Table of Contents

Overview

Introduction

The Commonwealth's new financial accounting and reporting system, Cardinal, is built on PeopleSoft version 9.1. There are three functional areas included in the base Cardinal system, which include: 1) General Ledger, 2) Accounts Payable, and 3) Accounts Receivable-Funds Receipts. However, there are four software modules included:
General Ledger
Accounts Payable
Expenses (non-payroll employee reimbursements)
Accounts Receivable

The business processes by Functional Area include the following:
General Ledger – business processes:
- System Setup and ChartFields
- Create and Process Budget Journals
- Create and Process Journals
- Period Close

Accounts Payable – business processes:
- Establish and Maintain Vendors
- Enter and Process Vouchers
- Expense Processing
- Process Payments
- Process 1099

Accounts Receivable – business processes:
- Enter Fund Receipts

The Cardinal Security Team is responsible for processing Cardinal access requests.

Policy

Cardinal Access Control

Cardinal Access Control is maintained by the Agency through their **Cardinal Security Officers** and by the Cardinal Security Team. The Cardinal Security Form must be completed by the Cardinal Security Officer (CSO), required approval signatures obtained, and the form submitted to the Cardinal Security Team in order for access to be granted to Cardinal. Training on Cardinal functionality and processes may also be required prior to access being granted.

Access is granted based on the specific work that an employee needs to perform and the associated Cardinal security role(s). The **Cardinal Security Handbook** contains a description of each security role. See *Agency Requirements* for further guidance.

Agency Requirements

Agencies must have sufficient and adequate controls and security over their data and systems.

Agencies should have policies and procedures in place for granting and periodically reviewing access to 1) Cardinal and 2) agency information systems. Access should be based on absolute necessity and use. Individuals who do not use their access frequently in the course of their jobs should be removed. These procedures should include processes for removing access timely for employees that have left the agency. The policies and procedures should include review and approval of access granted as well as the maintenance of documentation of user additions, deletions and periodic user reviews.

Agencies should develop and implement procedures, guidelines, and business practices that facilitate the safekeeping of critical data, which includes financial data. Agencies should ensure compliance with the Commonwealth's Information Security Standard contained in the current version of the ITRM Standard SEC 501 maintained by the Virginia Information Technologies Agency (VITA).

Agencies are also responsible for ensuring employees understand their roles in internal control over the transactions entered into Cardinal. The agency should have policies and procedures for all business processes.

Cardinal Security Form

To gain access to Cardinal, a **Cardinal Security Form** must be completed, signed by the user, and approved by the individual's supervisor, the agency Cardinal Security Officer, and DOA General Accounting (if applicable), and submitted to the Cardinal Security Team. Access should be granted based on the specific work that an employee needs to perform and the associated Cardinal security role(s) that allow those duties to be completed.

It is the agency's responsibility to maintain proper documentation of the approval of access that has been granted to Cardinal users. The agency is responsible for developing and maintaining sufficient internal controls over Cardinal access, which includes developing policies and procedures over the process of adding, changing, and deleting users.

A CSO cannot authorize their own access. The secondary CSO must complete and submit the Cardinal Security Form for the primary CSO.

Cardinal Security Officer

Introduction

Each agency is responsible for selecting **two key individuals** to be designated as Cardinal Security Officers (CSOs). These designations should be noted on the agency's **Authorized Signatories Form (DA-04-121)**. If the CSO changes, an updated **Authorized Signatories Form** should be submitted to DOA as soon as possible.

The Cardinal Security Officers must list their contact information (phone and e-mail) on the **Authorized Signatories Form (DA-04-121)**. This information will be utilized by the Cardinal Security Team.

For further information on the **Authorized Signatories Form**, please refer to CAPP – Cardinal Topic No. 20310, *Expenditures*.

Duties and Responsibilities of the CSO

The duties and responsibilities of the CSO are as follows:

- Sign the Cardinal Security Forms
- Sign the Annual Cardinal Security Review Certification Form on behalf of the agency (Business Unit),
- Ensure and certify that the requested user roles are in accordance with the **Cardinal Security Handbook**,
- Serve as Cardinal Security liaison between their Business Unit and the Cardinal Security Team to resolve Cardinal user security issues,
- Control an agency's access to Cardinal,
- Ensure adequate internal controls exist within the agency to prevent unauthorized access to Cardinal and the Cardinal data and datasets used to submit data to Cardinal. Note: It is the agency's responsibility to design and implement these controls. See subsection entitled *Agency Requirements***,**
- Ensure maintenance of documentation of the approval of access that has been granted to Cardinal users, including the periodic review of that access,
- Submit timely security deletion requests for staff who should no longer have access to Cardinal,
- Ensure receipt of current Cardinal policies, procedures, and subsequent updates related to Cardinal security and prompt dissemination to affected agency personnel.

