**Logical Access Controls Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standard, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates access controls to all “YOUR AGENCY NAME” systems. This policy and procedure establishes the minimum requirements for the control of logical access to “YOUR AGENCY NAME”’s computer systems including test and production.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.1 Access Control Family, Controls AC-1 through AC-16, AC22, to include specific requirements for “YOUR AGENCY NAME” in AC-2-COV and AC-8-COV.

# SCOPE

All “YOUR AGENCY NAME” Employees (classified, hourly, or business partners) who administer computer systems owned and/or operated by “YOUR AGENCY NAME”, Data Owners, as well as all System Owners. This policy also includes virginia.gov or other contractually hosted Web sites or server administration.

# ACRONYMS

AC: Access Control

CSRM: Commonwealth Security & Risk Management

HRM: Human Resource Management Services

ISO: Information Security Officer

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

SSP: System Security Plan

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_Glossary.pdf)

# BACKGROUND

Managing access control of a system is one the most important steps in ensuring the security of the system. As such “YOUR AGENCY NAME” systems require a well-defined and well-implemented set of access controls. This policy directs that systems owned and/or operated by the “YOUR AGENCY NAME” meet these requirements as stipulated by COV ITRM Security Standard SEC501 and security best practices.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibility as described in the Statement of Process section. The following Roles and Responsibility Matrix describe 4 role specific activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Roles** | Users | User Supervisor | System Owner | System Admin | Human Resource Manager | Information Security Officer |
| **Tasks** |  |  |  |  |  |  |
| Create an access control document |  |  | R | C |  | A |
| Review accounts and privileges on an annual basis | I |  | A/R | C |  | I |
| Approve all user logical access to system |  | R | A | C |  |  |
| Ensure that no local administrator rights are granted |  |  | R | C |  | A |
| Notify system owner to remove an account or change access | R | A | C | C | I |  |
| Disable or change user’s access |  | I | A | R |  |  |
| Monitor account usage |  |  | A | R |  |  |
| Approve emergency access | I |  | A | R |  | I |
| Keep all user account data and information on file |  |  | A/R | C |  |  |
| Ensure that at least two individuals have administrative accounts to each it system |  |  | A | R |  |  |
| Ensure that system administrators have both an administrative account and a user account |  |  | A | R |  |  |
| Deactivate temporary accounts |  |  | A | R |  |  |
| Verify that background checks have been completed before establishing accounts |  |  | A | R | C |  |
| Ensure that users are not sharing accounts |  | I | A | R |  |  |
| Ensure that access credentials are delivered in a confidential manner | I |  | A | R |  |  |
| Audit account creation, modification, disabling, and termination actions |  | I | A | R |  |  |
| Associate access levels with group membership |  |  | A | R |  |  |
| Prohibit guest accounts on sensitive systems |  |  | A | R |  |  |
| Document all hardware and service accounts |  |  | A | R |  |  |
| Document where two-factor authentication cannot be used |  |  | A | R |  | I |
| Investigate any unusual system access activities |  |  | A | R |  | I |
| Employ and document access control mechanisms |  |  | A | R |  | I |
| Control information flow |  |  | A | R |  |  |
| Implement and document separation of duties |  |  | A | R |  | I |
| Ensure the concept of least privilege for each user |  |  | A | R |  |  |
| Implement a policy for unsuccessful logins |  |  | A | R |  | I |
| Display an approved system notification message | I |  | A | R |  |  |
| Implement a session locking policy |  |  | A | R |  |  |
| Identify and document user actions that can be performed without identification and authentication |  |  | A | R |  |  |
| Designate and train individuals authorized to post information on a publicly accessible system |  |  | A | R |  | I |
| Review content of publicly accessible information |  |  | A | R |  | I |
| Remove nonpublic information from publicly accessible systems, if discovered |  |  | A | R |  | I |

**STATEMENT OF POLICY**

In accordance with SEC501, AC-1, AC-2, AC-2-COV, AC-3, AC-4, AC-5, AC-7, AC-8, AC-8-COV, AC-11, AC-14, and AC-22, Access Control, “YOUR AGENCY NAME” will develop, disseminate, and review/update the Local Access Controls Policy on an annual basis.

