Commonwealth of Virginia

Information Technology Resource Management

INFORMATION SYSTEMS FACILITIES 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 of VITA's Policy, Practice and Architecture (PPA) Division. PPA 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	04/27/2009	

Preface

Publication Designation
ITRM Information Systems Facilities Security Guideline

Subject
Information Systems Security

Effective Date
April 27, 2009

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") that manage, develop, purchase, and use information technology (IT) resources in the Commonwealth.

Purpose
To provide agencies with guidance in meeting COV Information Security Program requirements and in the development and implementation of the facilities security component of their agency information security program.

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*

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 and independent State agencies and institutions of higher education are responsible for complying with all Commonwealth ITRM policies and standards, and considering Commonwealth ITRM guidelines that address security of state government electronic information from unauthorized uses, intrusions or other security threats issued by the Chief Information Officer of the Commonwealth.

Definitions

Agency - All executive, legislative, and judicial branch and independent State agencies and institutions of higher education that manage, develop, purchase, and use IT resources in the Commonwealth of Virginia (COV).

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 COV IT systems and data.

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

Data Owner - An agency Manager, designated by the Agency Head or Information Security Officer, who is 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.

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

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.

Risk - The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

Risk Assessment (RA) - The process of identifying and evaluating risks so as to assess their potential impact.

Risk Mitigation - The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

Sensitivity - A measurement of adverse affect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled that compromise of IT systems and data with respect to confidentiality, integrity, and/or availability could cause IT systems and data are sensitive in direct proportion to the materiality of the adverse effect caused by their compromise.

Sensitivity Classification - The process of determining whether and to what degree IT systems and data are sensitive.

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.

Threat - Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data and/or denial of service by exploiting vulnerability.

Vulnerability*:* A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Related ITRM Policy and Standards

Current version of COV ITRM Security Policy

Current version of COV ITRM Security Standard

Current version of COV ITRM Security Audit Standard

TABLE OF CONTENTS

1. Introduction

1.1 Information Security

This Guideline presents a methodology and guidance that agencies can use in developing and implementing the facilities security component of their agency information security program. This guidance supports the Commonwealth's Information Security Program as defined in the current version of the Commonwealth of Virginia Information Technology Resource Management (COV ITRM) Security Policy and related COV ITRM security standards.

The function of the Security Policy is to define the overall COV Information Security Program, while the standards define the minimal COV Information Security requirements that must be included in agency information security programs. Agencies are not required to use the methodologies in guidelines, and may use methodologies from other sources or develop their own, provided that they meet the requirements identified in COV ITRM security related standards.

1.2 Facilities Security

Facilities Security is the practice of providing protection to people, processes, and information assets through the implementation of logical, physical, and environmental controls. Complementing security controls must be in place to safeguard the facilities that house COV Information Technology (IT) equipment, systems, services, and personnel.

1.3 Roles and Responsibilities

The agency's security program should include a facility policy that addresses safeguards to protect the facility. A facilities security policy should include provisions for the facility access and facilities security incident handling and reporting. The ISO or designated individual is responsible for the agency's or its service provider's IT facilities security components.

Appendix A provides an example and template of a Facilities Security Policy.

1.4 Principal of Least Privilege for Facilities

Physical access to essential computer hardware, wiring, displays, and networks should be controlled by the principle of least privilege, which requires that users have only the minimum access rights necessary to fulfill their responsibilities.

For additional information regarding principle of least privilege, refer to the Personnel Security Guideline, section 2.2.1 Determining Access Requirements.

2 Facilities Security Practices and Safeguards

2.1 *Safeguarding IT Systems and Data*

The physical facility is the building, vehicle, or other structure housing the system and network components. Facilities can be characterized, based upon their operating location, as static, mobile, or portable. They may be operated in wide variety of locations, including buildings, vehicles, in temporary outdoor enclosures.

Physical characteristics of these facilities determine level of exposure to physical threats such as fire, roof leaks, or unauthorized access.

