COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

INFORMATION TECHNOLOGY PERSONNEL SECURITY 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 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	02/15/2008	New

Publication Designation
ITRM IT Personnel Security Guideline

Subject
Information Technology Personnel Security

Effective Date
02/15/2008

Scheduled Review
One (1) year from effective date

Authority
Code of Virginia § 2.2-603(F)
(Authority of Agency Directors)

Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; "VITA;" Appointment of Chief Information Officer (CIO))

Scope
This *Guideline* is offered as guidance to all executive, legislative, and judicial branch and independent State agencies and institutions of higher education (collectively referred to as "Agency").

Purpose
To guide Agencies in the implementation of the information technology personnel security requirements defined by ITRM Standard SEC501-01, Section 8.

General Responsibilities
(Italics indicate quote from the Code of Virginia)

Chief Information Officer
In accordance with *Code of Virginia* § 2.2-2009, the Chief Information Officer (CIO) is assigned the following duties: *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. Such policies, procedures, and standards will apply to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education."*

Chief Information Security Officer
The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth of Virginia's IT systems and data.

IT Investment and Enterprise Solutions Directorate
In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the IT Investment and Enterprise Solutions Directorate the following duties: *Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions*."

All Executive, Legislative, and Judicial Branch and Independent State Agencies
In accordance with §2.2-2009 of the *Code of Virginia,*, all executive, legislative, and judicial branch State agencies and institutions of higher education 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 to provide for the security of state government electronic information from unauthorized uses, intrusions or other security threats.

Definitions
Agency - All executive, legislative, and judicial branch and independent State agencies and institutions of higher education.

Alford plea - A plea in criminal court. In this plea, the defendant does not admit the act and asserts innocence, but admits that sufficient evidence exists with which the prosecution could likely convince a judge or jury to find the defendant guilty.

CISO - Chief Information Security Officer – The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of Commonwealth of Virginia (COV) IT systems and data.

Data - An arrangement of numbers, characters, and/or images that represent concepts symbolically.

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.

Electronic Information - Any information stored in a format that enables it to be read, processed, manipulated, or transmitted by and IT system.

Government Electronic Information - Electronic information owned or held by COV.

ISO – Information Security Officer - The individual designated by the Agency Head to be responsible for the development, implementation, oversight, and maintenance of the agency's IT security program.

Information Technology (IT) - Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Security - The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality.

Information Technology (IT) Security Audit - An independent review and examination of an IT system's policy, records, and activities. The purpose of the IT security audit is to assess the adequacy of IT system controls and compliance with established IT security policy and procedures.

Least Privilege - The minimum level of data, functions, and capabilities necessary to perform a user's duties.

Sensitive Data - Any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled.

Sensitive IT Systems - COV IT systems that store, process, or transmit sensitive data.

Separation of Duties - Assignment of responsibilities such that no one individual or function has control of an entire process. It is a technique for maintaining and monitoring accountability and responsibility for IT systems and data

System Owner - An agency Manager, designated by the Agency Head or Information Security Officer, who is responsible for the operation and maintenance of an agency IT system.

Related ITRM Policy and Standards

ITRM Policy, SEC500-02: Information Technology Security Policy (Revised 07/01/2007)
ITRM Standard SEC501-01: Information Technology Security Standard (Revised 07/01/2007)
ITRM Standard SEC502-00: Information Technology Security Audit Standard (Revised 09/01/2006)

TABLE OF CONTENTS

1 Introduction

1.1 Information Technology Security

This Guideline presents a methodology for Information Technology (IT) personnel security 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 personnel security 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 Personnel Security

In the context of IT security, personnel security comprises administrative activities which restrict access to IT systems and data to Commonwealth employees, contractors, and visitors who require access to these systems to meet a business need. IT personnel security requirements create a foundation that allows management to instruct authorized users in their IT security responsibilities and in the acceptable uses of COV IT systems and data. The Standard describes personnel security requirements in the following three areas:

- Access Determination and Control
- Security Awareness and Training
- Acceptable Use

1.3 Roles and Responsibilities

Agencies must designate, in writing, an individual to be responsible for administering the agency's IT security program, including its IT personnel security components. It is recommended this responsibility be assigned to the agency Information Security Officer.

Effective IT personnel security controls include the careful selection of personnel in the hiring and contracting processes as these controls play an integral role in maintaining effective IT personnel security standards. Therefore, it is important that all IT personnel security efforts be closely coordinated with each agency's human resources and supply chain management organizations.

