Table of Contents

PREFACE ................................................................................................................................. 3
SCOPE .................................................................................................................................... 3
PURPOSE ................................................................................................................................. 3
DEFINITIONS ............................................................................................................................ 3

1. ENTITY eVA SECURITY OFFICER DESIGNATION AND ACCESS LEVEL ......................... 9
   1.1. ENTITY ADMINISTRATIVE HEAD TO APPOINT PRIMARY AND BACKUP SECURITY OFFICERS .......................................................................................................................... 9
   1.1.1. BACKGROUND CHECK FOR ENTITY eVA SECURITY OFFICER .......................................................................................................................... 9
   1.2. BASIC LEVEL SECURITY DELEGATION ........................................................................ 9
   1.3. ADVANCED LEVEL SECURITY DELEGATION ............................................................. 9
   1.3.1. ENTITY eVA SECURITY PLAN REQUIRED ................................................................ 10
   1.3.2. ENTITY ADVANCED LEVEL SECURITY ADMINISTRATION REQUIRED ............... 10
   1.4. EXCEPTION TO SECURITY DELEGATION .................................................................... 10

2. AUTHENTICATION AND AUTHORIZATION – SYSTEM ACCESS ..................................... 11
   2.1. ACCEPTABLE USE OF eVA ....................................................................................... 11
   2.2. UNACCEPTABLE USE OF eVA AND EXCEPTIONS .................................................... 11
   2.3. AUTHORIZING AND SUBMITTING AN eVA USER PROFILE REQUEST ....................... 11
   2.4. PROCESSING APPROVED eVA USER PROFILE REQUEST ......................................... 12
   2.5. USER-ID, PASSWORD & COMPLETION OF eVA ACCEPTABLE USE ACKNOWLEDGEMENT ............................................................................................................ 13
   2.6. PASSWORD REQUIREMENTS .................................................................................... 13
   2.7. PASSWORD CHANGES AND RESETS ....................................................................... 13
   2.8. DEACTIVATION OF eVA ACCESS ............................................................................. 14
   2.9. REACTIVATION OF eVA ACCESS ............................................................................. 15
   2.10. CHANGES IN USER DUTIES AFFECTING eVA ACCESS ........................................... 16

3. SECURITY INCIDENT .......................................................................................................... 16
   3.1. MEASURES FOR INFORMATION SECURITY NON-COMPLIANCE ............................... 16

4. SYSTEM INTEROPRABILITY SECURITY ............................................................................. 17
   4.1. DATA EXCHANGE ...................................................................................................... 17

5. MONITORING, REVIEW AND CERTIFICATION ................................................................ 17
   5.1. SYSTEM MONITORING ............................................................................................ 17
   5.2. QUARTERLY SYSTEM ACCESS REVIEW ................................................................... 17
   5.3. ANNUAL CERTIFICATION OF SYSTEM ACCESS ....................................................... 18
   5.4. RECORDS .................................................................................................................. 18

APPENDIX A REQUEST FOR EXCEPTIONS ............................................................................ 20

APPENDIX B eVA ACCEPTABLE USE ACKNOWLEDGEMENT .................................................. 22

APPENDIX C COVA ENTITY eVA DESIGNATION .................................................................. 26

APPENDIX D eVA ANNUAL USER CERTIFIED REPORT ......................................................... 27

APPENDIX E REQUEST FOR eVA USER PROFILE ................................................................. 28

APPENDIX F REQUEST eVA USER DEACTIVATION ............................................................... 30
PREFACE

Publication Designation
Electronic Procurement Security

Subject
eVA Security Standards

Effective Date
07/01/2015

Compliance Date
10/01/2015

Supersedes
eVA Electronic Procurement System Security Standards dated July 23, 2014

Scheduled Review
One (1) year from effective date

Authority
Code of Virginia § 2.2-1111
(DGS/DPS Authority and Responsibility)

SCOPE

This policy is applicable to all entity employees, contractors, vendors, business partners and any other authorized users of the Commonwealth’s electronic procurement system otherwise known as eVA.

The following are exempt: Public Sector and Non-profit buying Entities that are not part of Commonwealth of Virginia state government (Virginia localities, other states, etc). These entities must maintain a security program that complies with COVA and CGI requirements and is in accordance with any memorandum of understanding or other agreements between the entity and the Department of General Services / Division of Purchases and Supply.