Agency Cardinal Acknowledge-ment

The Cardinal Security Officers listed on the Authorized Signatories Form have been granted authority to add, change, and delete users in Cardinal that are both preparers and approvers of transactions in Cardinal. Persons granted select approver roles in Cardinal have the authority to approve and release revenue, and expenditure documents and transactions for their agency, department or institution. By approving a transaction in Cardinal, the agency, department or institution, and its employees and agents agree to the certifications contained in the Commonwealth's Accounting Policy and Procedure Manual for the applicable transaction.

Employee Notification of Responsibilities

With the exception of the initial security access granted through Cardinal implementation of the role mapping task, users must sign the Cardinal Security Form which contains an acknowledgement that transactions entered into Cardinal should be in accordance with applicable CAPP – Cardinal Topics. However, the agency is responsible for ensuring employees understand their roles in internal control over the transactions entered into Cardinal. The agency should have policies and procedures for all business processes. See *Agency Requirements* for more information.

Statewide Cardinal Security Handbook

The **Statewide Cardinal Security Handbook** is attached hereto as Exhibit A. The Cardinal security roles are explained in detail in the handbook by role, description, separation (segregation) of duties requirements and other role considerations.

Segregation of Duties Policy Exceptions

Agencies that are very limited on staff may request an exception to the segregation of duties requirements contained in the Cardinal Security Handbook by submitting an exception request that includes the following:

- Providing a written justification to DOA's Director of General Accounting,
- Having this exception request signed by the Agency Head
- Providing a description of the internal controls implemented by the agency to mitigate the lack of segregation of duties.

DOA will notify the Agency and the Cardinal Security Team when the exception is granted.

DOA Contact
Assistant Director, General Accounting
(804) 225-3325
gacct@doa.virginia.gov

Transfer File Security for Interface Agencies

Transfer File Security

Agencies that utilize their own internal financial systems and interface (transfer files) to Cardinal must have sufficient and adequate controls and security over the data and systems. This includes but is not limited to:

- **Access controls:** Agencies should have policies and procedures in place for granting and periodically reviewing access to 1) internal financial systems, 2) Cardinal, and 3) supporting information systems. Access should be based on absolute necessity and use. Individuals who do not use their access frequently in the course of their jobs should be removed. These procedures should include processes for removing access timely for employees that have left the agency. The policies and procedures should include review and approval of access granted as well as the maintenance of documentation of user additions, changes, deletions and periodic user reviews.
- **Information Security:** Agencies should develop and implement procedures, guidelines, and business practices that facilitate the safekeeping of critical data, which includes financial data. Agencies should ensure compliance with the Commonwealth's Information Security Standard contained in the current version of the ITRM Standard SEC 501 maintained by the Virginia Information Technologies Agency (VITA). **Agencies are responsible for ensuring the secure transfer of accurate and complete data to Cardinal.**

See CAPP – Cardinal Topic No. 70210, *Cardinal Media Interface Requirements*, for account access forms and security protocols for file transfer.

Internal Controls

Internal Control

The control of an agency's access to Cardinal is vital. The CSO is responsible for ensuring the existence of a comprehensive system of internal control over both online and offline access to Cardinal files. This access control is vital to ensure the integrity of accounting transactions submitted to Cardinal. See the subsections *Agency Requirements* and *Transfer File Security* for more information. The internal controls must be documented sufficiently to allow examination by the Auditor of Public Accounts. DOA is not responsible for the existence, design, or function of such internal control systems. See CAPP – Cardinal Topic No. 10305, *Internal Control*, for further guidance.

Records Retention

Records Retention

Cardinal access records and documentation must be retained for three (3) years or until audited by the Auditor of Public Accounts, whichever is longer. See CAPP – Cardinal Topic No. 21005, *Records and Retention*, for further guidance.

Subject Cross References

References

CAPP – Cardinal Topic No. 10305, *Internal Control*
CAPP – Cardinal Topic No. 21005, *Records and Retention*
CAPP – Cardinal Topic No. 20310, *Expenditures*
CAPP – Cardinal Topic No. 70210, *Cardinal Media Interface Requirements*

Suggested Forms and Job Aids

Suggested Forms and Job Aids

The following form can be found on the Cardinal Website, under Statewide Toolbox – Forms, DOA Forms:

Authorized Signatory Form (DA-04-121)

The following can be found on the Cardinal Website, under Statewide Toolbox – Cardinal Security:

Cardinal Security Form

Instructions

Additional job aids and training materials may be available on the Cardinal website.