1. **ACCOUNT MANAGEMENT**
   1. All “YOUR AGENCY NAME” directorates will ensure proper access management to agency-owned systems and systems belonging to business partners who house “YOUR AGENCY NAME”-owned information.
   2. The System Owner shall create an Access Control Document that defines the processes and procedure that the organization will use to manage access to “YOUR AGENCY NAME” systems. The document will include, at a minimum, the following:
      1. An account type dictionary which includes a list of all account types used by the organization / system (i.e., individual, group, system, application, guest/anonymous, temporary, etc.) and a definition of that account type;
      2. A group membership policy definition section which establishes a list of all groups and conditions for group membership. For example, group membership includes but is not limited to accesses grouped by Read Only, Read/Write;
      3. A well-defined process for identifying authorized users access to the information system and specifying access privileges. The process will include:
         1. Definition of appropriate approvals required for requests to establish new accounts;
         2. Definition of appropriate approvals required for requesting modification (addition or subtraction of privileges);
         3. Process for establishing, activating, modifying, disabling, and removing accounts; and
         4. Procedures for specifically authorizing and monitoring the use of guest/anonymous and temporary accounts.
      4. A process for notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes.
   3. The System Owner shall review accounts and privileges at least on an annual basis.
   4. The user’s supervisor and the System Owner (or designee) shall approve all user logical access to “YOUR AGENCY NAME” systems.
      1. As part of the access request, the user’s supervisor must include the user’s need for access.
      2. The System Owner (or designee) maintains the documented approvals.
      3. The ISO shall approve accounts for users requiring administrative and/or privileged access.
   5. The organization security lead and the System Owner will ensure that no local administrator rights are granted:
      1. Unless there is a documented exception on file, for employees that are primarily responsible for developing and/or supporting IT applications and infrastructure.
   6. Users and/or a user’s supervisor must notify the System Owner when a user’s account is no longer needed, or when access needs change. The System Owner then notifies the System Administrator and Human Resources of the change. The user’s access is disabled within 24 hours.
      1. Logical access rights must be temporary disabled when:
         1. Personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose, and
         2. Personnel are suspended for greater than 1 day for disciplinary purposes.
   7. The System Owner (or designee) must monitor account usage to ensure that no account goes over 90 consecutive days without usage.
      1. The information system must be configured to automatically disable accounts if not used for 90 days.
   8. The System Owner (or designee) shall approve emergency access to sensitive IT systems for a predetermined period not greater than 30 days, and notifies the ISO for oversight. If the emergency access request leads to changes in the user’s access level, attributes for the account are included in the documentation and maintained on file.
      1. The information system must be configured to automatically terminate temporary and emergency accounts after a predetermined period not greater than 30 days.
   9. The System Owner (or designee) must keep all user account data, information, and documentation associated with a user’s logical access on file, in accordance with “YOUR AGENCY NAME”’s Records Management Policy and Procedure.
   10. The System Owner shall be responsible for ensuring:
       1. That at least two individuals have administrative accounts to each IT system in order to help provide continuity of operations.
       2. That System Administrators have both an administrative account and at least one user account and that administrators use their administrative accounts only when performing tasking requiring administrative privileges.
       3. The deactivation of:
          1. Temporary accounts that are no longer required, and
          2. User accounts of terminated or transferred users are disabled within 24 hour of notification.