2 Access Determination and Control

Access Determination and Control requirements support an agency's overall IT security program, of which IT Personnel Security is a part, by restricting access to IT systems and data only to authorized personnel. These requirements include:

- Background Investigations – Evaluating the work and personal history of an individual to determine if they are a suitable candidate for a role that requires access to sensitive IT systems and data;
- Facility Access Restrictions – Providing adequate controls to protect IT systems and data from unauthorized access;
- Non-Disclosure and IT Security Agreements – Obtaining agreement from users of IT systems and data to restrictions and responsibilities for their use, based on sensitivity and risk;
- Termination or Transfer of Access – Protecting IT systems and data through termination and transfer practices that require return of agency logical and physical assets that provide access to IT systems and data, when appropriate.
- Separation of Duties – Protecting IT systems and data so that no one individual or function has control of an entire process; and
- Least Privilege – Protecting IT systems and data so that users have only the minimum access rights necessary to fulfill their responsibilities.

Some Access Determination and Control requirements within the IT Personnel Security section of the Standard are complementary to requirements of the Standard related to Logical Access Control and Facilities Security. The differences among these requirements are primarily related to their focus:

- Access Determination and Control requirements within IT Personnel Security focus on security controls to which users of IT systems and data are subject;
- Logical Access Control requirements focus on security controls to which IT system accounts are subject; and
- Facilities Security requirements focus on security controls to which facilities that house IT systems and data are subject.

2.1 Background Investigations

Background investigations conducted during the process of evaluating whether an individual is an appropriate candidate for a role that requires access to internal COV IT systems and data are an important part of IT personnel security. These individuals may be employees, contractors, volunteers, or interns. Verifying the backgrounds of these individuals who will have access to COV internal IT systems and data through background investigations increases the likelihood that these individuals will adhere to the agency's IT security policies, standards, and procedures. This likelihood, in turn, facilitates the protection of agency IT systems and data commensurate with sensitivity and risk.

The nature and scope of these background investigations will vary from role to role, and from agency to agency. In developing an agency policy regarding background investigations, agencies should consult the:

- *Code of Virginia* § 2.2-1201.1 (http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-1201.1); and
- Department of Human Resource Management (DHRM) Policy Number 2.10 (http://www.dhrm.virginia.gov/hrpolicy/web/pol2_10.html)[1].

[1] These hyperlinks are current as of December 2007.

Additional details on COV policy regarding background investigations and other reference checks may be found in the DHRM *Human Resource Management Manual*, Chapter 11, Recruitment and Employment (http://www.dhrm.virginia.gov/resources/hrmanual.pdf)[2]. In addition, several COV agencies have background investigation requirements mandated by the *Code of Virginia*. Each agency must determine which internal and external requirements apply to it, and document appropriate policies, standards, and procedures to meet these requirements.

In addition, the provisions of § 2.2-1201.1 of the *Code of Virginia* apply only to "any final candidate for a position that has been designated as sensitive", while the background investigation provisions of DHRM Policy Number 2.10 apply only to "background checks prior to employment". Agencies are advised to adopt mitigating controls to compensate for existing employees whose background may have changed since it was investigated, or who may have joined the agency when different background investigation policies were in effect.

As an alternative, agencies may wish to consult with the Office of the Attorney General regarding development of policies for conducting background investigations of existing employees. Some agencies have adopted policies that require a background investigation for any employee who undergoes a personnel action while in the employment of the agency that involves the employee assuming a position classified as sensitive under § 2.2-1201.1 of the *Code of Virginia* , including promotion, demotion, lateral transfer, etc.

Moreover, agencies are strongly advised to coordinate development of background investigation policies, standards, and procedures with the agency human resources and supply chain management organizations.

Agencies may require background investigations for candidates for employment, contracting, volunteering, and internships. If agencies require background investigations for contractors, they should be aware that these requirements, in combination with other factors, may result in the agency being "considered the employer under provisions of the Fair Labor Standards Act and other laws and regulations."[3]

In order to avoid being considered the employer of contractors, agencies may wish to make the responsibility for conducting background investigations and evaluating the results part of the terms and conditions under which the staffing vendor provides the contractors to the agency. Another means of avoiding the appearance that the agency is the employer of contractors is to assign responsibility for conducting and evaluating the results of background investigations for employees and contractors to separate organizations within the agency. An agency, for example, could assign responsibility for employee background investigations to the agency human resources organization. Responsibility for contractor background investigations could be assigned to the agency's purchasing or supply chain management organization.

[2] This hyperlink is current as of December 2007.
[3] DHRM *Human Resource Management Manual,* Appendix C, p. 5.