Agency IT systems and data may reside in any of the types of facilities listed below and must be safeguarded. Mobile facilities are capable of moving or being moved readily, and utilizing motor vehicles for ready movement.

- Static facilities (such as buildings). Static systems are installed in or on structures at fixed locations.
- Mobile facilities (such as computers mounted in vehicles). Mobile systems are installed in vehicles that perform as a facility but not at a fixed location.
- Portable facilities (such as movable command centers)

The potential safeguards listed below should be deployed based on the value of the technology and data assets and the type of facility.

- Locks on facility doors and windows
- Access control systems
- Physical monitoring systems
- Alarm systems
- Security guards
- Visitor logging and controls

2.2 *Safeguards to Protect Against Human, Natural, and Environmental Risks*

All facilities face a certain level of risk associated with various threats. These threats may be the result of intentional acts to cause harm, natural events or accidents. Agencies should deploy safeguards that provide adequate protection to facilities that house IT equipment, personnel, systems, services, and Commonwealth information assets.

A facility's general geographic operating location determines the characteristics of events either enabled or caused by humans, natural and environmental events. Common threat sources and examples of threat actions are shown in the table below.

Table 1: Common Threat Sources and Examples

Source	Action
Human	Bombs, terrorism, insider theft, burglary, civil disorders, social engineering and network based attacks or unauthorized access to confidential areas.
Natural	Floods, earthquakes, tornadoes, hurricanes, landslides, flooding, and other such events.
Environmental	Pollution, chemical spills, fire, and other such events.

Controls for protecting against human, natural, and environmental risks may vary from agency to agency, depending on unique agency protection needs, costs, and benefits. The analysis and management of risks should be modified as appropriate, dependent on the type of facility, and if it is static, mobile or portable.

Agencies should perform a risk assessment on IT facilities. Please refer to the IT Risk Management Guideline for additional information on performing risk assessments.

3 Logical Access Controls

3.1 *Electronic Access Control*

Physical access control is a matter of who, where, and when. Who is allowed to enter or exit, where they are allowed to enter or exit, and when they are allowed to enter or exit. Access should be based on the principle of least privilege, and enforced with the electronic access control systems. Authentication is proving who you are and authorization is granting access based on authentication. These components create the principal of authentication, authorization and accounting, (AAA) and can be applied to logical access controls for physical security.

In the past this was partially accomplished through keys and locks. When a door is locked, only someone with a key can enter through the door depending on how the lock is configured. Mechanical locks and keys do not restrict the key holder to specific times, dates or provide records of the key used on any specific door. Also, keys can be easily copied or transferred to an unauthorized person. When a key is lost or the key holder is no longer authorized to enter the protected area, the locks must be re-keyed.

Electronic access control systems use computers to solve the limitations of mechanical locks and keys. Credentials can be used to replace mechanical keys and locks. An electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded in a log. When access is refused, the door remains locked and the attempted access is recorded and recorded in a log. Access logs should be reviewed on a regular basis according to agency policy. The system will monitor the door and alarm if the door is forced open or held open too long after being unlocked.

3.2 *Two Factor Authentication for Highly Sensitive Areas*

When a credential is presented to a reader of an electronic access control system, the reader sends the credential's information, usually a number from a badge, to a control panel. The control panel compares the credential's badge number to an access control list defined in a system, grants or denies the presented request, and sends a transaction log to a database. When access is denied, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a flashing red light if access is denied and a flashing green light if access is granted.

The above description is an example of a single factor transaction. In this case, credentials can be shared, excluding biometrics, thus defeating the purpose of the access control list. For example, employee A has access rights to the server room but employee B does not. Employee A either gives Employee B their badge or Employee B takes it and now has access to the server room. To prevent this, two factor authentication can be used. In a two factor transaction, which is more difficult to share, the presented credential, such as a badge, and a second factor, such as a PIN or biometric, is needed for access to be granted. The second factor can be a PIN, a second credential, a badge or token, operator intervention, or a biometric input. Under certain conditions a biometric single factor authentication system can be more secure than a non biometric two factor system. Considering this, it is important to select difficult to exchange factor combinations. Based on risk and sensitivity, consider the use of two factor authentication, such as tokens and biometrics, for access to highly sensitive areas.