PURPOSE

To define the minimum requirements for authorizing access to eVA by entity personnel, including, but not limited to, managers, administrators, requestors, approvers, and buyers by establishing a practical security environment that meets the following requirements:

- Protecting the confidentiality and integrity of eVA data
- Preventing unauthorized access to eVA
- Verifying adequate security measures are used by all entities using eVA
- Providing a secure method of conducting eVA on-line transactions
- Providing a secure bid placement environment
- Securing eVA user data from unauthorized users
- Securing a vendor’s data from other vendors
- Ensuring that eVA security policies and procedures are consistently enforced

DEFINITIONS

Advanced Level Security Access
Advanced Level Security Access includes all security responsibilities and capabilities given to an Entity eVA Security Officer at the basic level plus access to and responsibility for the user account administration functions (User Management and User Bulkload) on the Secure Portal for their entity.
Basic Level Security Access
Generally, all Entity eVA Security Officers are at the basic level upon initial designation by the Entity Administrative Head. At the basic level, the Entity eVA Security Officer is responsible for approving user role changes within personal profiles and coordinating the user account management process for their entity.

Custodian/Steward
An individual at the agency granted access to a deactivated account for the purposes of completing outstanding changes to purchase orders, receiving or completing active Quick Quotes. The individual shall not perform any approvals in the custodial account.

Department of General Services / Division of Purchases and Supply (DGS/DPS)
The Department of General Services /Division of Purchases is charged by the Code of Virginia § 2.2-1110 to maintain the Commonwealth’s central electronic procurement system. At a minimum this procurement system shall provide for the purchase of goods and services, public posting of all Invitations to Bid, Requests for Proposal, sole source award notices, emergency award notices, and reports on purchases. Every Entity shall utilize the Department of General Services’ central electronic procurement system as their purchasing system beginning at the point of requisitioning for all procurement actions, including but not limited to technology, transportation, and construction, unless otherwise authorized in writing by the Division.

Division of Purchases and Supply (DPS) Account Executive
The Division of Purchases and Supply staff member assigned to the entity to assist them in effectively using and configuring eVA. Advanced Level Security Access will be granted for all assigned entities upon completion of advance level security training and approval by the Global eVA Security Officer.

Entity
Commonwealth of Virginia public body which is defined in the Code of Virginia §2.2-1110 and §2.2-4301 as “any legislative, executive or judicial body, agency, office, department, authority, post, commission, committee, institution, board, political subdivision, or other unit of state government created by law to exercise some sovereign power or to perform some governmental duty, and empowered by law to undertake the activities described in the Virginia Public Procurement Act.” or similar jurisdiction or private organization.

Entity Administrative Head
Entity Administrative Head is used in the code of Virginia to mean the highest ranking person in the entity. For eVA purposes the Entity Administrative Head is the administrative head as used in sections §15.2-1541 (local government) or 2.2-106 (state executive agencies) in the Code of Virginia. For institutions, authorities, universities, legislative or judicial entities the Administrative Head is the highest ranking employee with direct responsibility for the organization’s administrative functions. Customary titles would include Executive Director, VP Administration, Commissioner, Deputy Commissioner for Administration, Clerk, etc.
**Entity eVA Security Officer**  
Individual designated in writing by the Entity’s Administrative Head to administer security of eVA for the organization.

**Entity eVA Lead**  
An Individual designated by the Entity Procurement Director that is responsible for the entity’s day to day eVA functions including working with the Entity eVA Security Officer and the DPS Account Executive to ensure proper agency setup and user access is maintained.

**Entity Procurement Director**  
An individual designated by the Entity Administrative Head that is responsible for the entity’s day to day management of the purchasing function and having been delegated the authority to bind the agency in making contractual commitments.

**eVA Acceptable Use Acknowledgement Form**  
eVA Acceptable Use Acknowledgement Form is an agreement between the user and the DGS/DPS Director that specifically identifies user responsibilities in order to be granted access to eVA. An Acceptable Use Agreement shall be signed before access is given to a user. Refer to Appendix B for written format. Entities may establish and use an electronic equivalent of the written format. The content of the electronic format must be submitted to the eVA Global Security Officer for approval prior to implementation.

**eVA Users**  
Any approved individual that is granted a login and password. When used for the purpose of this document, the term “eVA Users” reflects the secured portal users of eVA (known requestors, known buyers, known receivers).

**Global eVA Security Officer**  
Individual designated at the Commonwealth level to administer overall security of eVA.

**Global eVA Technical Lead**  
Individual designated at the Commonwealth level to oversee all technical aspects of eVA.

**Portal**  
The portal is the electronic gateway through which entities’ and vendors’ transactions pass in order to do business electronically within eVA. The portal presents one face for procurement to entities and vendors.

**Service Provider Administrator (CGI)**  
CGI employee(s) responsible for maintaining security, reliability, and data integrity of the eVA service offering.

**REGULATORY REFERENCES**

- Code of Virginia § 2.2-1110 (DGS/DPS Authority and Responsibility)
- International Standards  
- DGS Information Security Standard ITRM SEC501-09
GENERAL RESPONSIBILITIES

Department of General Services / Division of Purchases and Supply (DGS/DPS)
The Department of General Services /Division of Purchases and Supply is responsible for ensuring the eVA policy and standards are maintained and enforced.