Contacts

Assistant Director, DOA General Accounting
☎ (804) 225-3325
✉ gacct@doa.virginia.gov

Cardinal Security
✉ Cardinal.Security@doa.virginia.gov

Exhibit A: Cardinal Security Handbook – Statewide

Statewide Cardinal Security Handbook starts on page 11.

Summary of Cardinal Security Handbook Changes as of January 29, 2016:

1. New roles added to the handbook
    a. Accounts Payable Roles
        i. Travel Expense Configurator
    b. Accounts Receivable Roles
        i. Funds Receipt Manager Multi BU
    c. Additional Roles Section
        i. APA Audit Special
        ii. Audit Inquiry
    d. Statewide Roles
        i. DOA Special Paycycle Processor
        ii. Voucher Spreadsheet Processor
        iii. Voucher Spreadsheet Approver
        iv. Oversight Viewer
        v. GL Revenue Reporter
        vi. DOA Journal Bypass

Statewide Security Handbook

Cardinal
Commonwealth of Virginia

January 2016

TABLE OF CONTENTS

Cardinal Security Handbook

Each agency is established as a Business Unit in Cardinal and each user in Cardinal is assigned a Row Level Security permission list. This permission list determines the Business Units that the user can access. The purpose of Row Level Security is to prevent users from being able to modify or view data for other agencies. A user can only view, enter, or process transactions for Business Units included in their Row Level Security permission list.

Cardinal users need to be assigned the appropriate roles and security settings in the Cardinal System to have access to do their jobs. This Cardinal Security Handbook is designed to help agencies determine the correct roles for Cardinal users.

Cardinal Security Officers (CSO)

The Cardinal Security Officers listed on the Department of Account (DOA) Authorized Signatories Form (DA-04-121) have been granted authority to authorize the Cardinal Security Team to add, update and delete users in Cardinal that are both preparers and approvers of transactions in Cardinal. By approving a transaction in Cardinal, the agency, department or institution, and its employees and agents, agree to the certifications contained in the Commonwealth Accounting Policy and Procedure Manual for the applicable transaction.

Cardinal Security Form

The Cardinal Security Form must be completed by the applicable agency's Cardinal Security Officer (CSO). The form should include required signatures prior to submitting to the Cardinal Security Team, in order for access to be granted in Cardinal.

The Cardinal Security Form can be found in the Statewide Toolbox tab on the Cardinal website using the following path:

Statewide Toolbox > Cardinal Security > Cardinal Security Form (SE-SW-001)

Use this form to:

- Assign users to roles within Cardinal
- Update existing Cardinal user information
- Lock out users no longer requiring access to Cardinal

The Cardinal Security Officer will submit the completed form to the Cardinal Security Mailbox at: cardinal.security@doa.virginia.gov

Cardinal User Roles

Use the Cardinal Security Handbook as a reference when completing the Cardinal Security form. It defines Cardinal roles by functional area.

You will find the following information in the handbook regarding Cardinal roles:

- Role descriptions
- Segregation of duties
- Other role considerations

Segregation of Duties Policy Exceptions:

Several combinations of Cardinal security roles have been noted as potential segregation of duty (SOD) conflicts in this handbook. As a general rule, 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. 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.

- Submit a written request to DOA's Director of General Accounting (email:gacct@doa.virginia.gov) that includes:
    - Exception requested
    - Justification for the exception
    - Description of the internal control implemented by the agency to mitigate the lack of segregation of duties
    - Approval (signature) from your Agency Head
- DOA General Accounting will notify the agency in writing if the exception is granted.

Once the SOD Exception has been approved by DOA General Accounting, the agency should take the following additional steps when submitting a Cardinal Security Form (SE-SW-001) for any user requesting SOD conflicting role combinations:

- Complete the Cardinal Security form (flagging the SOD Exception), attach a copy of the DOA General Accounting notification granting approval of the **applicable** agency exception
- Scan and email the form and exception approval notice to DOA's Director of General Accounting (email:gacct@doa.virginia.gov)
- If approved, DOA General Accounting will sign the form, scan and email the approved form to Cardinal Security at cardinal.security@doa.virginia.gov and to the Cardinal Security Officer for that agency

Accounts Payable User Roles

Accounts Payable (AP) is the main source of all non-payroll payment information for a financial entity. AP includes the following processes:

- Establish and Maintain Vendors
- Enter and Process Vouchers
- Expense Processing
- Process Payments
- Process 1099

About this Section

This section outlines the available roles for AP in Cardinal. Use the AP User Roles and Descriptions Table below to determine the appropriate AP roles needed by agency users in Cardinal.