2.1.1 Types of Background Investigations

Agencies should base the types of background investigations they conduct on the role which an individual will assume, and the access to sensitive IT systems or data required to fulfill the responsibilities of that role. For sensitive systems, background investigations should be conducted prior to the individual's assuming the role that requires this access. The form of background investigation conducted should be determined by the agency, based on the type, sensitivity, and risk of the IT system(s) and/or data to which the individual will have access.

These investigations may vary according to the nature of the role, and can include review or verification of the individual's:

- Academic record;
- Licenses and certifications;
- Employment history and references;
- Financial history and status;
- Credit reports;
- Criminal history;
- Driving record; and/or
- Other records or information related to the individual's suitability for the position.

Agencies are urged to:

- Conduct criminal background checks for all authorized users of internal COV IT systems, and especially for IT personnel;
- Conduct credit checks for roles in procurement, accounting, and roles that require access to systems with fiduciary responsibility, or which contain personally identifiable information on individuals.

2.1.2 Evaluating Information Obtained through Background Investigations

Unfavorable information regarding an individual obtained through background investigations does not necessarily bar a candidate a role requiring access to sensitive IT systems and data. Based on an assessment of the following COV best practices, each agency should develop its own criteria for evaluating information obtained through background investigation that consider, at a minimum:

1. The individual's suitability for the role;
2. How recent an event is documented by the unfavorable information; and
3. The relationship between the unfavorable information and the role for which the individual is being considered.

Criminal Convictions

A criminal conviction does not bar an individual from a role within an agency. Agencies, however, are advised not to assign individuals to roles that require access to sensitive systems if

they have a criminal conviction for, an Alford plea[4] or plea of *nolo contendere* (no contest) to, and/or outstanding warrants or charges pending disposition within the last five (5) years for:

1. Any felony within the past ten (10) years;
2. A misdemeanor involving moral turpitude within the past five (5) years;
3. Multiple misdemeanors, depending on type within the past five (5) years;
4. Any violent sex offense, irrespective of when the offense occurred;
5. Any violent crime, irrespective of when the crime occurred;
6. Crimes indicating serious financial misjudgment and/or irresponsibility, irrespective of when the crimes occurred; and/or
7. Felony possession, distribution, or manufacture of drugs, irrespective of when the crime occurred.

Employment History, Personal History, Education, and Certification

Agencies are advised not to assign individuals to internal IT user roles if background investigations reveal:

1. Any material misrepresentation of facts regarding employment history, criminal history, or degrees or certifications held; and/or
2. Poor references.

Credit History

Agencies are advised not to assign individuals to roles, particularly if the individual would have fiduciary responsibilities or the ability to compromise information for monetary gain, if background investigations reveal recent:

1. Bankruptcy (or current bankruptcy proceedings);
2. Loan default and/or foreclosure; and/or
3. Court judgments.

If an agency conducts a credit check on an individual, the agency should also evaluate the following, in conjunction with other information, to determine the individual's suitability for the proposed role:

1. Number of credit inquiries;
2. Number of credit rejections;
3. History of late payments;
4. Past due and/or unpaid payments;
5. Repossessions; and/or
6. Garnishments.

DMV Driving Record

[4] A plea in criminal court in which the defendant does not admit the act and asserts innocence, but admits that sufficient evidence exists with which the prosecution could likely convince a judge or jury to find the defendant guilty.

If driving is a bona fide requirement of the role, agencies are advised not to assign individuals to the role if background investigations reveal:

1. Lack of a valid Motor Vehicle Operator's license.
2. Lack of Commercial Driver's License (CDL) and/or special endorsements, if required for the position.
3. Excessive demerit points.
4. Any conviction for Driving under the Influence (DUI) within the last five (5) years.

Other Background Investigations

Depending on the nature of the position, agencies may wish to conduct additional background investigation, and to reject individuals if these checks indicate they are unsuitable for the role for which they are being considered. These additional background checks include:

1. State and Federal tax records;
2. Food stamp history; and
3. Other agency clearance investigations, including those required by the Virginia State Police and the U.S. Department of Defense

2.2 Facility Access Restrictions

Legitimate business needs require access to facilities which house IT systems or data. Agencies must, therefore, establish practices that control the access to such facilities. As stated in the Standard, agencies must restrict access to facilities that house sensitive IT systems and data, at a minimum. Agencies are advised to apply these controls to all facilities that house agency IT systems and data.

2.2.1 Determining Access Requirements

It is a best practice to limit access to all facilities that house IT systems and data on the basis of least privilege, allowing access only in order to meet a documented agency business need. For example, systems engineers and vendor hardware support personnel may require occasional access to facilities that house IT systems data, in order to make repairs to or upgrade IT system hardware.