Division of Purchases and Supply (DPS) Account Executive
The Division of Purchases and Supply staff member assigned to the entity to assist them in effectively using and configuring eVA. This staff member shall also be responsible for coordinating Security Access training with the Global eVA Security Officer.

Entity Administrative Head
Entity eVA Security Management and business continuity planning for entity purchasing is the responsibility of the Entity Administrative Head. Each Entity Administrative Head will designate, in writing, primary and backup Entity eVA Security Officer(s) for his/her organization by submitting the “COVA Entity eVA Designation Form” (Refer to Appendix C.)

Entity eVA Lead
Responsible for the entity’s day to day eVA functions including working with the Entity eVA Security Officer and the DPS Account Executive to ensure proper agency setup and user access is maintained.

Entity eVA Security Officer
The Entity eVA Security Officer shall be responsible for ensuring all entity eVA users have signed the eVA Acceptable Use Acknowledgement and maintain a copy either electronically or in hard copy form. The Entity eVA Security Officer is responsible for ensuring Entity Personnel identified in this standard are trained and are aware of their responsibilities to comply with these standards. The Entity eVA Security Officer shall perform the user access review quarterly and annually.

Entity Procurement Director
The Entity Procurement Director shall be responsible for authorizing access to eVA. The procurement director shall notify the Entity eVA Security Officer and the DPS Account Executive in writing of any Entity eVA Lead that is also approved to authorize access to eVA by submitting the “COVA Entity eVA Designation Form” (Refer to Appendix C.)

Global eVA Security Management
Global eVA Security Management is the responsibility of DGS. The DGS Director shall designate the Global eVA Security Officer based on the recommendation of the DPS Director and the Director of DGS Information Systems and Services.

Global eVA Security Officer
The Global eVA Security Officer is responsible for administering, monitoring and facilitating the eVA Security program in compliance with the eVA Security Policy and Standards. This position will also be responsible for developing and maintaining the procedures necessary for the execution of the eVA Security Policy and Standards. These procedures must be reviewed and approved by the DPS Director or designee. The Global eVA Security Officer will create, update, or deactivate any user account at the request of the Entity eVA Security Officer.
Officer, the Entity Administrative Head, or Designee where the request cannot be performed by the Entity or the DPS Account Executive.

The Global eVA Security Officer is empowered to take or authorize appropriate actions deemed necessary to protect COVA from fraud, misuse, or abuse. Actions taken to prevent or respond to incidents including: fraud, waste, or abuse shall be reported to the DPS Director or designee and the Director of DGS Information Systems and Services, who will review the action within ten (10) workdays. The DPS Director or designee shall approve the action or direct access to be re-established with or without conditions.

**Global eVA Technical Lead**

The Global eVA Technical Lead is empowered to take or authorize appropriate actions deemed necessary to protect COVA from security incidents. For occurrences of intrusion reported by service provider, the DGS Information Security Officer will also be notified.

**Service Provider Administrator (CGI)**

Overall security to protect eVA is the responsibility of CGI. Examples of their responsibilities include providing:

- Technical training materials to the Global eVA Security Officer.
- A technical security architecture that secures telecommunications, data and systems interoperability.
- Physical security for the service offering hardware, software, and data as well as personnel security.
- Threat detection, incident handling, and monitoring and controlling of systems activities as required, detecting security violations and maintaining audit trails of security administration activities and/or system administration access to the eVA service offering.
- For establishment of an incident response team charged with responding to misuse, abuse, or unauthorized access of eVA. The Global eVA Security Officer shall be a member of this response team and shall follow all directives of the designated response team leader.
- For monitoring of the eVA solution, responding to incidents, and informing the Global eVA Security Officer of any intrusions or attacks that penetrate eVA firewalls or violations of eVA or CGI- security standards.
- For business continuity of eVA.
INTRODUCTION

eVA is the Commonwealth’s web-based purchasing solution provided by CGI Inc. and administered by the Department of General Services / Division of Purchases and Supply (DGS/DPS). eVA streamlines and automates government purchasing activities. The ability to provide a robust, fully hosted electronic procurement solution such as eVA that is highly dependent on the security of its infrastructure, as well as the security of each and every transaction that takes place in the eVA solution.

As a service offering, CGI maintains ultimate control and responsibility for providing a consistent service offering that is secure and does not compromise data integrity. Although CGI is responsible for security of the system, each entity is responsible for ensuring that its connection to the eVA secure portal is protected.

This document sets forth the minimum requirements used for securing connections to and authorizing the use of eVA by entity personnel in accordance with all applicable statutes, regulations, policies and standards.

