Cardinal Form SE-SW-001 Instructions

Statewide Access Overview

Cardinal Core user access (access beyond Employee Self-Service) is granted based on specific work that an employee needs to perform in the system and the associated security roles set up by their agency.

Cardinal HCM Employee Self-Service (ESS) access is granted systematically and does NOT require a security form. However, the Cardinal Security Statewide Access Form is required for any and all Cardinal core user access. The form must be completed by the agency's Cardinal Security Officer (CSO) and should include required signatures prior to submitting to the Cardinal Security Team in order for access to be granted in Cardinal.

The Cardinal Security Statewide Access form **(Cardinal SE-SW-001)** must be submitted to the **Cardinal.Security@doa.virginia.gov** email mailbox.

- Forms will be returned to the CSO if information required is not complete or correct.
- Email notifications regarding the creation of new Cardinal user accounts, and/or updates to those accounts, will be sent directly to the user and the CSO.

Requesting Statewide Access

- In order to establish a Cardinal Statewide account, please retrieve the current version of the Cardinal Security Statewide Access Form (Cardinal Form SE-SW-001) from the Cardinal Project website at: http://www.cardinalproject.virginia.gov/security.
- The agency Cardinal Security Officer (CSO) submits the Cardinal Security Statewide Access Form (Cardinal Form SE-SW-001) to the Cardinal Security Team at the following email address (cardinal.security@doa.virginia.gov) to have the account created.

To Add or Update Core User Access

1. Under **Security Action Requested** select the Add/Update Core user Access for users who need to be granted core roles or an update to an existing core user access.
2. Complete the Cardinal Security Form, checking every role the user needs (i.e., roles should be selected for all Cardinal applications the user needs access to, even if you are only making changes to roles in one application).
3. If you are submitting a form to delete a role, you will need to check every role the user currently needs and simply do not check the role you want deleted. **The Cardinal Security Team will remove all roles that are not checked on the form.**
4. When updating an existing core user's access, run the PT_SEC_USER_ROLES query (in HCM and/or FIN as applicable) to identify the user's current access using the following path: **Main Menu > Reporting Tools > Query > Query Viewer. Key in the user's Cardinal User ID.**
5. To view all of your Agency users, run the V_PT_SEC_ROLE_USERS query (in HCM and/or FIN as applicable). This query will show users and the roles assigned. You can also put in criteria to confirm if an account has been locked.
6. Provide all required signatures – user, user's supervisor, Cardinal Security Officer and DOA Approver if conflicting roles, statewide roles, or statewide permission lists are requested.
7. Email the completed form to the Cardinal.Security@doa.virginia.gov mailbox.

To Remove ALL Core User roles or Lock Out Core Users

1. Under **Security Action Requested** select the Remove/Lock Out Core User access for existing users whose core roles need to be removed. Actual account Lock Outs will only be completed for Contract Workers or HR Level 4 users, as they do not need ongoing system access to Employee Self-Service (ESS).
2. Complete the **User Information** section of the Cardinal Security Form.
3. Provide signatures from the user's supervisor and the Cardinal Security Officer.
4. Email the completed form to the Cardinal.Security@doa.virginia.gov mailbox.
5. In lieu of the Cardinal Security Form, the Cardinal Security Officer may send an email to Remove ALL Core User roles or Lock Out a Core User Cardinal account. Include the user's name, user's Cardinal ID, Business Unit, Department ID, Supervisors' Name and copy the user's supervisor on the email.

Overview of each section of the Cardinal Security Statewide Access Form:

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

SECURITY ACTION REQUESTED (select one)	
☐ Add/Update Core User Access (complete all applicable fields and roles)	☐ Remove/Lock Out Core User Access (complete User Info Section Only)

   a. **Add/Update Core User Access –** Check this box to grant Core User roles or update an existing Core User account.

   b. **Remove/Lock Out Core User Access –** Check this box if all Core User roles should be removed or if account needs to be locked for a contractor or HR Level 4 user.