To restrict access to facilities that house IT systems and data to situations that meet a documented agency business need, agencies should create written policies and procedures to govern visitor access. For agencies whose business needs do not require frequent access to facilities that house agency IT systems and data, the policy and procedures might be quite simple. An example of a policy that may meet the needs of smaller agencies may be found in Appendix A. For agencies whose business needs necessitate frequent visits to facilities that house agency IT systems and data, a more comprehensive and customized policy and set of procedures is strongly recommended.

Recommended practices to govern visitor access to facilities housing IT systems and data include:

- Logging all entrances and departures;
- Logging all equipment brought into and removed from the facility;

- Verifying identity of individuals accessing the facility by means of a government-issued photo identification card (drivers license, state ID card, military ID);
- Actively monitoring access logs to ensure each arrival entry has a corresponding departure entry, and that no equipment leaves the facility that was not brought in;
- Requiring an agency employee to escort all visitors at all times;
- Prohibiting use of personal data storage devices, such as USB drives; and
- Prohibiting use of cameras, except with written agency Head approval.

2.2.2 Logging Access

Agencies should log all arrivals and departures, regardless of their purpose. Depending on the agency's requirements and capabilities, access logs can be paper-based or electronic. Regardless of the format, access log files must be retained for a minimum of six months after last entry or use in accordance with General Schedule Number 108, Series Number 012273, of the Library of Virginia's *Records Retention and Disposition Schedule*. An example paper access log and template may be found in Appendix B.

2.2.3 Monitoring Access Logs

At a minimum, it is recommended the agency policy require daily review of access logs. If a substantial number of individuals access the facility, more frequent reviews will provide enhanced security. Log monitoring can be as simple as reviewing the log once at the end of each day to verify that each entry into the facility documented in the log has a corresponding exit documented in the log.

2.3 Non-Disclosure and IT Security Agreements

As stated in the Standard agencies must require non-disclosure and IT security agreements for access to IT systems and data, based on sensitivity and risk. Non-disclosure and IT security agreements, which may be combined, should be customized to the specific agency business requirements and situation. These agreements should be signed by users prior to access to IT systems and data being granted. Examples of a template for a combined Non-Disclosure and IT Security Agreement can be found in Appendix C.

Non-disclosure and security agreements have three objectives:

- Educating the signer about agency restrictions on the release or communication of specific agency information;
- Educating the signer about his or her responsibilities to protect the security of agency information, IT systems, and data; and
- Contractually binding the signer to support those restrictions.

Agencies should require each individual subject to non-disclosure and/or IT security agreement to reaffirm these agreements no less than once every two years, or more often, based on sensitivity and risk. Agencies may wish to make reaffirmation of these agreements part of the annual IT Security Awareness training (see Section 3) or as part of the annual review process.

In executing the reaffirmation of these agreements, however, agencies should provide a process that requires all individuals subject to these agreements to reaffirm them. Using the IT Security Awareness training for this purpose will not require individuals (such as contract cleaning crews)

who are not IT system users to reaffirm their non-disclosure agreements, while the annual review process will not require reaffirmation of agreements by non-employees.

2.4 Termination and Transfer of Access

Access to IT systems and data should be granted only while a business need exists. Should the business need for an individual's access to IT systems and data cease, their access must be terminated immediately.

In addition to playing a key role in IT Personnel Security, access termination and transfer procedures are a key element of the Logical Access Control and Physical Security portions of each agency's IT security program. Agencies must document practices and procedures for situations such as termination of employment for cause, organizational realignment, or transfer of duties that provide for the:

- Immediate termination of all physical and logical access; and
- Require return of agency logical and physical assets that provide access to sensitive IT systems and data and the facilities that house them.

Such logical and physical assets include, but are not limited to:

- Software;
- Laptop computers;
- Personal Digital Assistants (PDAs);
- Cellular Telephones;
- Security tokens; and
- Access badges.

Agencies are required by the Standard to apply these controls to sensitive IT systems and data and the facilities that house them. In addition, agencies are advised to apply these controls to all IT systems, data, and facilities.

