Security Audit Access – Release 1 & 2

Cardinal Form SE-AUDIT-001 Instructions

Audit Access Overview

Audit Inquiry Access is designated for Audit Staff responsible for conducting agency audits. This role has access to comprehensive Read-Only inquiry including sensitive data.

To maintain segregation of duties between Auditor access versus Core User/Employee Self-Service access, there is a requirement for an employee needing auditor access to have two separate User IDs with a separate business email address not associated to their Employee Self-Service email address or Employee ID.

Cardinal Audit Access must be requested on the Cardinal Security Audit Access Form (Cardinal SE-AUDIT-001) and submitted by the Cardinal Security Officer (CSO) for that agency to the **Cardinal.Security @doa.virginia.gov** mailbox.

- Cardinal User ID created will be in the format of AUDIT_FIRSTNAME.LASTNAME
- Forms will be returned to the Cardinal Security Officer if information required is not complete or correct.
- Email notifications regarding the creation of new Cardinal Audit user accounts, and/or updates to those accounts, will be sent directly to the user and the CSO.

Requesting Audit Access

1. In order to establish a Cardinal Audit account, a new business email address (provided by your agency) is required that is not used or tied to a user's Core/Employee Self-Service account or Employee ID number.
2. The agency Cardinal Security Officer (CSO) submits the Cardinal Security Audit Access Form (Cardinal Form SE-AUDIT-001) to the Cardinal Security Team at the following email address (cardinal.security@doa.virginia.gov) to have the account created. (Form is located on the Cardinal Project website: www.cardinalproject.virginia.gov/security).
3. **Finance (FIN)** Audit access is defined by only two roles, Audit Inquiry and APA all pages – read only FIN role (APA Only).
4. **Human Capital Management (HCM)** Audit access is defined by read-only (Benefits, HR, Payroll and Time and Attendance) roles for each module section and Audit Inquiry HR Sensitive, APA all pages – read only HCM role (APA Only).
5. Audit Access requires you to select the Primary Permission List needed by Business Unit for FIN and HCM.

6. **Overview of each section of the Cardinal Security Audit Access Form**

   a. **Security Action Requested** (Required)

Security Action Requested		
☐ **New User** Setup (complete all applicable fields and roles)	☐ **Update Existing User** (Complete all applicable fields and roles)	☐ **Lock Out Existing User** (Complete User Information Section Only)

   i. **New User Setup** – Check this box to create a new user account or if account was previously locked.

   ii. **Update Existing User** – Check this box if access to Cardinal needs to be updated.

   iii. **Lock Out Existing User** – Check this box if user account needs to be locked.

   b. **User Information (Required)**

User Information	
Name - Last, First, Middle Initial ☐ Name Change	Email Address*(must be different from Employee Self-Service email)*
Business Unit:	Department ID:
User's Job Title:	Cardinal User ID:
Supervisor Name:	Supervisor Employee ID:

   i. **Name –** Last, First, Middle Initial (ex: Doe, John B.)

   ii. **Name Change –** Check box if this is an existing user with a name change.

   iii. **Email Address –** Must be a business email address that is different from the Core User/Employee Self-Service email address.

   iv. **Business Unit –** Enter your agency's 5-digit Business Unit ID (e.g., 50100-VDOT, 15100-DOA, etc.)

   v. **Department ID –** Enter your agency Department ID (e.g., 10015-VDOT, 95400-DOA, etc.)

   vi. **User's Job Title –** User's current job title. (e.g., Financial Services Specialist)

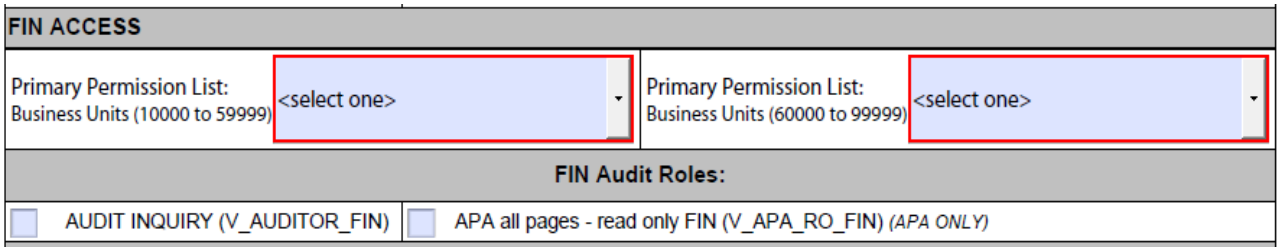
   vii. **Cardinal User ID –** Needed for Existing Users.

   - Leave this field BLANK for New Users Only.
   - If you are unaware of the ID please run the V_PT_SEC_ROLE_USERS query (in HCM and/or FIN as applicable). This query will show User ID, Dept. ID, Account Lock (yes or no), Business Unit, Oprid Description and security roles for the selected application (HCM or FIN).

   viii. **Supervisor Name** and **Supervisor Employee ID Number**

   - Supervisor's Name (ex: Doe, John B.)
   - Supervisor's Employee ID Number - Employee ID Number is the 11-digit number assigned by Cardinal (e.g., 00123456700). You must enter the full 11-digit number on this form.

c. **FIN Section** (Fill out if Audit access is needed in FIN, if not skip this section)



i. **Primary Permission List -** Select the required FIN Primary Permission List to which access is required by using the drop down box. Primary Permission List selection should coincide with the users' agency Business Unit (e.g., users in 13300 should only select Primary Permission Lists for Business Unit 13300):

- 13300 – V_R_13300_APA_OVERSIGHT
- 13300 – V_R_13300_USERS

ii. A detailed list of Primary Permission Lists by Business Unit can be found on the Cardinal Project website. **Choose only one FIN Primary Permission List per user**.