Any Entity Administrative Head or designee requesting an exception in whole or in part to this standard should send a request to the eVA Global Security Officer or designee stating the (refer to Appendix A):

1. Exception requested,
2. Reason why such an exception is necessary, and
3. Compensating controls.

Requests for exceptions may be submitted by FAX, E-mail, or conventional paper (hard copy) correspondence to the address, FAX number, or email address listed in Appendix A.

The eVA Global Security Officer shall route requests to the DGS/DPS Director or Designee who is authorized to grant exceptions. Copies of approved exception request will be provided by the DGS/DPS Director or Designee to the DPS Account Executive.

From time to time the eVA Global Security Officer will issue directives pertaining to eVA Security Standards.
1. ENTITY eVA SECURITY OFFICER DESIGNATION AND ACCESS LEVEL

1.1. Entity Administrative Head to Appoint Primary and Backup Security Officers

The Entity Administrative Head shall designate, in writing, a primary and may designate a backup Entity eVA Security Officer for the organization by submitting the Entity eVA Security Officer Designation form to the eVA Global Security Officer (refer to Appendix C). The eVA Global Security Officer will work with the Entity Assigned DPS Account Executive to review the designation form.

The Entity eVA Security Officers shall receive additional training before being granted Security administration access to the eVA Secure Portal. The Entity Assigned DPS Account Executive will coordinate this training with the eVA Global Security Officer.

1.1.1. Background Check for Entity eVA Security Officer

At the discretion of the Entity Administrative Head or designee, completion of a criminal background check may be required prior to designation of the Entity eVA Security Officer(s). It is recommended for advanced level security delegation.

1.2. Basic Level Security Delegation

All Entity eVA Security Officers will be granted initial privileges for eVA Security at the Basic level. The following criteria shall be used to select individuals to fill the position of Entity eVA Security Officer:

- Must be an employee of an entity participating in the eVA program.
- No known prior disciplinary actions for security related issues.
- Capable of fulfilling the responsibilities as defined in the eVA Security Standards
- Has a workflow that requires an approver at zero dollars.
- Has not been assigned the “eVA-No Supervisor, “eVA-RefireWorkflow_None”, “eVA_NoReApprovalwithApprovalEdit”, and/or the “eVA-ChangeManager” roles within eVA.
- Because most Entity Procurement and Fiscal Officers and the Entity Administrative Head will have some level of final expenditure or procurement approval authority they should not be designated as the Entity eVA Security Officer.

1.3. Advanced Level Security Delegation
All Entity eVA Security Officers will be granted initial privileges for eVA Security at the basic level. Advanced Level Security privileges will be granted when the following criteria are met:

- All basic level criteria are met
- No significant Entity procurement weaknesses or eVA system misuse noted in the most recent report available by APA, DPS, or comparable audit organization.
- Completed eVA Security training and has completed the associated test.
- Approved Entity eVA Security Plan for each organization for which the Entity eVA Security Officer is requesting User Administration.

1.3.1. Entity eVA Security Plan Required

For each organization that is required or elects to take on advanced level security, the Entity eVA Security Officer will develop and submit for approval an Entity eVA Security Plan. A sample plan is available from the eVA Global Security Officer for guidance in developing the Entity’s unique plan. The security plan will contain, at a minimum, the following:

- Names of the primary and backup security officers
- Statement of actions to be taken to manage user accounts
- Statement describing the security awareness program
- Statements governing auditing of user accounts
- Statement that you will not grant prohibited applications to users

1.3.2. Entity Advanced Level Security Administration Required

Entity eVA Security Officers for entities with more than 100 eVA users shall be required to have Advanced Level Security unless the Entity fails to meet the criteria.

Entities shall assume these responsibilities within six months of enrolling more than 100 active eVA users.

1.4. Exception to Security Delegation

In instances where an Entity has fewer than 20 active users, the Entity Administrative Head or designee may submit an Entity Request for Exception (Appendix A) requesting that the DGS/DPS serve as the eVA Entity Security Officer. Once approved the Entity Administrative Head or designee shall designate, in writing, by submitting the Entity eVA Security Officer Designation form to the eVA Global Security Officer (refer to Appendix C).
Individuals from Local Public Entities participating in eVA utilizing eVAlite, are not required to designate an Entity eVA Security Officer. The Global eVA Security Officer or designee is responsible for ensuring security for eVA Users in eVAlite.

Individuals from Private Colleges participating in eVA are not required to designate an Entity eVA Security Officer. The Global eVA Security Officer or designee is responsible for ensuring security for eVA Private College Users in eVA.

2. AUTHENTICATION AND AUTHORIZATION – SYSTEM ACCESS

2.1. Acceptable Use of eVA

The use of eVA is restricted to official purposes. Acceptable use of eVA is stipulated in Appendix B of this standard.