       4. That disabled accounts are retained in accordance with “YOUR AGENCY NAME”’s records retention policy.
       5. That activation of accounts or granting of privilege is based on:
          1. The principle of least privilege;
          2. Valid access authorization documentation;
          3. Intended system usage;
          4. Meeting the missions and business functions of “YOUR AGENCY NAME”; and
          5. In accordance with the “YOUR AGENCY NAME” HRM Criminal History Record Information Policy and Procedure, background checks must be completed before (or as soon as feasible) to establishing user accounts.
       6. That users are not sharing accounts, unless the system resides on a guest network.
       7. That access credentials, for internal IT systems, are be delivered to the user in a confidential manner based on information already on file.
       8. That access credentials, for Internet-facing only systems, must be securely delivered (e.g., by alternate channels such as U.S. Mail) to all external users of all sensitive external IT systems after confirming requests.
       9. That the information system automatically audits account creation, modification, and disabling, and termination actions and notifies, as required, appropriate individuals.
       10. That access levels are associated with group membership, where practical, and that every system user account is a member of at least one user group.
       11. That guest accounts are prohibited on sensitive IT systems.
       12. That all service and hardware accounts are documented, including, but not limited to granting, administering and terminating access.
           1. If the service or hardware account is not used for interactive login with the system, the account is exempt from the requirement to change the password at the interval defined in the “YOUR AGENCY NAME” CSRM IT Identification and Authentication Policy.
       13. That in cases where two-factor authentication cannot be used, the analysis of why two-factor authentication is not used must be documented.
   11. The user of “YOUR AGENCY NAME” systems shall ensure that:
       1. Accounts are not being shared;
       2. Initial passwords are changed upon first use;
       3. Proper notification is given to System Owners to temporarily disable access when the user will not need such access for a prolonged period in excess of 30 days due to leave, disability or other authorized purpose; and
       4. System use is within the policies and guidelines.
   12. System Owners and System Administrators must investigate any unusual system access activities observed in logs or reported to them by staff and employees. Investigation activities shall include the following:
       1. Monitor for atypical usage of information system accounts;
       2. Report atypical usage to the ISO; and
       3. Track and monitor privileged role assignments (e.g., key management, network and system administration, database administration, and web administration).
   13. A users’ continued need for access to all IT systems must be reviewed at least on an annual basis.
       1. System Owners will advise users of the need to recertify a continued need for access to the system.
       2. The user will advise supervisor by email of the need to recertify.
       3. The supervisor will review the need and notify the System Owner of the continued need.
2. **ACCESS ENFORCEMENT**
   1. System Owners must employ and document access control mechanisms in the organization Access Control Document as described in Section A-2, of this document. These include but are not limited to identity-based policies, role-based policies, attribute-based policies, as well as access enforcement mechanisms such as access control lists, access control matrices, and cryptography. Cryptography employed for access control must adhere to the Federal Information Processing Standard (FIPS) 140-2.
3. **INFORMATION FLOW ENFORCEMENT**
   1. System Owners must ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
      1. Flow control restrictions include, but are not limited to, the following:
         1. Keeping export controlled information from being transmitted in the clear to the Internet,
         2. Blocking outside traffic that claims to be from within the organization, and
         3. Not passing any web requests to the Internet that are not from the internal web proxy.
      2. Flow control is based on the characteristics of the information and/or the information path.