The AP User Roles & Descriptions Table provides the following information:

- Role Descriptions
- Segregation of Duties
- Other Role Considerations

AP User Roles & Descriptions Table

Descriptive Role Name	Role Description	Segregation of Duties	Other Role Considerations
Vendor Conversation Processor V_AP_COVA_VENDOR_CONVERSATION	This role is for users routinely involved in the Vendor Procure to Pay process who have a need to interact with vendors. This role has access to: • Record Vendor Conversations	N/A	N/A
Voucher Processor V_AP_COVA_VOUCHER_PROCESSOR	This role has access to: • Enter and maintain vouchers • Review voucher accounting entries • Delete vouchers	Should not be given to a user with the Voucher Approver or Final Voucher Approver roles.	N/A

Descriptive Role Name	Role Description	Segregation of Duties	Other Role Considerations
Special Voucher Processor V_AP_COVA_SPEC_VCHR_PROCESSOR	This role has access to everything the Voucher Processor has. In addition, this role has access to: • Manually schedule payments • Record manual payments • Update vouchers with payment offsets (liens, garnishments) • Unpost Vouchers • Close vouchers • Place holds on vouchers	Should not be given to a user with the Voucher Approver or Final Voucher Approver roles.	This role is the only role that is able to update/ correct Scheduled Due Date when the 00PP pay term is used.
Voucher Approver V_AP_COVA_VOUCHER_APPROVER	This role has access to: • Approve vouchers	Should not be given to a user with the Final Voucher Approver, Voucher Processor, Petty Cash Processor Special Voucher Processor or Workflow System Administrator roles.	N/A
Final Voucher Approver V_AP_COVA_VCHR_FINAL_APPROVER	This role has access to: • Approve vouchers Note: There must be a user with the Voucher Approver level role for the Final Voucher Approver level role to be used. This is an option for a 2nd level of agency voucher approval.	Should not be given to a user with the Voucher Approver, Voucher Processor, Petty Cash Processor Special Voucher Processor or Workflow System Administrator roles.	N/A

Descriptive Role Name	Role Description	Segregation of Duties	Other Role Considerations
Voucher Upload Error Reporter V_AP_COVA_VCHR_ERROR_REPORTER	This role has access to: • View and execute the voucher upload error report. Note: This report can contain sensitive data, so this role should only be assigned to authorized users based on agency secure data policies.	N/A	This role is only available for interfacing agencies.
Payment Reconciler V_AP_COVA_PAYMENT_RECONCILER	This role has access to: • Manually reconcile petty cash payments	N/A	N/A
1099 Administrator V_AP_COVA_1099_ADMINISTRATOR	This role has access to: • Create 1099 reporting file to IRS • Create vendor Copy-B reports • Run 1099 processes • Make adjustments for 1099 reporting • Run 1099 reports and queries containing sensitive data	N/A	This role will have access to sensitive data, as it will be able to view Vendor TIN on the vendor record.
Expenses Employee V_AP_COVA_EXPENSES_EMPLOYEE	This role has access to: • Enter travel authorizations • Enter cash advances • Enter expense reports for self or as a proxy to others • View their own employee profile • Delete travel authorizations • Delete cash advances • Delete expense reports • Cancel travel authorizations	Should not be given to a user with the Expense Approver role.	Users with this role must be designated by the agency as an Expense Proxy.

Descriptive Role Name	Role Description	Segregation of Duties	Other Role Considerations
Expenses Processor V_AP_COVA_EXPENSES_PROCESSOR	This role has access to: • Reconcile cash advances • Close expense reports • View expense accounting entries • Authorize an employee to enter expenses on behalf of another employee (proxy configuration) • Create templates • Run Expense reports with sensitive data • View Expense Report and Cash Advance payments and cancelations.	N/A	N/A
Employee Profile Maintenance V_AP_COVA_EMP_PROFILE_MAINT	This role has access to: • Create/update employee profiles not including banking information	N/A	The agency will need to maintain employee profiles. There should be at least one individual at each agency with this role.
Expense Approver V_AP_COVA_EXPENSES_APPROVER	This role has access to: • Approve expense transactions	Should not be given to a user with the Expenses Employee role.	Any user that may approve expenses should be given this role, even if they are not designated as a Fiscal Officer or Agency Head. Users with this role must be designated by the agency as an Expense Proxy.
Expenses Reassign V_AP_COVA_EXPENSES_REASSIGN	This role has access to: • Move expense transactions from one approver's worklist to another	N/A	N/A