2.2. Unacceptable Use of eVA and Exceptions

The eVA Secure Portal shall not be used to promote outside business interests. Any use of the system for illegal, inappropriate, or unapproved business related purposes or in support of such activities is prohibited. eVA shall not be used for private consulting or personal gain. eVA shall not be used to support or engage in any conduct prohibited by Commonwealth of Virginia, other statutes applicable to the entity or entity policies. Users will not examine, or attempt to examine, another eVA user's or entity’s files or data without authorization.

Exceptions are allowed for personnel who must examine these files or data while performing their assigned duties during the auditing process, DPS reviews, Entity controller reviews, or other approved activities to monitor and manage business. Users will not post/send/display defamatory, harassing, pornographic, obscene, or sexually explicit materials. Activities of this type are specifically prohibited by statute.

2.3. Authorizing and Submitting an eVA User Profile Request.

The Entity Procurement Director or Entity eVA Lead will authorize access to any part of eVA. Authorization must be in the form of a signed paper eVA User Profile form submitted by mail or fax or an electronic request via email.

For agencies with Basic Level Security, the Entity Procurement Director or Entity eVA Lead will submit an eVA user Profile Form (Appendix E) or other electronic format (e.g. eVA Bulkload file, email request) to the DPS Account Executive with a copy to the Entity eVA Security Officer.

For agencies with Advance Level Security, Entity Procurement Director or Entity eVA Lead will submit an eVA user Profile Form (Appendix E) or
other electronic format (e.g. eVA Bulkload file, email request) to the Entity eVA Security Officer.

2.4. Processing Approved eVA User Profile Request

The privileges of all eVA users shall be restricted, based on roles (least privilege). Users shall be granted the minimum set of privileges required to perform their assigned duties.

For Entities with Basic Level Security, the assigned DPS Account Executive will create the user account and grant approved application access by using the on-line User Management Application or the Data Management Application through the batch Bulkload function. In the event that the assigned DPS Account Executive or their backup is unavailable the Entity eVA Security Officer should contact the Policy, Consulting, and Review Administrative Support at 804-371-8355. The administrative support will assign a DPS Account Executive to handle the Entity’s request; the DPS Account Executive will obtain assistance from the eVA Global Security Officer if required.

For Entities with Advance Level Security, the Entity eVA Security Officer will create the user account and grant approved application access by using the on-line User Management Application or the Data Management Application through the batch Bulkload function. As an exception process the Entity eVA Security Officer with Advance Level Security may utilize the assigned DPS Account Executive as described in the paragraph above for Entities with Basic Level Security.

Advanced Level Entity eVA Security Officer may not grant the following applications to any entity users; Administration, Catalog Administration, Contractor Management, Customer Care Reports, Data Management, Full Advantage and/or VSS Administration.

Advanced Level Entity eVA Security Officer may only grant the following Report roles to any entity users; R-BuyerLandingPage, R-StandardAccess, and R-StandardBuyer.

In instances where the responsible parties in the above two processes are unavailable and the need for access is time critical the request may be submitted to the eVA Global Security Officer. The eVA Global Security Officer will create the user account and grant approved application access, notify the requestor and copy the Entity eVA Security Officer and DPS Account Executive.

Requests can be submitted by using the paper form (Appendix E) or by using the User Request eForm.

Reference guidance provided by DGS/DPS.
2.5. Distribution of User-ID & Password and Acceptable Use of eVA and Completion of eVA Acceptable Use Acknowledgement

The created User-ID and temporary password will be sent under separate correspondence (electronic or paper) to the original requestor.

The original requestor shall provide the end user with their login ID, temporary password, and the eVA Acceptable Use Agreement for timely completion. The signed Acceptable Use Agreement (electronic or paper) shall be submitted to and maintained by the Entity eVA Security Officer.

Acceptable use of eVA is stipulated in Appendix B of this standard.

2.6. Password Requirements

Temporary passwords expire upon first use and require the user to establish their new password.

The minimum password length required by the system must be 8 characters. The system edits checks password history to ensure that passwords can not be reused for 24 logins.

Passwords shall contain at least three of the following four:
1. Special characters
2. Alphabetical characters
3. Numerical characters
4. Combination of upper and lower case letters

eVA users shall not utilize any password management utility (e.g. Internet browsers).

Passwords shall not be written down and left in a place where unauthorized persons might discover them.

Passwords shall not be shared or revealed to anyone else besides the owner. To do so exposes the owner to responsibility for actions that the other party takes with the password.

*Password minimum and maximum lifetime restrictions of 24 hours minimum and 90 days maximum.*”

2.7. Password Changes and Resets

Users may change their password at anytime through buyer portal preference functionality.
Users may reset their password utilizing the “Login help” located on the eVA home page next to the Buyer login.

