access to other information on DRM’s computer systems, I must obtain authorized access to that information from the Data Owner;

I will not disclose information concerning any access control mechanism of which I have knowledge unless properly authorized to do so by DRM, and I will not use any access mechanism which has not been expressly assigned to me;

I agree to abide by all applicable Commonwealth of Virginia and DRM policies, procedures and standards which relate to the security of DRM computer systems and the data contained therein;

If I observe any incidents of non-compliance with the terms of this agreement, I am responsible for reporting them to the information security officer and management of DRM as well as to the Office of the Chief Information Security Officer of the Commonwealth;

**By signing this agreement**, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that any infractions of this agreement will result in disciplinary action, including but not limited to the termination of my access privileges

\_\_\_\_\_  
**Employee/Consultant Name (Print)**

\_\_\_\_\_  
**Date**

\_\_\_\_\_  
**Employee/Consultant Signature**

Department of Regulatory Management  
**Agency Name**

\_\_\_\_\_  
**Division Name**

# Template

## Information Security Access Agreement

As a user of the computer systems which are operated by the *(agency name and acronym)*, I understand and agree to abide by the following terms which govern my access to and use of the processing services of *(agency acronym)*:

Access has been granted to me by *DRM* as a necessary privilege in order to perform authorized job functions. I am prohibited from using or knowingly permitting use of any assigned or entrusted access control mechanisms (such as log-in IDs, passwords, terminal IDs, user IDs, file protection keys or production read/write keys) for any purpose other than those required to perform my authorized employment functions;

If, due to my authorized job functions, I require access to other information on *(agency acronym)*'s computer systems, I must obtain authorized access to that information from the Data Owner;

I will not disclose information concerning any access control mechanism of which I have knowledge unless properly authorized to do so by *(agency acronym)*, and I will not use any access mechanism which has not been expressly assigned to me;

I agree to abide by all applicable Commonwealth of Virginia and *DRM* policies, procedures and standards which relate to the security of *(agency acronym)* computer systems and the data contained therein;

If I observe any incidents of non-compliance with the terms of this agreement, I am responsible for reporting them to the information security officer and management of *(agency acronym)* as well as to the Office of the Chief Information Security Officer of the Commonwealth;

**By signing this agreement**, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that any infractions of this agreement will result in disciplinary action, including but not limited to the termination of my access privileges

*(employee/consultant name)* \_\_\_\_\_  
**Employee/Consultant Name (Print)**

*(date)* \_\_\_\_\_  
**Date**

*(employee/consultant signature)* \_\_\_\_\_  
**Employee/Consultant Signature**

*(agency name)* \_\_\_\_\_  
**Agency Name**

*(division name)* \_\_\_\_\_  
**Division Name**

## **Appendix B – Access Request / Authorization Form Template and Example Example**

# Template

## IT System Access Form

Date: \_\_\_\_\_

Name: \_\_\_\_\_

Department: \_\_\_\_\_

Phone: \_\_\_\_\_

E-mail: \_\_\_\_\_

IT systems on which access is required:

System Name:			
User Role			
System Administrator:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data Administrator:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group Manager:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Applicant's Signature

\_\_\_\_\_  
/

Authorized By  
User's Supervisor (print/sign)

\_\_\_\_\_  
/

Authorized By  
System Owner (print/sign)

Comments: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_