Descriptive Role Name	Role Description	Segregation of Duties	Other Role Considerations
Secure Payment Reporter V_AP_COVA_SECURE_PMNT_REPORTER	This role has access to: • Run payment reports containing sensitive data • Run Payment History by Vendor, Payment History by Bank, Payment History by Payment, and Trial Register reports	N/A	N/A
Petty Cash Processor V_AP_COVA_PETTY_CASH_PROCESSOR	This role has access to: •Create petty cash checks via express pay page	Should not be given to a user with the Voucher Approver or Final Voucher Approver roles.	N/A
Payment Cash Configurator V_AP_COVA_PYMNT_CASH_CONFIG	This role has access to: •Set payment priorities for specific vouchers, expense reports, and/or cash advances via cash checking transaction priority page	N/A	N/A
WF System Administrator V_COVA_WF_WL_REASSIGN	This role has access to: •Move worklist items from one User to another. •Set the Alternate User ID to which future transactions will flow.	Should not be given to a user with approval access to Vouchers and Journals.	This role should be assigned to one User and no more than 2 backups per agency.
EDI VIEWER V_AP_COVA_EDI_SRC	This role has access to: •Run the query for the EDI vendor list. Note: This role is available to Tier II and Tier III agencies only.	N/A	This role will have access to sensitive data, as it will be able to view Vendor TIN.

Accounts Payable Workflow

About this Section

Workflow is an automated process that takes a Cardinal transaction and routes it to the next approver level for action (approve or deny).

Expenses Workflow

Expense transactions are routed for approval based on Department IDs

The following Expense role(s) are tied to workflow:

- Expense Approver

As a general rule, only employees assigned to the Expense Approver role because it deals with the approval of expenses. Non-employees cannot be assigned to this role. When an expense transaction is entered for an employee, the person who is identified in Cardinal as their supervisor in their expense profile will be the first level of Cardinal approval for online agencies. This is not necessarily their operational supervisor, as not all supervisors have users IDs in Cardinal. The supervisor approver level does not apply for interfacing agencies.

Please use the information provided below to select the appropriate Expense Approver workflow profile for your users in Cardinal and list the department ID ranges for which the user will approve. **A user can only be assigned to one of the below expense approver profiles and only one user per profile/department range combination.**

Expense Approver Profile	Profile Description
Fiscal Officer	Approval of all expense reports, travel authorizations, and cash advances. This approval level is optional for online agencies.
Agency Head	Approval of expense reports and travel authorizations containing expense amounts over the allowable amount and/or over $500. Interfacing agencies will not have the Agency Head approval level in Cardinal.
DOA Pre Audit	Approval of expense reports for Capital Outlay projects. This role may only be selected by employees of the following agency(s): Department of Accounts – General Accounting

Voucher Workflow

Users assigned the following role will be assigned the agency specific route control profile(s) in order to properly route transactions for approval. Route control profiles are assigned to users to identify the areas on which they work.

- Voucher Approver or Final Voucher Approver

If the user is assigned to the Voucher Approver or Final Voucher Approver role, agencies will need to identify the Business Unit number(s) for which that user can perform approvals. Please note, the Final Voucher Approver role is only applicable to agencies that have previously selected two levels of voucher approval.

Accounts Receivable User Roles

Accounts Receivable (AR) is the functional area that handles a series of accounting transactions dealing with funds receipts. AR includes the following process:

- Enter Funds Receipts

About this Section

This section outlines the available roles for AR in Cardinal. Use the AR User Roles & Descriptions Table below to determine the appropriate AR roles needed by agency users in Cardinal.

The AR User Roles & Descriptions Table provides the following information:

- Role Descriptions
- Segregation of Duties
- Other Role Considerations

AR User Roles & Descriptions Table

Descriptive Role Name	Role Description	Segregation of Dutie	Other Role Consideration
Funds Receipt Processor V_AR_COVA_FUNDS_REC_PROCESSOR	This role has access to: • Enter deposits for miscellaneous payments • Enter direct journal accounting entries for deposits	N/A	N/A
Funds Receipt Manager V_AR_COVA_FUNDS_REC_MANAGER	This role has access to everything the Funds Receipts Processor role has. In addition, this role has access to: • Review and Complete direct journal accounting entries • Budget Check journal entries online • Group and approve deposits with a custom deposit certificate for submission to CARS and the Department of Treasury.	N/A	N/A

Descriptive Role Name	Role Description	Segregation of Duties	Other Role Consideration
Funds Receipts Processor for Multiple GL BU **V_AR_COVA_FUNDS_REC_MULTIBU**	This role has access to: • Enter payments and deposits • Enter directly journaled payments • Process for multiple GL business units on a Funds Receipt transaction	The role will be restricted to a select group of users from the Department of the Treasury.	Approval is required by a designated Cardinal DOA Approver to obtain this role.
Funds Receipt Manager Multi BU **V_AR_COVA_FUNDS_REC_MGR_MULTI**	This role has access to everything the Funds Receipts Multi BU Processor role has. In addition, this role has access to: • Review and Complete direct journal accounting entries for Multi BU transactions • Budget Check journal entries online for Multi BU transactions Group and approve deposits with a custom deposit certificate for submission to CARS and the Department of Treasury.	N/A	Approval is required by a designated Cardinal DOA Approver to obtain this role.