2. **User Information Requested** (Required)

USER INFORMATION		
Name - Last, First, Middle Initial	Business Email Address - *@agency.virginia.gov*	
Employee ID:	Cardinal User ID:	
User's Job Title:	Business Unit:	Department ID:
Is the User a contract worker or HR Level 4 employee? If so, check box and provide User's Supervisor Name and Employee ID: ☐		
Supervisor Name:	Employee ID:	

   a. **Name –** Last, First, Middle Initial (e.g., Doe, John B.)

   b. **Name Change –** Check this box if this is an existing Core User with a name change. Employees should initiate all name changes with their agency HR department.

   c. **Business Email Address –** Enter the user's business email address (e.g., John.Doe@agency.virginia.gov) (Note: For new COVA agency users, make sure users have logged on to their email in order for their account to show up in OKTA Directory before submitting security form)

d. **Employee ID –** 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.

e. **Cardinal User ID –** Needed for Existing Users (including ESS users requesting Core User access).

   i. Leave this field BLANK for New Contractors and HR Level 4 employees.

   ii. If you are unaware of a users' existing ID please run the V_PT_SEC_ROLE_USERS query (in HCM 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).

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

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

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

i. **Check box if contract worker or HR Level 4 employee?** Check this box only if the user is a Contract Worker or HR Level 4 employee (e.g., without a Cardinal Employee ID).

j. **Provide Supervisor Name and supervisor Employee ID Number for contract workers and HR Level 4 employees Only**

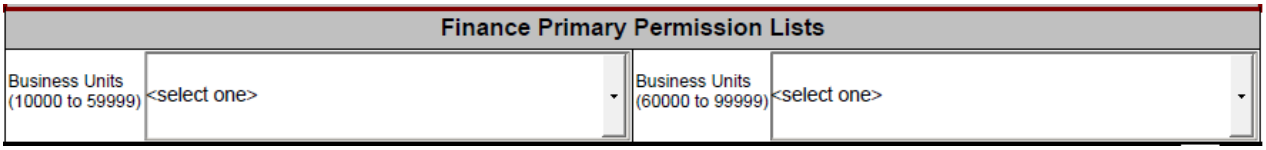
   i. Supervisor's Name (e.g., Doe, John B.)

   ii. Supervisor's Employee ID Number - Employee ID Number is an 11-digit number assigned by Cardinal (e.g., 00123456700). You must enter the full 11-digit number on this form.

3. **FIN Section**

Complete this section as applicable for users requiring core access to FIN.

a. **Finance Primary Permission Lists**



   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.

b. **Finance Read Only Access**

Check here if only requesting Read Only Access to FIN:		

i. Check box if user is only requesting Read Only access to FIN and needs no additional FIN roles.

ii. Read Only roles ***(Cardinal Reporter, Cardinal Viewer and PeopleSoft User)*** will be assigned. These roles are also assigned to users automatically when other FIN Core roles are selected.

c. **Finance Expense Approver Profiles**

Finance Expense Approver Profiles			
☐ Agency Head	☐ Fiscal Officer	☐ DOA Pre Audit *(DOA Only-Statewide)*	☐ Check to Remove Profile
If **Agency Head** or **Fiscal Officer**, enter **Business Unit(s) and Department ID number(s)** user approves.			

i. **Expense Approver Profiles** – If user is an Expenses Approver and need a profile for transactions to route based on Department IDs, please check only one profile per user. You must supply the Department ID Numbers user approves for Agency Head and Fiscal Officer. Profile is not needed if user is a supervisor or backup approver.

ii. **Check to Removal Profile** – If expense profile is no longer needed on user setup, please check box to have it removed.

d. **Finance Accounts Payable Roles** (check all roles requested)

Finance Accounts Payable Roles (check all roles requested)		
☐ Supplier Conversation Processor	☐ Voucher Processor	☐ Special Voucher Processor
☐ Voucher Approver*	☐ HCM Voucher Processor	☐ Voucher Upload Error (Interfacing Only)
☐ Payment Reconciler	☐ 1099 Administrator	☐ Expenses Employee
☐ Expense Processor	☐ Employee Profile Sync Maintenance	☐ Expenses Approver
☐ Expense Reassign	☐ Secure Payment Reporter	☐ Petty Cash Processor
☐ Payment Cash Configurator	☐ Workflow System Administrator	☐ EDI Viewer (Tier II and Tier III Only)
Statewide Central Roles:		
☐ Supplier Maintenance Specialist	☐ Supplier Maint Spreadsheet Upld	☐ EDI Coordinator
☐ Payment Processor	☐ Special Payment Processor	☐ Banking Configurator
☐ Paycycle Configurator	☐ Travel Expense Configurator	☐ Voucher Spreadsheet Processor
☐ Voucher Spreadsheet Approver	☐ Payment Cash Trans Override	☐ Oversight Viewer
☐ DOA Special Paycycle Processor	☐ Statewide Pre Audit Approver	