In the event that a user is unable to reset their password using either of the above options they may submit an email to the Entity eVA Security Officer or Entity eVA Lead to request a password reset. The request must be sent from the same email address that is recorded on the eVA user account and should include the eVA User ID.

For agencies with Basic Level Security, the Entity eVA Security Officer or Entity eVA Lead will submit the request for password reset to the DPS Account Executive. The assigned DPS Account Executive will reset the password by using the on-line User Management Application or the Data Management Application through the batch Bulkload function. In the event that the assigned DPS Account Executive or their backup is unavailable the Entity eVA Security Officer should contact the Policy, Consulting, and Review Administrative Support at 804-371-8355. The administrative support will assign a DPS Account Executive to handle the Entity’s request; the DPS Account Executive will obtain assistance from the eVA Global Security Officer if required.

For Entities with Advance Level Security, the Entity eVA Security Officer will reset the password by using the on-line User Management Application or the Data Management Application through the batch Bulkload function. As an exception process the Entity eVA Security Officer with Advance Level Security may utilize the assigned DPS Account Executive as described in the paragraph above for Entities with Basic Level Security.

2.8. Deactivation of eVA Access

Access to eVA shall be deactivated when the requirement for access no longer exists. Since eVA is a web-based application accessible from anywhere, removing a user from the entity’s network is not sufficient. The user’s eVA user id must be deactivated.

In accordance with the Entity’s internal system access procedures the work supervisor shall notify the Entity eVA Security Officer or the Entity eVA Lead when an individual’s access should be deactivated.

The Entity eVA Security Officer may deactivate Access to eVA when the account has not been accessed for more than 90 days; in such cases the work supervisor or the Entity eVA Lead must approve the deactivation of the user.

Access will also be deactivated in case of separation of the employee, transfer, or a change of duties.
In cases involving personnel issues such as termination, or unacceptable use of eVA, those employees with eVA access shall be reported immediately to the Entity eVA Security Officer so action can be taken to deactivate access as needed.

Reference guidance provided by DGS/DPS.

For agencies with Basic Level Security, the Entity eVA Security Officer or Entity eVA Lead will submit the request for deactivation to the DPS Account Executive. An email request can be sent in lieu of a form. The assigned DPS Account Executive will deactivate by using the on-line User Management Application or the Data Management Application through the batch Bulkload function. In the event that the assigned DPS Account Executive or their backup is unavailable the Entity eVA Security Officer should contact the Policy, Consulting, and Review Administrative Support at 804-371-8355. The administrative support will assign a DPS Account Executive to handle the Entity’s request; the DPS Account Executive will obtain assistance from the eVA Global Security Officer if required.

For Entities with Advance Level Security, the Entity eVA Security Officer will deactivate by using the on-line User Management Application or the Data Management Application through the batch Bulkload function. As an exception process the Entity eVA Security Officer with Advance Level Security may utilize the assigned DPS Account Executive as described in the paragraph above for Entities with Basic Level Security.

2.9. Reactivation of eVA Access

Requests to reactivate eVA user access may be granted when meeting criteria stated below:

Return to Entity: Consideration must be given whether it is appropriate to reactivate the deactivated access or establish new access based on the role and function of the returning employee. Returning employees must complete a new eVA Acceptable Use Agreement.

Custodial/Steward access: This access shall require a written request with the name of the user who will assume responsibility for the account. If Custodian/Steward does not have a current eVA Acceptable Use Agreement, one must be completed prior to granting access. Privilege is granted to only process change orders, receiving, and completion of active Quick Quotes. It is prohibited to perform approval functions as Custodial/Steward of an account. The only exception granted is in the instance when processing a change order that is to a non-electronic vendor and the responsibility of PO print falls to the user account and the custodial/steward must approve the change to complete the order.

Custodial/Steward accounts standard reactivation is for 3 months. Remove PCard associated with the account prior to granting Custodial/Stewardship. If during the
quarterly review by the Entity eVA Security Officer (as described in Section 5) a
determination is made that the account is no longer needed, the custodial
assignment should be removed and the account deactivated.

Reference guidance provided by DGS/DPS.

For Entities with Basic Level Security, the assigned DPS Account Executive will
reactivate the account and grant approved application access by using the on-line
User Management Application or the Data Management Application through the
batch Bulkload function. In the event that the assigned DPS Account Executive or
their backup is unavailable the Entity eVA Security Officer should contact the
Policy, Consulting, and Review Administrative Support at 804-371-8355. The
administrative support will assign a DPS Account Executive to handle the Entity’s
request; the DPS Account Executive will obtain assistance from the eVA Global
Security Officer if required.