General Ledger User Roles

General Ledger (GL) is the functional area that handles the set of financial accounts used to: accumulate the results of transaction processing, create budgets, generate financial statements and provide source financial data for reporting purposes. GL includes the following processes:

- System Setup and ChartFields
- Create and Process Budget Journals
- Create and Process Journals
- Period Close

About this Section

This section outlines the available roles for GL in Cardinal. Use the GL User Roles & Descriptions Table below to determine the appropriate GL roles needed by agency users in Cardinal.

The GL User Roles & Descriptions Table provides the following information:

- Role Descriptions
- Segregation of Duties
- Other Role Considerations

GL User Roles & Descriptions Table

Descriptive Role Name	Role Description	Segregation of Duties	Other Role Considerations
Journal Processor V_GL_COVA_JOURNAL_PROCESSOR	This role has access to: • Enter journals online • Enter spreadsheet journals • Edit journals online • Budget check journals online • Copy a journal • Execute Spreadsheet Upload process (batch process) • Review budget check exceptions	Should not be given to a user with the Journal Approver role.	Agencies cannot enter an “agency to agency” (ATA) journal that crosses business units outside of their control group. Agencies will need to submit requests to DOA General Accounting when an ATA journal is needed (see CAPP Cardinal Topic 20405 for details).
Journal Processor Interfacing V_GL_COVA_JRNL_PROCESSOR_INT	This role is the same as the Journal Processor role above, but it is only available to Interfacing Agencies.	Should not be given to a user with the Journal Approver role.	N/A

Descriptive Role Name	Role Description	Segregation of Duties	Other Role Considerations
Journal Approver V_GL_JOURNAL_APPROVER	This role has access to: • Approve journals • Post journals through batch process or online • Review journal lines • Execute Spreadsheet Upload process (batch process) • Execute Journal Edit through batch process • Execute Journal Budget Check through batch process	This role should not be given to a user with the Journal Processor, Journal Processor – Interfacing or Workflow System Administrator roles.	N/A
Agency ChartField Administrator V_GL_COVA_AGENCY_CF_ADMIN	This role has access to: • Maintain Agency controlled ChartFields (Department, Project, Cost Center, Task, Asset, Agency Use 1, Agency Use 2) • Maintain SpeedTypes/ SpeedCharts	N/A	N/A
Budget Processor V_GL_COVA_BUDGET_PROCESSOR	The Budget Processor is responsible for budget journals at the agency-level. This role has access to: • Enter budget journals, budget transfers and budget adjustments • Upload journals using the Spreadsheet Budget Journal upload • Review and correct budget journal errors	Should not be given to a user with the Budget Approver role.	N/A
Budget Approver V_GL_COVA_BUDGET_APPROVER	The Budget Approver is responsible for agency-level budgets. This role has access to: • Post budget journals through online or batch process • Delete budget journals through online or batch process • Post budget transfers and adjustments • Override agency level budget exceptions Upload spreadsheet budget journals	Should not be given to a user with the Budget Processor role.	N/A

Descriptive Role Name	Role Description	Segregation of Duties	Other Role Considerations
General Ledger nVision Executer V_GL_COVA_NVISION_EXECUTER	This role has access to: • Maintain the scope of nVision reports • Create nVision report requests	This role may only be selected by employees of the following agency/division(s): • Department of Accounts • BOA	This role requires the user to also have the CAFR Processor role.
CAFR Processor V_GL_COVA_CAFR_PROCESSOR	This role has access to: • Enter and report on CAFR ledgers (Cash, Modified Accrual, Full Accrual) .	This role may only be selected by employees of the following agency/division(s): • Department of Accounts • BOA	This role has to be assigned in conjunction with the Journal Processor role in order to be able to enter journal entries to the CAFR ledgers. <or> This role has to be assigned in conjunction with the Journal Approver role to be able to post CAFR entries, although there is no approval process for CAFR entries.

General Ledger Workflow

About this Section

Workflow is an automated process that takes a Cardinal transaction and routes it to the next approver level to approve or deny. The GL Journal Approver is tied to workflow.

Users assigned to the following role will be assigned the agency specific route control profile(s), to properly route transactions for approval. Route control profiles are assigned to users to identify the areas on which they work.

- Journal Approver

If the user is assigned to the Journal Approver role, agencies will need to enter the Business Unit(s) for which that user can perform approvals.

Additional User Roles

The additional roles that follow relate to reporting, queries, PeopleSoft user system setup and Special Approval roles.