Two-factor authentication generally consists of utilizing any two of the following credentials together:

- something you have, such as a badge or token,
- something you know, e.g., a password or PIN, or
- something you are, typically a biometric input.

4 Physical Access Controls

Physical access controls should be deployed to prevent unauthorized individuals from gaining physical access to facilities that house IT equipment, systems, services, and personnel.

In facilities security, the term access control refers to the practice of restricting entrance to a property, a building, or a room, or mobile or portable locations to authorized persons. Physical access control can be achieved in several ways. Within these environments, manual management of physical keys and locks may also be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets.

Physical access controls should include:

- Access control systems including logging and reporting
- Authentication Systems
- Physical monitoring systems (e.g., CCTV)
- Security guards

Note: For information on visitor controls, logging, escort and sponsorship, refer to the Personnel Security Guideline ITRM SEC513-00.

4.1 *Physical Monitoring Systems (e.g., CCTV)*

Closed Circuit Television Systems (CCTV) and video monitoring and surveillance systems are being used more often. The latest monitoring and recording systems are integrated with business networks and utilize hardware such as Digital Video Recorders (DVRs), online storage, and network accessible cameras. Older systems typically used off line tape storage and stand alone systems that were not part of business networks.

One of the most significant benefits of the newer business networked digital surveillance systems is that images can be viewed anywhere within the business organization with software and network connectivity. External connectivity can be enabled broadening the monitoring base. Flexibility and can be enhanced with Pan Tilt Zoom (PTZ) and analytic camera technologies. Images can be viewed by multiple parties simultaneously enabling shared review of monitored events. IP addressable cameras can be placed anywhere on existing business network infrastructure thus reducing implementation time. Storage is now moving to more reliable network based hardware such as Network Attached Storage (NAS) and Storage Area Networks (SAN) that can offer redundancy thus eliminating any single point of failure.

4.2 *Security Guards*

The use of security guards should be based on the sensitivity and risk to provide the level of security controls necessary to protect the assets housed in a facility. Security guards may be employees or employed by a third party company with expertise in facilities security that is paid to protect property, assets, or people. Often, security guards are uniformed and act to protect property by maintaining a high visibility presence to deter illegal and inappropriate actions.

Security guard duties include observing (either directly, or by watching alarm systems or video cameras) for signs of crime, fire or disorder; then taking action and reporting any incidents to the agency and emergency services as appropriate. Security guards, electronic controls such as access control systems and CCTV monitoring complement each other in securing a facility.

4.3 *Physical Access Monitoring and Auditing*

Physical access to sensitive IT systems should be carefully controlled (based on job role and legitimate business needs), commensurate with sensitivity and risk. Logs should be maintained that document who is granted physical access to sensitive IT systems and when. Logs should be

regularly monitored and audited to ensure that those who physically access sensitive IT systems are authorized and have a legitimate business need. Monitoring of data centers can be performed through closed circuit television (CCTV) or other forms of video surveillance.

An example of a facility access log and template is located in Appendix B.

4.4 *IT System Physical and Logical Access Review*

Physical access logs should be reviewed periodically for the list of persons allowed physical access to sensitive IT systems. This review should confirm that physical access to sensitive IT systems is authorized and there is a legitimate business need.

The frequency of these reviews should be relative to the level of sensitivity of the systems and the risk involved. A facility that houses many or all of an agency's systems and data may justify a regular monthly review while a closet that houses wiring components and network equipment for a segment of an agency's network may justify six month reviews.