For Entities with Advance Level Security, the Entity eVA Security Officer will
reactivate the account and grant approved application access by using the on-line
User Management Application or the Data Management Application through the
batch Bulkload function. As an exception process the Entity eVA Security Officer
with Advance Level Security may utilize the assigned DPS Account Executive as
described in the paragraph above for Entities with Basic Level Security.

2.10. Changes in User Duties affecting eVA Access

Entity eVA Security Officer shall ensure that management promptly reports all
significant changes in end-user duties. These changes shall be reported as soon as
they are known including the effective date of the change.

3. SECURITY INCIDENT

3.1. Measures for Information Security Non-Compliance

In the event the Global eVA Security Officer becomes aware of a suspected non-
compliance incident it will be reported to the Entity eVA Security Officer and the
DGS/DPS Account Executive for resolution.

In the event the Entity eVA Security Officer becomes aware of a suspected non-
compliance incident, the following steps should be taken.

1) Notify the Entity eVA Lead who should, if appropriate, notify the Entity
Administrative Head and/or designee.
2) The Entity eVA Security Officer will work in conjunction with the Entity eVA Lead to develop and implement a corrective plan to remediate the situation in a manner which causes the least amount of disruption to entity

In addition to the above, any use of information resources for a fraudulent transaction falls under the Code of Virginia, §30-138.

4. SYSTEM INTEROPERABILITY SECURITY

4.1. Data Exchange

DGS/DPS and CGI electronically exchange data with external systems. When a regular exchange of data occurs between systems, the Entity eVA Security Officer shall coordinate with the Global eVA Technical Lead to ensure that a Memorandum of Understanding or other form of third-party agreement will be executed detailing the security policy that governs that connection. The agreement shall detail how the organizations will handle security in regards to authentication, authorized resource access, encryption requirements, and the data integrity validation process.

5. MONITORING, REVIEW AND CERTIFICATION

5.1. System Monitoring

The Global eVA Security Officer will coordinate the development of monitoring reports to facilitate compliance with these standards.

The Global eVA Security Officer shall coordinate the development of exception based reports to be used to identify inappropriate permissions or unauthorized eVA Entity Security activities which may be in violation of established policies or procedures.

The Global eVA Security Officer will monitor Entity eVA Security Officer compliance with these standards using reports and required submittal documents.

The Entity eVA Security Officer will use reports to monitor the system access and permissions and take appropriate actions when needed for their designated entities.

5.2. Quarterly System Access Review

The Entity eVA Security Officers shall review all of their designated entities’ system access granted in eVA on a quarterly basis at a minimum. The purpose of this review is to:

- Determine that changes in end-user duties reported by Management are appropriately reflected in current system access.
• Determine that eVA users that no longer require system access have been deactivated. This includes reviewing assigned custodial accounts.

• Confirm that a signed acceptable use policy (Appendix B.) is on file for all active eVA users. Electronic Agreements are acceptable.

• Confirm that all active eVA users have a valid email address, phone number, and ensure the user’s Expenditure Limit Approver and Supervisor are active eVA users.

5.3. Annual Certification of System Access

By November 1st of each year, all Entity eVA Security Officers must submit to the Global eVA Security Officer the eVA Annual System Access Certification (Appendix D.) certifying compliance. First submittal is due November 1, 2015.

Submission of the completed certification by email:

• Completed certification shall be attached to the email.
• The email must be sent from the Entity eVA Security Officers email account (this must match the email address on file).
• The email shall identify in the subject line the Entity name and Code.
• The email shall copy the Entity eVA Lead, Entity Administrative Head or designee and the assigned DPS Account Executive.
• Submission by email - eVASecurity@dgs.virginia.gov

Submission of the completed certification by mail or fax:

• Must be signed by the Entity eVA Security Officer and the Entity Administrative Head or designee.
• Copies should be sent to the eVA Global Security Officer, Entity eVA Lead, Entity Administrative Head or designee and the assigned DPS Account Executive.
• Submission by mail - ATTN: eVA Global Security Officer, Department of General Services, 1111 E. Broad Street, 6th floor Richmond, VA 23219.
• Submission by fax - ATTN: eVA Global Security Officer, Department of General Services, (804) 786-5712.

5.4. Records

Entity eVA Security Officer shall maintain all records (hardcopy or electronic) necessary to demonstrate compliance with the eVA Policies and Standards.
- eVA acceptable Use Acknowledgement (APPENDIX B) for all active eVA Users
- Quarterly Review: A record of the completed review shall be maintained for auditing purposes by the Entity eVA Security Officer.
- Annual System Access Certification: A record of the completed certification shall be maintained for auditing purposes by the Entity eVA Security Officer.
- All other documentation executed in compliance with the eVA Policies and Standards.