2.5 Separation of Duties

Agencies should base their policies and procedures for access determination and control on the principle of separation of duties, especially for personnel whose job functions include regular access to and/or processing of sensitive data. Separation of duties requires assignment of responsibilities so that no one individual or function has control of an entire process. Separation of duties helps control collusion, and can make some security compromises more difficult to execute or hide. Separation of duty best practices that enhance IT security includes:

- Review of operations logs by non-operations personnel;
- Assignment of security administration and system administration responsibilities to different employees or contractors;
- Organization of responsibilities so that system administrators do not report to the Information Security Officer (ISO);
- Establishing role based access control in which privileges and access levels to sensitive IT systems are assigned to specifically named roles, with specific users associated with specific roles. Role based access control lessens the complexity of managing user rights

and privileges to agency IT systems. Roles must be carefully assigned to ensure that no one role has excessive privileges;

- Utilizing identity and access management activity reporting which inform IT security managers of the following:
    a. What each user has access to;
    b. Activities of each user; and
    c. Reporting of separation of duties violations, remediation activities, and exceptions;
- Use of user lock-out, which automatically locks a computer workstation or terminal after a pre-determined amount of inactivity; and
- Logging of all role creation, user assignments, and privilege activity.

Separation of duties can be greatly enhanced by conducting in-depth process mapping and risk assessments of all business processes (including data flows and transactional flows), and the participating organizational entities that participate in those processes. Business process mapping and process risk assessments support separation of duties efforts by:

- Identifying possible areas of fraudulent or illegal activity;
- Identifying areas lacking in proper separation of duties controls;
- Identifying risk areas that are adequately controlled and must remain so; and
- Evaluating the effectiveness of existing separation of duties controls.

When complete separation of duties is not possible for a given activity, recommended compensating controls include:

- Increased supervisory review;
- Reduced span of control;
- Rotation of assignments;
- Independent monitoring or auditing; and
- Time-delimited, specific access authorization with audit review.

In addition, where lack of separation of duties prevents the agency from complying with a requirement of the *COV ITRM IT Security Standard (ITRM Standard SEC501-01)*, the agency must request an exception to the requirement from the CISO. The exception request must document:

- The business need;
- The scope and extent;
- Mitigating safeguards;
- The specific duration; and
- Agency Head approval.

More information regarding the exception request process is contained in section 1.5 of SEC501-01 and in the Appendix of SEC501-01.

Agencies are required by the Standard to apply controls based on separation of duties to sensitive IT systems and data. In addition, agencies are advised to apply these controls to all IT systems and data.

2.6 Least Privilege

Agencies should develop their policies and procedures for access determination and control in accordance with the principle of least privilege. The principle of least privilege grants the minimum level or scope of access that enables an individual to perform his/her agency required functions and business processes. Agencies are required by the Standard to apply the rule of least privilege in granting logical and physical access to sensitive IT systems and data. In addition, agencies are advised to apply this rule in granting logical and physical access to all IT systems and data.

In addition to the logical and physical access elements of the principle of least privilege, agencies should also consider applying least privilege time restrictions. Least privilege time restrictions dictate that a user should be granted the minimum amount of time required to performs his/her required functions and business processes. Variations of least privilege time restrictions include:

- Restricting a user's access to a sensitive IT system to specific working hours only;
- Restricting a user's access to a sensitive IT system to pre-determined time intervals (i.e. specific times of the day/week/month); and
- Restricting a user's access to a sensitive IT system only while the person fills a specific role in the agency.

Proper execution of the principle of least privilege is made possible only when agencies apply strong user authentication requirements on IT systems, commensurate with the system's sensitivity and risk. Effective user authentication requirements confirm that a user is who they say they are which helps to enforce the principle of least privilege. Authentication procedures for sensitive IT systems must provide the following assurances in order to properly support the principle of least privilege:

- A specific user ID must be available only to the anticipated user, and
- There must be singular ownership of system user IDs to ensure that activities associated with a user ID can be traced back to one user.

3 IT Security Awareness and Training

IT Security Awareness and Training provides IT system and data managers, system administrators, and users with awareness of IT system and data security requirements, and their responsibilities to protect COV IT systems and data. Agencies may wish to refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* in designing their IT Security Awareness and Training Program.

Agencies should conduct an initial IT Security Awareness and Training needs assessment to help determine the agency's high priority training requirements and to guide the strategic planning surrounding the agency's IT Security Awareness and Training program. An agency should update this needs assessment and its IT Security Awareness and Training program whenever available evidence indicates that the IT Security Awareness and Training program is not meeting its intended objectives. Such evidence may include:

- Findings and/or recommendations regarding the IT Security Awareness and Training program from IT Security Auditors;
- Conversations with agency management, System Owners, and other agency staff whose business functions rely on IT systems and data;
- IT security incidents, such as compromise of passwords, data security breaches, website defacements, and successful virus attacks; and
- Major changes to the agency's IT infrastructure and/or applications.