*If **Voucher Approver**, enter **Accounts Payable Business Unit number(s)** user approves.	
***DJJ, DBHDS, Treasury, DOA & CSA ONLY**-If **Voucher Approver**, also enter **Dept ID number(s)** user approves.	

i. **Voucher Approver* role –** if checked you must list the Accounts Payable Business Unit Numbers user approves. DJJ, DBHDS, Treasure, DOA and CSA only must also list the Department ID Numbers user approves in the box provided.

ii. **AP Department of Accounts Only Statewide Roles**– Are not available to agencies. These roles may only be selected by Department of Accounts (DOA) users.

e. **Finance Accounts Receivable Roles** (check all roles requested)

Finance Accounts Receivable Roles (check all roles requested)	
☐ Funds Receipts Processor	☐ Funds Receipts Manager
☐ Funds Receipts Processor for Multiple GL BU (Restricted)	☐ Funds Receipts Manager Multi BU (Restricted)

i. **AR Restricted Roles** – requires additional DOA approval. (refer to the Security Handbook).

f. **Finance General Ledger Roles** (check all roles requested)

Finance General Ledger Roles (check all roles requested)		
☐ Journal Processor	☐ Journal Processor - Interfacing	☐ Journal Approver*
☐ Agency Chartfield Administrator	☐ Budget Processor	☐ Budget Approver
Statewide Central Roles		
☐ GL nVision Executer	☐ ACFR Processor	☐ Statewide Journal Approver
☐ Statewide ChartField Admin	☐ GL Tree Combo Maintenance	☐ Statewide GL Sys Administrator
☐ Statewide GL Sys Processor	☐ Statewide Budget Administrator	☐ Statewide Budget Processor
☐ Statewide Budget Approver	☐ GL Revenue Reporter	☐ DOA Journal Bypass
☐ Journal Source Bypass	☐ SPO Crosswalk Configurator	
*If **Journal Approver**, enter **General Ledger Business Unit Number(s)** user approves.		
***DJJ, DBHDS, Treasury, DOA, and CSA ONLY** - If **Journal Approver**, also enter **Department ID number(s)** user approves.		

i. **Journal Approver* role –** if checked you must list the General Ledger Business Unit Numbers user approves. DJJ, DBHDS, Treasury, DOA and CSA only must also list the Department ID Numbers user approves in the box provided.

ii. **GL Department of Accounts Only Statewide Roles –** are not available to agencies. These roles may only be selected by Department of Accounts (DOA) and Tax users.

g. **Business Intelligence Section (Finance Only)**

Complete this section as applicable for users requiring core access to BI. Note: General access to Cardinal Business Intelligence is granted automatically with FIN Core User access.

Business Intelligence Section (Finance Only) (if applicable)*
☐ BI Adhoc User (Restricted)

i. **BI Adhoc User role** – requires additional DOA approval. (refer to the Cardinal Security Handbook).

4. **HCM Section**

Complete this section as applicable for users requiring core access to HCM.

HCM Section - Benefits, Human Resources, Payroll and Time & Attendance Roles (if applicable)

a. **Human Capital Management (HCM) Primary Permission List**

HCM Primary Permission Lists			
Business Units (09000 to 59999)	<select one>	Business Units (60000 to 99999)	<select one>

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:
- 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.**

b. **HCM Benefit Roles (check all roles requested)**

HCM Benefits Roles (check all roles requested)		
☐ Benefits Administrator	☐ Benefits Read Only	☐ HBO Benefits Support
Statewide Central Roles:		
☐ OHB Benefits Administrator	☐ OHB Benefits Operations	☐ OHB Benefits Config Read Only
☐ VRS Benefits Administrator	☐ TLC Datasheet Administrator	

i. OHB roles are for users in the DHRM Office of Health Benefits Only.
ii. VRS role is for users in the Virginia Retirement System agency Only.

c. **HCM Human Resources Roles** (check all roles requested)

HCM Human Resources Roles (check all roles requested)		
☐ HR Administrator	☐ HR Position Management	☐ HR Manager Reports
☐ HR Read Only	☐ HR Read Only Sensitive Data	☐ EPR Only Entry
Statewide Central Roles:		
☐ HBO HR Administrator	☐ DHRM HR Operations	☐ DGS Reporter
☐ DVS Reporter		

i. HR Administrator role cannot be assigned to users with the PY Administrator role.
ii. DHRM role is for users in the Department of Human Resource Management agency Only.
iii. DVS role is for users in DVS agency Only.
iv. DGS role is for users in DGS agency Only.