Note: Flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics).

1. **SEPARATION OF DUTIES**
   1. The System Owner separates duties of individuals as necessary, to prevent malevolent activity without collusion.
   2. The System Owner is responsible for ensuring and documenting separation of duties.
   3. The System Owner, in coordination with the systems administrator, will implement separation of duties through assigned information system access authorizations.
   4. Separation of duties include, but are not limited to, the following:
      1. Mission functions and distinct information system support functions are divided among different individuals/roles;
      2. Different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security);
      3. Security personnel who administer access control functions do not administer audit functions; and
      4. Different administrator accounts for different roles.
2. **LEAST PRIVILEGE**
   1. “YOUR AGENCY NAME” shall employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
      1. The System Owner is responsible for ensuring that each user has only enough access to conduct their job;
      2. The ISO explicitly approves and authorizes access to administrative or privileged accounts; and
         1. Super-user accounts will be limited to system administration personnel.
      3. The System Owner requires that users of information system accounts, or roles, with access to administrative accounts, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.
      4. The System Owner prohibits privileged access to the information system by non-”YOUR AGENCY NAME” users.
3. **UNSUCCESSFUL LOGIN ATTEMPTS**
   1. The organization and the System Owner will implement a policy for unsuccessful logins. The policy shall be documented in the organization access control document and enforced automatically by the system.
      1. The information system will be configured to:
         1. Enforce a limit of a maximum of 10 consecutive attempts within 15 minutes.
         2. Automatically lock a non-sensitive account/node for a minimum period of 15 minutes when the maximum number of unsuccessful attempts is exceeded.
         3. Automatically lock a sensitive account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.
      2. These controls apply regardless of whether the login occurs via a local or network connection. However, an organization may opt for more stringent controls on a remote connection if practical.
      3. The information system provides additional protection for mobile devices, such as smart phones or personal digital assistants, accessed via login by purging information from the device after not more than ten consecutive, unsuccessful login attempts to the device.
         1. This requirement may not apply to mobile devices if the information on the device is encrypted with sufficiently strong encryption mechanisms, making purging unnecessary.
         2. The login is to the mobile device, not to any one account on the device. Therefore, a successful login to any account on the mobile device resets the unsuccessful login count to zero.
4. **SYSTEM USE NOTIFICATION**
   1. The System Owner must notify users, both internal and external to the organization, that the monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the Agency Head); and user commands; email and Internet usage; and message and data content.
      1. The information system must be configured to:
         1. Display an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance and states that:
            1. Users are accessing a Commonwealth of Virginia information system;
            2. System usage may be monitored, recorded, and subject to audit;
            3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
            4. Use of the system indicates consent to monitoring and recording.
         2. Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information system.
      2. Publicly accessible systems will:
         1. Display the system use information when appropriate, before granting further access;
         2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
         3. Include in the notice given to public users of the information system, a description of the authorized uses of the system.
5. **SESSION LOCK**
   1. The System Owner is responsible for implementing a session locking policy that prevents further access to the system by initiating a session lock after a maximum of 30 minutes, or less, of inactivity or upon receiving a request from a user.
      1. The user should log off of systems not currently being used.
   2. The System Owner is responsible to ensure that a session lock is retained until the user reestablishes access using established identification and authentication procedures.
6. **PERMITTED ACTION WITHOUT IDENTIFICATION OR AUTHENTICATION**
   1. It is the policy of the Commonwealth of Virginia to ensure that all system users be identified and authenticate to ensure proper access to the system. However, from time to time it may become necessary for a system to grant access without authentication. In these cases, the following must be adhered to:
      1. The System Owner is responsible for identifying and documenting specific user actions that can be performed without identification or authentication.
         1. Documentation and the supporting rationale must be included in the System Security Plan.
      2. The System Owner is responsible for providing limited access to specific functions based a particular need to accomplish a particular business or mission.
7. **PUBLICLY ACCESSIBLE CONTENT**
   1. The System Owner shall designate individuals authorized to post information onto an agency information system that is publicly accessible;
   2. The System Owner is responsible for training authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
   3. The System Owner (or designee) reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the agency information system;
   4. The System Owner (or designee) reviews the content on the publicly accessible agency information system for nonpublic information at least every 60-days; and
   5. The System Owner (or designee) removes nonpublic information from the publicly accessible agency information system, if discovered.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO”““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

[ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History | | |
| --- | --- | --- |
| Version | Date | Change Summary |
| 1 | 09/22/2005 | Original |
| 2 | 05/02/2006 | Title changed from System Access Control Policy. Records retention statement deleted. Added a Statement of Procedure that: “Each Director shall provide an inventory of all systems to Security Services by July 1 of each year as well as a copy of the process used to control access.” |
| 3 | 09/28/2007 | Added significant requirements to the Statement of Policy and added Attachment E. |
| 4 | 01/22/2009 | Added Acronym “CSRM” as well as new Items #7 and #8 under Statement of Policy; and, subsequent re-numbering of Items #9 through #14. |
| 5 | 06/15/2010 | Major rewrite as well as updates to be in compliance with the COV ITRM Information Security Standard - SEC501 (Revision 5) dated 08/11/2009. |
| 6 | 07/01/2014 | Complete rewrite from previous version in compliance with the ITRM Information Security Standard SEC501 Revision 8 with Role Matrix added. |
| 7 | 12/29/2021 | Formatting changes |

# ATTACHMENT A

Logical System Access Control Policy

Process Documentation Guidance

The process documentation should address “Logical Access”protection mechanisms (e.g., User authentication or permission levels) that provide Users' logical access to information. It should list the job titles of staff responsible for the logical access processes, and include copies of all forms associated with these processes.