Documentation involved in a review should be a printed access control list from an automated system if one is used, or a list of individuals' issued keys if mechanical locks are used. Also, a list of the visitor logs for the period should be included in this review. Following is a list of items to check for during the review:

- Terminated employees or contractors with access,
- Any employees or that have been transferred and no longer have a business need for access,
- Where duties have changed and access is no longer necessary, or
- Any contractors that are no longer on contract to provide services that require access.

5 Environmental Controls for IT Systems and Data

Appropriate environmental controls such as electric power, fire detection and suppression, heating, ventilation, air conditioning and air purification should be deployed, for the protection of facilities housing systems and information. These controls are deployed to mitigate natural or manmade disasters. Environmental Controls for IT systems and data should be deployed in accordance with IT system requirements and any applicable laws and regulations

5.1 *Environmental Controls*

Environmental risks and threats should be assessed in the IT risk management process. Controls in place to mitigate these risks and threats should be assessed in the IT security audit process and tested and verified with IT security audits. Following is a list of recommended environmental controls agencies should consider in order to protect IT systems and data:

1. There should be sufficient means provided to allow for air flow and cable management (e.g., raised floors, cable trays, etc.), as well as high ceilings to allow for heat dispersal.

2. American Society of Heating, Refrigerating and Air Conditioning Engineers "Thermal Guidelines for Data Processing Environments" recommends a temperature range of 20–25 °C (68–75 °F) and humidity range of 40–55% with a maximum dew point of 17°C as optimal for data center conditions.

3. Computer rooms should have an air filtration system implemented.

4. Uninterruptible Power Systems should provide a minimum of power to provide and orderly equipment shutdown in the event of power loss.

5. Redundant access to power, and cooling should be available.

5.2 *Fire Detection and Suppression*

Fires are a unique threat because of the potential for damage to hardware and data, the risk to human life and the pervasiveness of the damage. Smoke and corrosive gases from fire, anywhere in the building, can damage systems throughout the entire building. Consequently, it is important to evaluate the fire safety of buildings that house IT systems and data.

1. Agencies or their service provider should provide fire detection and appropriate fire suppression as required by building code.

2. Consider deployment of a HFC-227, or similar, inert gaseous fire suppression system.

3. Agencies or their service provider should train personnel working in the IT facility in fire detection and fire suppression.

4. There should be fire detection and fire suppression solutions in place in each data center.

5. There should be emergency power-off switches in the data center.

6. There should **not** be wet pipe sprinkler systems installed in the data center.

5.3 *Proactive Design Control*

When building a new facility or relocation of an existing facility the impact of natural threats should be considered. Agencies should address building contractor requirements and contractor relationships should be carefully defined in Agency policies. The facility should not be located where the threat of natural disaster is high. The threat of the occurrence of floods, earthquakes, tornadoes, hurricanes, landslides, and other such events should be evaluated. The Telecommunications Industry Association (TIA) created the Telecommunications Infrastructure

Standards for Data Centers document, TIA-942. This document covers site space and layout, cabling infrastructure, tiered reliability and environmental considerations. Data Centers are rated with the term Tiered Reliability on a scale of Tier 1 to Tier 4. This rating system can be used in proactive design control to provide a baseline for agencies to consider when designing a Data Center. Information on the TIA-942 standard is available on the Telecommunications Industry Association Internet site at http://www.tiaonline.org/standard . Additional guidance is available in the VITA Enterprise Technical Architecture, ETA Networking and Telecommunications Domain Report on the VITA Internet site.

5.4 *Additional Considerations Related to Environmental Controls*

IT systems and the people who operate the systems need to have a reasonably well-controlled operating environment. Consequently, failures of electric power, water, and other utilities will usually cause a service interruption and may damage hardware.

1. Agencies should schedule testing to make certain that all utilities, including the associated elements such as power and water function properly.

2. There should be battery backup power onsite with sufficient duration to switch over to a continuous power generation or provide for an orderly automatic equipment shutdown.

3. Backup power equipment should be tested on a regular schedule. This scheduled testing should be conducted on a monthly or quarterly basis commensurate with sensitivity and risk.