3.1 Program Requirements

At a minimum, the agency IT Security Awareness and Training program must support these requirements:

- Annual basic IT security training of all internal IT users;
- Additional role-based IT security training for agency employees, contractors, vendors, business partners, and third parties with special IT security responsibilities beyond those of all IT system users, as required, including:
  - System Owners, Data Owners, and System Administrators;
  - IT Disaster Recovery team members; and
  - IT Security Incident Response Team members.

In addition to basic and role-based IT security training, IT security awareness activities should be another key component of each agency's IT Security Awareness and Training program. IT security awareness activities reinforce the material presented in the basic IT security training that all IT users receive. The effectiveness of the overall IT Security Awareness and Training program depends on delivering IT security awareness messages not only through periodic training, but also through multiple channels and at a high frequency. Agencies are advised, therefore, to use several of the following delivery mechanisms in communicating with personnel regarding IT security awareness:

- Agency-wide messages;
- Agency Intranet pages;
- Posters;
- Agency newsletters;
- "Do and Don't" lists;
- Screensavers;
- Warning banners and messages;
- Web-based sessions;
- "Brown bag" seminars; and
- Information Security Day

The topic of these communications may involve any aspect of IT security, and will vary from agency to agency, based on each agency's needs. Suggested areas for emphasis, however, include:

- Creating and maintaining strong passwords;
- Effective practices for virus protection;
- Remote access and portable device security;
- Software patches and security settings on client systems;

- Software license restriction issues; and
- Laws and regulations controlling the use of state IT systems.

3.2 Program Responsibility and Administration

Each agency must designate an individual to be responsible for all aspects of an agency's IT Security Awareness and Training program including development, implementation, testing, training, monitoring attendance, and periodic updates. Some agencies will find it effective for this responsibility to be part of the ISO's role. Other agencies may wish to designate the manager or a staff member of the agency's organizational development and training function to fulfill this responsibility. Even if an individual other than the ISO is designated to fulfill this responsibility, the ISO remains accountable for the IT Security Awareness and Training program, as part of the agency's overall IT security program.

Administration of the agency IT Security Awareness and Training program must include:

- Providing basic IT security training to users before or soon after they receive access to agency IT systems and data;
- Monitoring and tracking of IT users receiving training; and
- Documentation of user acceptance of agency IT security policies, including the Acceptable Use policy.

3.3 Content Requirements

As stated in the Standard, the basic agency IT security training must, at a minimum, cover these topics over time:

- The agency's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
- The concept of separation of duties;
- Prevention and detection of IT security incidents, including those caused by malicious code;
- Proper disposal of data storage media;
- Proper use of encryption products;
- Access controls, including creating and changing passwords and the need to keep them confidential;
- Agency acceptable use policies;
- Agency Remote Access policies;
- Agency Telework policies; and
- Intellectual property rights, including software licensing and copyright issues.

It is further recommended that agency IT security training focus on information security threats that are often caused by the behaviors of IT system users, and are therefore avoidable. Focusing IT security training on avoidable behaviors helps agency IT system users to more fully understand the implications of their actions. Avoidable behaviors that should be emphasized include:

- Introducing a virus onto the agency's network;
- Releasing sensitive information to unauthorized parties; and
- Bypassing the firewall to enable testing, or to make access to certain information easier.

4 Acceptable Use

An "Acceptable Use" policy defines the authorized uses of agency IT systems. At a minimum, agencies must require their employees and other agency IT systems users to adhere to DHRM *Policy 1.75 – Use of Internet and Electronic Communication Systems.* Agencies must also supplement the policy as necessary to address the requirements of SEC501-01 and specific agency needs. The DHRM COV-wide policy may be found at http://www.dhrm.virginia.gov/hrpolicy/policy/pol1_75.pdf.[5]

4.1 Consent to Monitoring and Disclosure

As stated in the Standard, the agency Acceptable Use policy must inform users that their use of agency IT systems may be monitored, and that any data sent, received, processed, or stored may be accessed and disclosed.

4.2 Prohibited Uses

The agency Acceptable Use policy must prohibit the following actions:

- Using agency-owned or leased computer equipment to access, download, print or store any information infrastructure files or services having sexually explicit content, in accordance with the provisions of § 2.2-2827 of the *Code of Virginia.*
- Installing or using unauthorized encryption – all encryption used must be authorized by the agency ISO;
- Tampering with workstation security controls – users may not attempt to defeat installed security controls;
- Installing or using unauthorized software – all software used must be authorized by the agency ISO;
- Unauthorized hardware changes – users may not modify, attach, detach, add, subtract or make any other kinds of changes to the configuration of agency hardware without authorization by the agency ISO;
- Use of copyrighted and licensed materials unless the COV owns the materials or COV has otherwise complied with intellectual property laws governing the materials;
- Connecting unauthorized devices to agency IT systems or networks- including personal computers, laptops, or hand held devices; and
- Transmitting unencrypted sensitive data.