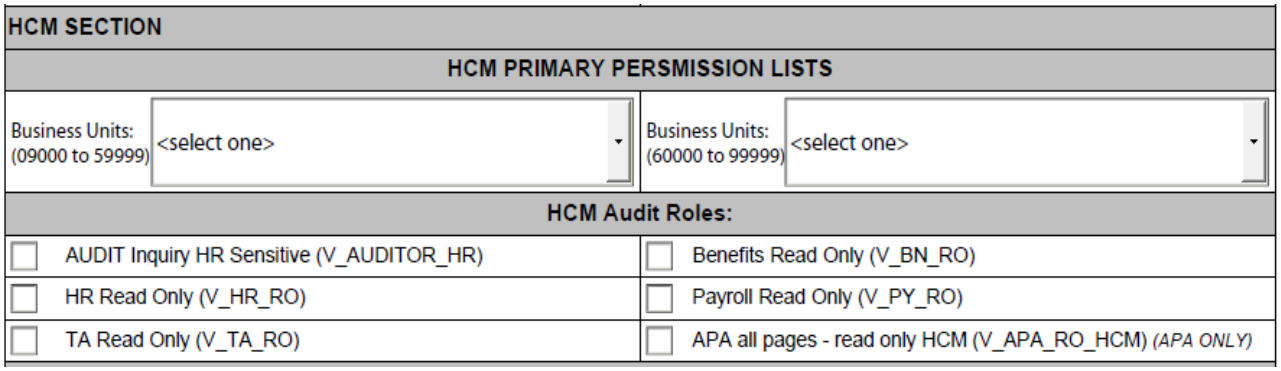
iii. **FIN Audit Roles** (Description of Roles can be found in the Cardinal Security Handbooks)

- Read Only Audit Inquiry role is available
- APA all pages – read only FIN role:

  (a) is restricted for APA Users Only

  (b) and requires a Statewide Permission List (DOA Approval needed)

d. **HCM Section** (Fill out if Audit access is needed in HCM, if not skip this section)



i. **Primary Permission List –** Select the required HCM Primary Permission List to which access is required by using the drop down box. Primary Permission List selection should coincide with the users' agency Business Unit (e.g., users in 15100 should only select Primary Permission Lists for Business Unit 15100). ***Exceptions to this rule are allowed for Auditor access for the Auditor of Public Accounts and for the Office of Inspector General, who will need targeted agency access to conduct specific audits/review***.

- 15100 – V_PRIM_DOA_FISCAL
- 15100 – V_PRIM_DOA_OVERSIGHT
- 15100 – V_PRIM_15100_USERS

- 15100 – V_PRIM_15100_PSB_OVERSIGHT

ii. A detailed list of Primary Permission Lists by Business Unit can be found on the Cardinal Project website. **Choose only one HCM Primary Permission List per user**.

iii. **HCM Audit Roles** (Description of Roles can be found in the Cardinal Security Handbooks)

- Read-Only roles are available for each HCM Section in Cardinal (BN, HR, PY and TA)
- Read Only Audit Inquiry HR Sensitive
  (a) Buddy Role is HR Read Only
- APA all pages – read only HCM role:
  (a) is restricted for APA Users Only
  (b) and requires a Statewide Permission List (DOA Approval needed)

e. **Approval** (Required)

Approvals		
User Printed Name	User Signature (sign above)	Date
Supervisor Printed Name	Supervisor Signature (sign above)	Date
Cardinal Security Officer Printed Name	Cardinal Security Officer Signature (sign above)	Date

i. User printed name, user signature, and date

ii. Supervisor printed name, supervisor signature, and date

iii. Cardinal Security Officer printed name, signature, and date

iv. Digital Signatures are allowed only if they include a system generated date stamp as show in example below:

Example:

v. We will accept email approvals form a user's business email account in the event they cannot physically sign the form. The form must be attached with the email approval showing evidence that the form was transmitted from the user, supervisor and/or the CSO. The approver should state the following:

- **User** –*"Please accept this email as my approval of the attached form as the user."*
- **Cardinal Security Officer** – *"Please accept this email as by approval of the attached form as the Cardinal Security Officer."*
- **Supervisor** – *"Please accept this email as my approval of the attached form as the supervisor."*

f. **Department of Accounts Approval** (Only Required for Statewide Primary Permission Lists)

Department of Accounts Approval *(Only Required for Statewide Primary Permission Lists)*		
DOA Approver Printed Name	DOA Approver Signature (sign above)	Date

i. DOA Approval needed for Statewide Primary Permission List

- Please review the Primary Permission Listing found on the Cardinal Project website (www.cardinalproject.virginia.gov/security) for those marked “Statewide Access Group” – as these will require DOA Approval.