About this Section

This section outlines additional roles in Cardinal. Please use the Additional User Roles & Descriptions Table below to understand the roles all Cardinal users will receive.

The Additional User Roles & Descriptions Table provides the following information:

- Role Descriptions
- Segregation of Duties
- Other Role Considerations

Additional User Roles & Descriptions Table

Descriptive Role Name	Role Description	Segregation of Duties	Other Role Consideration
Cardinal Viewer **V_COVA_CARDINAL_VIEWER**	This role has access to: • Read only pages in Cardinal that do not contain sensitive data	N/A	All Cardinal Users will receive this role.
Cardinal Reporter **V_COVA_CARDINAL_REPORTER**	This role has access to: • Run public queries that do not contain sensitive data	N/A	All Cardinal Users will receive this role.
Cardinal PeopleSoft User **V_COVA_PEOPLESOFT_USER**	This role has access to: • Run public queries that do not contain sensitive data	N/A	All Cardinal Users will receive this role.
BI_Adhoc_User **V_BI_ADHOCUSER_FIN**	This role is for select users designated as Cardinal BI reporting super users. This role has access to: • Develop ad hoc private reports and queries in the Cardinal Business Intelligence (BI) application	This role may only be selected by limited users who have been approved to participate in the Cardinal BI Pilot.	Special approval is required by Enterprise Application Director to obtain this role until further notice.
APA Audit Special **V_ALLPAGES_APA_RO**	This role is designated for APA Staff responsible for auditing the Cardinal Financial System. • Read Only access to production database for all business units • Create private queries • Read Only access to Remote Desktop, SQL Developer Read Only & Application Designer	Only PeopleSoft User, Cardinal Reporter, and Cardinal Viewer roles can be assigned to users with the APA role.	Special approval is required by a designated Cardinal DOA Approver to obtain this role.
Audit Inquiry **V_AUDITOR**	This role is for designated Audit Staff responsible for conducting agency audits. This role has access to: • Comprehensive Read Only inquiry including sensitive data.	Only PeopleSoft User, Cardinal Reporter, and Cardinal Viewer roles can be assigned to users with the Auditor Inquiry role.	

Appendix

Statewide Central Roles

Statewide Central Roles are only available to select agencies and/or operations, for example: Department of Accounts (e.g., General Accounting, Commonwealth Vendor Group), Department of Treasury, etc. Any request to assign a Statewide Central Role requires approval from a designated Cardinal DOA Approver or specific designee noted in the table that follows.

About this Section

This section outlines central roles in Cardinal. Please use the Statewide Central Roles & Descriptions Table below to understand the roles in Cardinal that will be controlled by central departments.

The Additional User Roles & Descriptions Table provides the following information:

- Role Descriptions
- Restrictions
- Other Role Considerations

Statewide Central Roles & Descriptions Table

Descriptive Role Name	Role Description	Restrictions	Other Role Considerations
Vendor Maintenance Specialist V_AP_VENDOR_MAIN_SPECIAL	This role has access to: • Enter vendors • Maintain vendors including financial sanctions, TIN matching, and 1099 reporting class setup • Configure Department of Small Business and Supplier Diversity (DSBSD) certification types and conversation keywords	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: CVG • Department of Accounts: General Accounting	Vendor additions and maintenance will be owned by CVG. Users assigned to this role must also be assigned the Vendor Conversation Processor role.
EDI Coordinator V_AP_EDI_COORDINATOR	This role has access to: • Enter EDI banking information for vendors and employees	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A

Descriptive Role Name	Role Description	Restrictions	Other Role Considerations
Payment Processor V_AP_COVA_PAYMENT_PROCESSOR	This role has access to: • View pay cycle exceptions • Cancel payments	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
Special Payment Processor V_AP_COVA_SPEC_PYMNT_PROCESSOR	This role has access to: • Use the Express Payment page to process Emergency Checks	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
Banking Configurator V_AP_COVA_BANKING_CONFIGURATOR	This role has access to: • Set up Commonwealth of Virginia bank accounts	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
Paycycle Configurator V_AP_PAYCYCLE_CONFIGURATOR	This role has access to: • Update check write dates on Pay Cycle	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
Travel Expense Configurator V_AP_TRAVEL_EXPENSE_CONFIG	This role has access to: • Maintain Expense configuration such as locations, lodging rates, mileage rates, per diem, etc.	This role may only be selected by employees of the following agency/division(s): • Department of Accounts	