4. There should be continuous power generation onsite; a minimum of 24 hours of fuel should be available onsite.
    a. Consider installation of a dual electrical power source system.
    b. Recommended. Fuel storage on the premises providing up to a week of fuel to the facility.
    c. Recommended. A contract for fuel delivery should be in place.

5. IT Facilities should be designed so that items such as plumbing lines are not placed in a manner that would endanger the IT equipment if a leak occurred. For existing facilities, agencies should know the location of plumbing lines that might leak and endanger system hardware. Preparations should be made to reduce risk such as:

    a. Relocating plumbing lines if hardware relocation is not feasible,
    b. Relocation of hardware if plumbing line relocation is impossible,
    c. Personnel training should include identifying shutoff valves,
    d. Provide water damage equipment such as mops, buckets, towels, wet-dry vacuums, fans, etc., and
    e. Deploy flood-control equipment such as pumps, tarpaulins, sand bags, etc.

6. Special requirements for the location, materials and construction of the actual computer room and equipment areas should be considered:
    a. Select or build a windowless room or floor if possible.
    b. If the facility is a multiple floor building middle floors are preferred.
    c. Use fire retardant and forced entry resistant building materials where applicable.
    d. If drop ceilings are present, walls should be full walls or modified prevent access to the computer room via the ceiling.
    e. Metal encased fireproof doors should be deployed.

Appendices

These Appendices provide templates that agencies may use to document their use of many of the methodologies described in this Guideline. The templates consist of:

1) An example of the document, completed with functional 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 - Facility Policy and Template

Department of Citizen Services (DCS)

Statement of Policy

The **Department of Citizen Services (DCS)** must establish procedures to protect Sensitive Information System Resources and Data from unauthorized physical access, tampering, and theft. It is the policy that access to **DCS** facilities that house IT systems and data is restricted to individuals who have a business need for such access. 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.

Purpose

This policy reflects the **(DCS)'s** commitment to identify and implement security controls that will keep risks to Information System Resources at reasonable and appropriate levels.

Policy

The **(DCS)** must protect the confidentiality, integrity, and availability of its Information Systems by preventing unauthorized physical access to, tampering with, and theft of these systems and the facilities in which they are located, while ensuring properly authorized access is allowed.

A Facility area containing Sensitive Data must be physically located where unauthorized access is minimized. The perimeter of a building or site containing Information Systems with Sensitive Data must be physically sound, the external walls of the site should be solidly constructed and all external doors must have appropriate protections against unauthorized access.

A Facility area containing Sensitive Data must be physically located where unauthorized access is minimized. The perimeter of a building or site containing Information Systems with Sensitive Data must be physically sound, the external walls of the site should be solidly constructed and all external doors must have appropriate protections against unauthorized access.

The level of protection provided for a Facility containing Sensitive Data must be commensurate with identified risks and aligned with Sensitive Data classification. An annual assessment of risks to the facilities storing Sensitive Data must be performed by the Information Security Officer (ISO) or designee.

All employees must wear the organization's employee identification visibly. Employees should be encouraged to report unescorted strangers or anyone not wearing visible identification. All visitors with a requirement for access to the facility must show proper identification and sign in prior to gaining physical access to secure areas where Sensitive Data is housed.

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 such actions as unauthorized access, removing or tampering with equipment, 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 Agency Information Security Officer or designee.

Access Logs

Access logs must be reviewed daily by the **security guard** for completeness. Logs should include entry and exit times and printed name and signature. Review should 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.

IT Security Facility Event

Any observable threatening occurrence to the IT Facility and/or any contents within is considered an IT Security Facility Event.. Although natural disasters and other non-security related disasters (power outages) are also called events, these reporting requirements are for IT Security Facility events only. Events can many times indicate an IT Security incident is occurring.

An IT Security Facility Event that has an adverse effect on the IT Facility and/or its contents, or the threat of the occurrence of such an event should be reported.