To promote security of its IT systems and data, agencies should implement network monitoring tools that support the enforcement of the prohibited uses listed above. Violations of the agency Acceptable Use policy (such as the downloading of prohibited applications) should be immediately identifiable and traceable, thus enabling rapid response to inappropriate and/or illegal user activity.

Some elements of the Acceptable Use policy will vary from agency to agency, based on the sensitivity and risk of each agency's IT systems and data. Each agency should consider how to most appropriately address the following items:

[5] This hyperlink is current as of December 2007.

- The agency Acceptable Use policy should address whether employees are permitted to use small, portable USB storage devices on agency IT systems. Agencies that operate systems containing highly sensitive information should consider restrictions on the use of small, portable USB storage devices, as these devices are extremely difficult to track and manage, thus increasing the possibility of loss or disclosure of sensitive information.
- The agency Acceptable Use policy should address acceptable use of the Internet on agency IT systems, including the use of personal e-mails accounts.

The Acceptable Use policy of each agency should include explanations of why certain activities are prohibited on the agency's IT systems. The more IT system users understand regarding the details and rationale of agency IT system prohibited uses, the more likely they are to adhere to those restrictions.

Appendices

These Appendices provide examples and templates that agencies may use to document their use of many of the methodologies described in this Guideline. Each template consists of:

1) An example of the document, completed with fictional information; and

2) A blank version of the template for use by COV agencies.

The examples use different fonts for instructions and example information, as follows:

- Times New Roman text is used for the template itself.
- **Shaded Arial Bold text** is example text.
- *Times New Roman Italic text* is provided as instructions for completing the template.

Appendix A – IT Facility Access Example and Template

DEPARTMENT OF CITIZEN SERVICES IT FACILITY ACCESS POLICY

Statement of Policy

IT is the policy of the **Department of Citizen Services (DCS)** that access to **DCS** facilities that house IT systems and data is restricted to individuals who have a legitimate business need for such access. Legitimate business needs include a primary work assignment to a **DCS** facility that house IT systems and data or access to a **DCS** facility that house IT systems and data to fulfill job responsibilities.

Visitor Sponsorship and Escort

A **DCS** employee or contractor must sponsor all visitor access to the facility, and must escort the visitor at all times. Both the visitor and the escort must sign the Facility Access log which will note the day and time of arrival, purpose of visit, and time of departure. Escorts will monitor visitor actions and will prevent visitors from connecting flash drives or other portable storage to **DCS** IT systems or from using cameras during the visit, unless such use has been approved by the Information Security Officer.

Access Logs

Access logs must be reviewed daily by the **security guard** to ensure all entries have a corresponding exit time. The **security guard** must verify the each individual's government-issued identification (e.g. drivers license, military ID, etc.) Upon first use, each access log page will be dated with the current date, and each log page will be retained for at least 30 days.

Questions regarding this policy should be directed to the Information Security Officer at **x1234**.

Agency Name
IT FACILITY ACCESS POLICY

Statement of Policy

IT is the policy of the *Agency Name and Abbreviation* that access to *Agency Abbreviation* facilities that house IT systems and data is restricted to individuals who have a legitimate business need for such access. Legitimate business needs include a primary work assignment to an *Agency Abbreviation* facility that house IT systems and data or access to an *Agency Abbreviation* facility that house IT systems and data to fulfill job responsibilities.

Visitor Sponsorship and Escort

An *Agency Abbreviation* employee or contractor must sponsor all visitors to the facility, and must escort the visitor at all times. Both the visitor and the escort must sign the Facility Access log which will note the day and time of arrival, purpose of visit, and time of departure. Escorts will monitor visitor actions and will prevent visitors from connecting flash drives or other portable storage to *Agency Abbreviation* IT systems or from using cameras during the visit, unless such use has been approved by the Information Security Officer.

Access Logs

Access logs must be reviewed daily by the *Log Reviewer to* ensure all entries have a corresponding exit time. The *Identity Verifier* must verify the each individual's government-issued identification (e.g. drivers license, military ID, etc.) Upon first use, each access log page will be dated with the current date, and each log page will be retained for at least 30 days.

Questions regarding this policy should be directed to the Information Security Officer at *Phone Number*.