Descriptive Role Name	Role Description	Restrictions	Other Role Considerations
DOA Special Paycycle Processor V_AP_DOA_SPEC_PAYCYLE_PROC	This role has access to: • Run the special Paycycles for Petty Cash, Wire and Treasury Accounts Payable Business Units	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	Users assigned this role should also be assigned the V_R_DOA_SPC_PAY Row Level Security Permission List.
Statewide Pre Audit Approver V_AP_PRE_AUDIT_APPROVER	This role has access to: • Approve Capital Outlay transactions • Approve Legal Services transactions	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
Voucher Spreadsheet Processor V_AP_COVA_DOA_VCHR_SPD	This role has access to: • Load vouchers into Cardinal using the Spreadsheet Upload	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	Should not be given to users who have the Voucher Spreadsheet Approver, Voucher Approver, or Final Voucher Approver roles.
Voucher Spreadsheet Approver V_AP_COVA_DOA_SPD_APPR	This role has access to: • Approve Spreadsheet Vouchers using the mass approval page	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	Should not be given to users who have the Final Voucher Approver, Voucher Spreadsheet Processor, Petty Cash Processor, Special Voucher Processor, or Workflow System Administrator roles. Users assigned this role should also be assigned the COVA Voucher Approver Role.

Descriptive Role Name	Role Description	Restrictions	Other Role Considerations
Payment Cash Transaction Override V_COVA_PYMNT_CASH_TRANSOVRD	This role has access to: • Record specific business unit/fund combinations for cash checking fund level processing rules of bypass, override and fiscal year option • Record specific vouchers, expense reports, and/or cash advances on cash checking transaction override page	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
Oversight Viewer V_OVERSIGHT_VIEWER	This role has view only access to: • Accounts Payable • Expenses • Vendors • Payments	This role may only be selected by employees of the following agency/division(s): • Department of Accounts	N/A
Statewide Journal Approver V_GL_STATE_JOURNAL_APPROVER	This role has access to: • Approve Journals • Post journals through batch process or online • Review journal lines • Upload import file • Execute Spreadsheet Upload process (batch process) • Execute Journal Edit through batch process • Execute Journal Budget Check through batch process	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A

Descriptive Role Name	Role Description	Restrictions	Other Role Considerations
Statewide ChartField Administrator V_GL_COVA_STATE_CF_ADMIN	This role has access to: • Maintain all Chart of Accounts values • Maintain SpeedTypes/ Speed Charts	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
General Ledger Tree Combo Maintenance V_GL_COVA_TREE_COMBO_MAINT	This role has access to: • Maintain trees in Cardinal Financials • Maintain Combination Edits	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
Statewide General Ledger System Administrator V_GL_COVA_STATE_SYSTEM_ADMIN	This role has access to: • Update Open Periods • Maintain TableSet Controls • Maintain Business Units • Maintain Calendars • Maintain Journal Sources • Maintain Ledger Configuration • Maintain ChartField Value Sets • Maintain Actuals Closing Rules • Maintain Journal Generator templates • Maintain Accounting Entry Definitions • Run ChartField Configurator • Execute and Validate Actuals Close processes	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A

Descriptive Role Name	Role Description	Restrictions	Other Role Considerations
Statewide General Ledger System Processor V_GL_COVA_STATE_SYST_PROCESSOR	This role has access to: • Unlock budget processes and GL Journals	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
Statewide Budget Administrator V_GL_COVA_STATE_BUDGET_ADMIN	This role has access to: •Maintain budget periods •Maintain budget structures •Maintain budget closing rules •Execute and validate Budget Close processes	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
Statewide Budget Processor V_GL_COVA_ST_BUDGET_PROCESSOR	The Statewide Budget Processor is responsible for Central-level Budgets. This role has access to: •Enter and delete budget journals •Enter budget transfers and adjustments •Review and correct budget journal errors •Upload spreadsheet budget journals	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A

Descriptive Role Name	Role Description	Restrictions	Other Role Considerations
Statewide Budget Approver V_GL_COVA_ST_BUDGET_APPROVER	The Statewide Budget Approver is responsible for Central-level Budgets. This role has access to: •Post budget journals through online or batch process •Delete budget journals through online or batch process •Override budgets •Post budget transfers and adjustments •Upload using Spreadsheet Budget Journal upload •Run the budget interface from Performance Budgeting	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	N/A
GL Revenue Reporter V_GL_COVA_REVENUE_REPORTER	This role has access to: •Run and receive the RGL304 General Fund/ Statement of Revenue Collections, Estimates & Transfers report	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting • Department of Taxation	N/A
DOA Journal Bypass V_GL_COVA_DOA_JRNL_BYPASS	This role has access to: •Bypass the Cash Account balancing and Transfer Account balancing Journal Edits	This role may only be selected by employees of the following agency/division(s): • Department of Accounts: General Accounting	This role has to be assigned in conjunction with the Journal Processor or Journal Approver or Statewide Journal Approver role.