d. **HCM Payroll Roles** (check all roles requested)

HCM Payroll Roles (check all roles requested)		
☐ Payroll Administrator	☐ Payroll Read Only	☐ SPOT Approver
☐ Payroll Budget Processor		
Statewide Central Roles:		
☐ SPO Payroll Operations	☐ SPO Payroll Processor	☐ SPO Payroll Garnishment Admin
☐ SPO Payroll Super User	☐ SPO Configurator Read Only	

i. PY Administrator role cannot be assigned to users with the HR Administrator role or the HR Position Management role
ii. It is recommended to assign the Payroll Budget Processor role to a user in the Finance or a user with the HR Administrator role.
iii. SPO roles are for users in the DOA's State Payroll Operations Only

e. **HCM Time and Attendance Roles** (check all roles requested)

HCM Time and Attendance Roles (check all roles requested)		
☐ Absence Administrator	☐ Absence Supervisor	☐ Time & Labor Administrator
☐ Employee TL Setup	☐ Time & Labor Supervisor	☐ Timekeeper
☐ TA Interface Administrator	☐ Delegation Administrator	☐ TA Reporter
☐ TA Restricted Special Approver	☐ TA Expired Grace Approver	

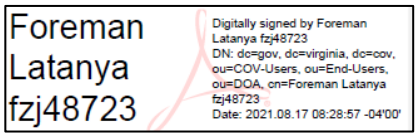
i. Employee T& L Setup role should only be assigned in conjunction with the Time & Labor Administrator and/or Absence Administrator role.
ii. Delegation Administrator role should only be assigned to a limited number of Core Users, as this is a very powerful role.
iii. TA Restricted Special Approver and TA Expired Grace Approver roles should be assigned to a maximum of three users at each agency and must be assigned to at least one user at each agency.

5. **Approvals**

Access Approvals			
By signing below, I acknowledge that I understand transactions added/ updated in the Cardinal system should be in accordance with the Commonwealth Accounting Policy and Procedures Manual Cardinal Topics 20310 and Cardinal Topic 70220.		By signing below, I certify that the Cardinal access requested for this user is necessary to perform his/her current job responsibilities. I also acknowledge this request is in accordance with the Commonwealth Accounting Policies and Procedures Manual Cardinal Topics 20310 and 70220.	
User Printed Name	Date	Supervisor Printed Name	Date
User Signature (sign above)		Supervisor Signature (sign above)	
I have reviewed this request for access and certify it is in accordance with the Commonwealth Accounting Policies and Procedures Manual Cardinal Topic 20310, Cardinal Topic 70220, and the Cardinal Security Handbook.			
Cardinal Security Officer Printed Name	Date		
Cardinal Security Officer Signature (sign above)			

a. **Certification Statement –** user's printed name, signature and date.
b. **Certification Statement –** supervisor's printed name, signature and date.
c. **Certification Statement –** Cardinal Security Officer (CSO) printed name, signature and date.
d. **Digital Signatures** are allowed only if they include a system generated date stamp as shown in the example below:

Example of Digital Signature:



e. We will accept email approvals from 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."
- **Supervisor** – "Please accept this email as my approval of the attached form as the supervisor."
- **Cardinal Security Officer** – "Please accept this email as my approval of the attached form as the Cardinal Security Officer."

7. **Department of Accounts Approval**

Department of Accounts Approval (as required)	
☐ Segregation of Duties Exception	☐ Statewide Permission List Request
DOA Approver Printed Name	Date
DOA Approver Signature (sign above)	

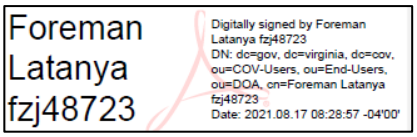
a. As a general rule, Segregation of Duties (SOD) role combinations will not be granted to Cardinal users. Exceptions can be requested for agencies where limited staffing is available or special circumstances exist.

b. Before completing or submitting a security form where an SOD role combination conflict is being requested for a user, the agency should first complete the following steps in order to obtain approval for an agency SOD conflict exception.

i. Submit a written request to DOA's Director of General Accounting (gacct@doa.virginia.gov) that includes:
- Exceptions requested
- Justification for the exception

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

Example of Digital Signature:



d. We will accept email approvals from 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:

- **DOA Approver** – "Please accept this email as my approval of the attached form as the DOA Approver."

8. **Comments/Notes Section (Optional)**

Comments/Notes

a. Area for any additional information