Appendix B – IT Facility Access Log Template

				Date	
Name (print) **Organization (print)**	**Signature**	**Time In**	**Time Out**	**Reason For Visit**	**Escort Signature**

Appendix C – Non Disclosure & IT Security Agreement – Example and Template

DEPARTMENT OF CITIZEN SERVICES NON-DISCLOSURE & IT SECURITY AGREEMENT

As a user of the computer systems which are operated by the **DEPARTMENT OF CITIZEN SERVICES (DCS)**, I understand and agree to abide by the following terms which govern my access to and use of the processing services of **DCS**:

Access has been granted to me as a necessary privilege in order to perform authorized job functions for the Commonwealth. I understand and agree that 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 job functions.

In the execution of my duties, I may be exposed to information that is sensitive and must be protected. This information may come in a variety of forms, including, but not limited to, business and technical plans, business processes and practices, financial information, technical drawings, network design, IT security plans and processes, computer programs, algorithms, scripts, and formulas. In handling this information I will

- Make every effort, in good faith, to ensure appropriate protection of information.
- Not release, divulge, share, loan, sell, or otherwise disclose this information to unauthorized parties or individuals.
- Use sensitive information only within the scope, and for the purpose, for which it was intended.
- Be responsible for my disclosure of **DCS** information, even if that disclosure was accidental, inadvertent, or unintentional.

I understand that my disclosure of **DCS** information may result in actions against me, including termination of employment and potential legal liability.

If, due to my authorized job functions, I require access to information on Commonwealth of Virginia‘s computer systems which is not owned by **DCS** or am requested to access such information by anyone, I must obtain authorized access to that information from the information owning agency’s Agency Head or Information Security Officer and present it to the Commonwealth’s Chief Information Security Officer or Deputy Chief Information Security Officer for approval prior to accessing that information. I will not discuss other agency’s information, whether sensitive or non-sensitive, with any individual unless such approval is obtained and will not disclose or discuss any information from other agencies which I do access.

I understand and agree that I will not disclose information concerning any access control mechanism of which I have knowledge unless properly authorized to do so by my employing agency, 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 DCS procedures and standards which relate to the security of Commonwealth Information Technology services and the information contained therein;

If I observe any incidents of non-compliance with the terms of this agreement, I am responsible for reporting them to the Commonwealth's Chief Information Security Officer or Deputy Chief Information Security Officer;

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

William J. Quirin _____ November 30, 2008 _____

Employee/Consultant Name (Print) **Date**

_____

Employee/Consultant Signature

Agency Name

NON-DISCLOSURE & IT SECURITY AGREEMENT

As a user of the computer systems which are operated by the *Agency Name and Abbreviation*, I understand and agree to abide by the following terms which govern my access to and use of the processing services of *Agency Abbreviation.*

Access has been granted to me as a necessary privilege in order to perform authorized job functions for the Commonwealth. I understand and agree that 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 job functions.

In the execution of my duties, I may be exposed to information that is sensitive and must be protected. This information may come in a variety of forms, including, but not limited to, business and technical plans, business processes and practices, financial information, technical drawings, network design, IT security plans and processes, computer programs, algorithms, scripts, and formulas. In handling this information I will

- Make every effort, in good faith, to ensure appropriate protection of information.
- Not release, divulge, share, loan, sell, or otherwise disclose this information to unauthorized parties or individuals.
- Use sensitive information only within the scope, and for the purpose, for which it was intended.
- Be responsible for my disclosure of *Agency Abbreviation* information, even if that disclosure was accidental, inadvertent, or unintentional.

I understand that my disclosure of *Agency Abbreviation* information may result in actions against me, including termination of employment and potential legal liability.

If, due to my authorized job functions, I require access to information on Commonwealth of Virginia‘s computer systems which is not owned by *Agency Abbreviation* or am requested to access such information by anyone, I must obtain authorized access to that information from the information owning agency’s Agency Head or Information Security Officer and present it to the Commonwealth’s Chief Information Security Officer or Deputy Chief Information Security Officer for approval prior to accessing that information. I will not discuss other agency’s information, whether sensitive or non-sensitive, with any individual unless such approval is obtained and will not disclose or discuss any information from other agencies which I do access.

I understand and agree that I will not disclose information concerning any access control mechanism of which I have knowledge unless properly authorized to do so by my employing agency, 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 *Agency Abbreviation* procedures and standards which relate to the security of Commonwealth Information Technology services and the information contained therein;

If I observe any incidents of non-compliance with the terms of this agreement, I am responsible for reporting them to the Commonwealth's Chief Information Security Officer or Deputy Chief Information Security Officer;

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 _____ *Date* _____
Employee/Consultant Name (Print) **Date**

Employee/Consultant Signature _____
Employee/Consultant Signature