Process Documentation Elements

1. **CREATE USER ACCESS** 
   1. Define the process for requesting and approving new User Access. Items to be included:
      1. How access is requested
      2. Level of accesses available
      3. Business justification needed for access and access level
      4. Approvals and/or authentications needed
      5. How user and/or requester is notified of approval or denial of access
      6. If notifications about decisions are given to others, and to whom
      7. who grants access, when & how
2. **CHANGE USER ACCESS** 
   1. Define the process for requesting and approving existing User Access Changes. Items to be included:
      1. How changes are requested
      2. Business justification for changes
      3. Approvals and/or authentications needed
      4. How user and/or requester is notified of approval or denial of changes to users access
      5. If notifications about decisions are given to others, and to whom
      6. Who grants access, when & how
3. **SUSPENSION OR TERMINATION OF USER ACCESS** 
   1. Define the process of suspending or terminating User Access when access is no longer required or authorized. Items to be included:
      1. When termination will be used and when suspension will be used with the business reasons
      2. How the System Owner is notified of the need that a user’s access be suspended or terminated including controls used to ensure timely notification of terminations and transfers
      3. Who is authorized to provide such notification
      4. Justification necessary
      5. Approvals needed
      6. How user and/or requester is notified of suspension or termination
      7. If notifications about decisions are given to others, and to whom
      8. Who suspends or terminates access, when & how
4. **USER ACCESS REVIEW** 
   1. Two periodic reviews are required:
      1. A review of existing accesses for continued necessity and appropriateness of level
      2. A review of user accesses for inactivity
   2. For the review of existing accesses the documentation should include:
      1. Frequency and timing of the reviews (intervals should be relative to risk)
      2. Method of review
      3. The criteria used for continued necessity\*
      4. The criteria used for appropriateness of level of access\*
      5. Who reviews users’ access for continued necessity
      6. Who reviews for appropriateness of level of access
      7. Approvals and/or authentications needed
      8. How user and/or requester are notified of results
      9. If notifications about decisions are given to others, and to whom
      10. What results may include in terms of access changes and who executes them
   3. \* Criteria used must include confirmation of:
      1. Continuing employment
      2. Current roles and responsibilities and/or any changes
      3. Current access levels and/or any needed changes
      4. Record of acceptable use of user’s access
   4. For the review of inactivity of accounts the documentation should include:
      1. Frequency and timing of the reviews (intervals should be relative to risk)
      2. Method of review
      3. The specified period of inactivity used for the review
      4. Any methods used to validate continued necessity for inactive accounts (who, what & how)
      5. The consequences of various levels of inactivity (suspension or termination)
      6. Approvals needed
      7. How user and/or supervisor is notified of access suspension or termination
      8. If notifications about decisions are given to others, and to whom
      9. How and when suspension or termination occurs
   5. Monitoring, Logging and Investigation of Unusual Activity should:
      1. Define the monitoring and logging of access to application and related database files
      2. Who is responsible for the monitoring and logging of access
      3. Describe the procedures for what is logged
      4. Define the process to monitor what is logged
      5. How and when the System Owner is notified when unusual activity occurs
      6. Describe how to investigate unusual activity
      7. Describe the reporting of unauthorized access

# ATTACHMENT B

Template Procedure

This sample procedure is provided to give guidance on documenting user access to the system.

1. Purpose:

To state the policies, procedures and mechanisms used to control logical access to the system and enforce the access policy and to document the process for Granting, Changing and Deleting user access to *System Name*.

1. Scope:

This procedure applies to all user access, but *does*/*does not* include customer agency users. There are approximately \_\_\_\_\_\_ users. This system is considered high, medium or low risk because \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. Requesting User Access to*System Name***:**

The user or his/her supervisor must document (may open a ticket with the VITA Customer Care Center (VCCC)) stating to what system access is requested for what period, for what business reason, and at what level. This document (ticket) is routed to the *System Name* group.

If the document was created (ticket was opened) by the user, the *System Name* group member obtains the supervisor’s approval prior to creating a *System Name* user ID or the document may be created (ticket was opened) by the supervisor on behalf of the user, thus supplying their approval. (Note: This is for a non-sensitive system. For a sensitive system there may be additional approval needed such as the System Owner (or designee).