Any suspected IT Security Facility event shall be reported immediately to the local authorities (police). A suspected IT Security Facility event includes, but is not limited to:

i. Break in
ii. Physical damage inside and/ outside the facility
iii. Vandalism
iv. Violence of any kind, including threats
v. Thief of property within and/or outside the facility

DCS staff will immediately report the IT Security Facility Incident to VITA as required by *Code of Virginia, § 2.2-603, et seq.*

Questions regarding this policy should be directed to the Information Security Officer at X**1234**.

Agency Name

Facility Security Policy

Statement of Policy

The *Agency Name* must establish procedures to protect Sensitive Information System Resources and Data from unauthorized physical access, tampering, and theft. It is the policy 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.

Purpose

This policy reflects the *Agency Name*'s commitment to identify and implement security controls that will keep risks to Information System Resources at reasonable and appropriate levels.

Policy

The *Agency Name* must protect the confidentiality, integrity, and availability of its Information Systems by preventing unauthorized physical access to, tampering with, and theft of these systems and the facilities in which they are located, while ensuring properly authorized access is allowed.

A Facility area containing Sensitive Data must be physically located where unauthorized access is minimized. The perimeter of a building or site containing Information Systems with Sensitive Data must be physically sound, the external walls of the site should be solidly constructed and all external doors must have appropriate protections against unauthorized access.

A Facility area containing Sensitive Data must be physically located where unauthorized access is minimized. The perimeter of a building or site containing Information Systems with Sensitive Data must be physically sound, the external walls of the site should be solidly constructed and all external doors must have appropriate protections against unauthorized access.

The level of protection provided for a Facility containing Sensitive Data must be commensurate with identified risks and aligned with Sensitive Data classification. An annual assessment of risks to the facilities storing Information Systems with Sensitive Data must be performed by the Information Security Officer (ISO) or designee.

All employees must wear the organization's employee identification visibly. Employees should be encouraged to report unescorted strangers or anyone not wearing visible identification. All visitors with a requirement for access to the facility must show proper identification and sign in prior to gaining physical access to secure areas where Sensitive Data is housed.

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 Agency Information Security Officer (ISO) or designee.

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.

IT Security Facility Event

Any observable threatening occurrence to the IT Facility and/or any contents within is considered an IT Security Facility Event. Although natural disasters and other non-security related disasters (power outages) are also called events, these reporting requirements are for IT Security Facility events only. Events can many times indicate an IT Security incident is occurring.

An IT Security facility event that has an adverse effect on the IT Facility and/or its contents, or the threat of the occurrence of such an event should be reported.

Any suspected IT Security Facility event shall be reported immediately to the local authorities (police). A suspected IT Security Facility event includes, but is not limited to:

vi. Break in
vii. Physical damage inside and/ outside the facility
viii. Vandalism
ix. Violence of any kind, including threats
x. Thief of property within and/or outside the facility

Agency Abbreviation staff will immediately report the IT Security Facility Incident to the VITA as required by *Code of Virginia, § 2.2-603, et seq.*

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

Appendix B IT Facility Access Log EXAMPLE and TEMPLATE

IT Facility Access Log

Date	01.02.2008					
Name (print) **Organization (print)**	**Signature**	**Badge or Tag #**	**Time In**	**Time Out**	**Reason For Visit**	**Escort Signature**
Tim Roberts Control Temp, Inc	Tim Roberts	527	08:16	10:03	A/C Repair	Turner Jones
Jane Matthews Finance Revenue Agency	Jane Matthews	019	09:08	10:15	Tour	Fred Banks
Thomas Robbins A & A Electric	Thomas Robbins	401	12:49	3:28	Electric Repair	Kathy Smith
Sally Goode CSB Group	Sally Goode	616	12:58	2:34	Sales Call	Sherman Lewis

IT Facility Access Log

Date						
Name (print) **Organization (print)**	**Signature**	**Badge** or Tag #	**Time In**	**Time Out**	**Reason For Visit**	**Escort Signature**