Define how the Manager of *Division* reviews and approves the request to ensure that access to *System Name* is necessary and appropriate. If access is required, a user ID is created in *System Name,* and the appropriate roles assigned to the user ID. Roles assigned are based on the user’s job requirements. If Root access to *System Name* is granted*,* the Manager of *Division* justifies the access as follows: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. The appropriate individuals, including 1) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_­­­­­\_\_\_\_\_\_\_\_\_\_\_; 2) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_­­­­­\_\_\_\_\_\_\_\_\_\_\_, etc., are notified, as necessary.

Note: Examples of Roles for different access levels for user IDs are “Read only”, and “Read/Write”(update capability). These types of roles can also be used for all of the data or for only some of the data. The requirement of least privilege (user should only have access to the data they need) should be followed when granting access.

The following criteria determine different access levels: *Level Name X* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; *Level Name Y* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, etc, such as emergency access.

1. Changing Existing User Access to *System Name***:**

At a user’s request or his/her supervisor’s request, the level of access assigned to the *System Name* user ID may be adjusted. This type of request might occur due to changes in the user’s responsibility. Documentation (may be a VCCC ticket) and supervisor approval, including justification, is required.

Define how the Manager of *Division* reviews the request to ensure that the requested changes to access are necessary and appropriate. If changes are required, the appropriate roles are added to/removed from the user ID. If Root access to *System Name* is granted*,* the Manager of *Division* justifies the access as follows: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. The appropriate individuals, including 1) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; 2) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, etc., are notified, as necessary.

1. Periodic Review of User IDs

By *Month, day*, of each year, the Manager of *Division* reviews active and inactive *System Name* user IDs by having report #123 run to determine if changes are necessary to access levels or if user’s access should be suspended.

(Note: The review intervals for higher risk levels are shorter, e.g., *Risk Level 1* is reviewed every \_\_\_\_\_\_ month(s); *Risk Level 2* is reviewed every \_\_\_\_\_\_ month(s), etc.)

The following criteria are used to support the need to continue a user’s access or access level: 1) confirmation of continuing employment; 2) confirmation of current roles and responsibilities and/or any changes; 3) confirmation of current access levels and/or any needed changes; 4) confirmation of current risk levels; 5) confirmation of record of acceptable use of access; 6) *other (list all)* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Any needed changes are made and the appropriate individuals, including 1) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; 2) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, etc., are notified, as necessary.

User access is reviewed for inactivity every \_\_\_\_\_\_\_\_\_\_\_\_\_\_by \_\_\_\_\_\_\_\_\_\_\_\_. If a user has not utilized this access in \_\_\_\_\_\_\_\_ the access is *suspended/terminated*.

After a period of \_\_\_\_\_\_ *days/weeks/months* of User Access inactivity, the *System Name* group receives documentation (may be a VCCC ticket) with notification, including justification, to suspend access to *System Name.*  The *System Name* group member who handles the ticket will access *System Name* to determine if the user has a *System Name* user ID. If the user does have a user ID, his/her access is locked out and all roles removed. The appropriate individuals, including 1)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; 2)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, etc., are notified, as necessary.

Exceptions to the standard period include \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. The process for reactivating a disabled user’s access is as follows: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. Monitoring, Logging and Investigation of Unusual Activity

Define the monitoring and logging of access to application and related database files. Describe the procedures for what is logged, monitor what is logged, how to investigate, and the reporting of unauthorized access in accordance with “YOUR AGENCY NAME”’s Information Security Incident Reporting Procedure.

1. Terminating and Suspending User Access

Define terminating and suspending user access in accordance with “YOUR AGENCY NAME”’s Supervisors’ Employee-Business Partner Moves Procedure when a:

* + User access will be terminated if the access has been inactive,
  + User terminates employment with “YOUR AGENCY NAME”,
  + User transfers to another position with in “YOUR AGENCY NAME”, or
  + User access is terminated or suspended for whatever reason.

If the user access account must be suspended, the *System Name* group receives documentation (may be a VCCC ticket) with notification, including justification, to remove or suspend access to *System Name.*  The *System Name* group member who handles the ticket will access *System Name* to determine if the user has a *System Name* user ID. If the user does have a user ID, his/her account is locked out and all roles removed. The appropriate individuals, including 1) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; 2) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, etc., are notified, as necessary.