The Entity eVA Security Officer shall maintain records in accordance with the State Library Records Retention Policy.
APPENDIX A REQUEST FOR EXCEPTIONS

Entity Request for Exception
eVA Electronic Procurement System
Security Standards

COVA ENTITY NAME: ____________________________________ Agency Code: ________

Date:______________________

Exception Requested:
________________________________________________________________________________
________________________________________________________________________________

Reason for Request:
________________________________________________________________________________
________________________________________________________________________________

Compensating Controls:
________________________________________________________________________________
________________________________________________________________________________

Entity Administrative Head Signature: ____________________________________________

Print Name _________________________________________________

Contact Person _____________________ Telephone Number ______________________

Requests for exceptions may be submitted by mail or fax.
Division of Purchases and Supply
Attn: eVA Global Security Officer
1111 East Broad Street, 6th floor
Richmond, VA 23219
FAX Number: (804) 786-5712

Department of General Services / Division of Purchases and Supply

☐ Approved    ☐ - Effective Until_______________  (date)

☐ Disapproved

☐ More information needed (specify and return to agency)    ☐

Signature ______________________________________  Date _____________________

DGS/DPS Director or Designee
APPENDIX B eVA ACCEPTABLE USE ACKNOWLEDGEMENT

eVA Acceptable Use Acknowledgement

Revised
July 1, 2015
Statement of User Responsibility

A. To be an authorized user of eVA, you must have job responsibilities consistent with the purpose of eVA, have obtained approval for your eVA user account from your COVA Entity’s eVA Security Officer, and be in good standing as a permanent, temporary, or contract employee of a COVA Entity.

B. As an authorized COVA Entity eVA user, you are responsible for the security and use of your eVA user account. You accept full responsibility for your account and for all activity performed on eVA under your eVA user account.

C. As an authorized COVA Entity eVA user, you are responsible for keeping user information current and accurate. This information includes email address, phone number, supervisor, delivery location and purchase card information.

D. It is prohibited for any eVA user other than the assigned eVA user account owner to use said eVA user account. Each authorized user is responsible for preventing unauthorized use of their eVA user account as well as refraining from using someone else’s eVA user account.

E. As an authorized COVA Entity eVA user, you are responsible for protecting personally identifiable information (PII) from public access, including among others Social Security numbers, Federal Tax ID numbers, Patient Information, and Personal Banking Information, in accordance with Federal and State law and procurement regulations. This information is to be removed from procurement documents or procurement files when made available to the public. It is only to be included on eVA purchase orders if including such information is required by law. If you must include such information, you must ensure that the comment field and separate file attachment capability at the line level and header level are used and the box is checked indicating the comment or attachment is proprietary information.

Password Requirement

The minimum password length required by the system must be 8 characters. The system checks password history to ensure that passwords can not be reused for 24 logins.

Passwords shall contain at least three of the following four;
1. Special characters
2. Alphabetical characters
3. Numerical characters
4. Combination of upper and lower case letters

Password minimum and maximum lifetime restrictions of 24 hours minimum and 90 days maximum.

eVA users shall not utilize the password management functionality contained in Internet browsers. If technically feasible, the password management function shall be disabled.

Passwords shall not be written down and left in a place where unauthorized persons might discover them.

Passwords shall not be shared or revealed to anyone else besides the owner. To do so exposes the owner to responsibility for actions that the other party takes with the password. Users are responsible for all activity performed with their personal user-IDs. Personal user-IDs shall not be utilized by anyone but the individuals to whom they have been issued. Users shall not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users.
When the User has a blocked eVA account or has forgotten their password they shall use the “Login help” located on the eVA home page next to the Buyer login. Users should contact the Entity eVA Security Officer or Entity eVA Lead if they are unable to reset their password.

**Definition of Appropriate Use**

Valid uses of eVA include, but are not limited to, using eVA for the intended and stated purposes of:

- Bid development
- Bid and contract awards
- Purchase approvals
- Placing orders
- Placing requisitions
- Recording of receipts
- Training
- Administrative purposes

To appropriately use eVA, each eVA user must:

- Adhere to the copyright protection of licensed software and documentation.
- Secure your user account and password at all times.
- Log out of eVA or secure your computer if you are away from the active session.
- Follow all COVA and eVA policies, as well as all local, state, and federal laws and policies.

**Definition of Inappropriate Use**

Inappropriate uses of eVA include, but are not limited to:

- Using any other individual’s eVA account or password.
- Managing your user account or access in a way as to make your password and/or eVA session available for use by others.
- Unauthorized copying, sending, or receiving of copyrighted or trade/service marked materials

It is a violation of Commonwealth of Virginia policy to use eVA for promoting outside business interests. eVA shall not be used for private consulting or personal gain. eVA may not be used to support or engage in any conduct prohibited by Commonwealth of Virginia or local COVA Entity statutes or policies, including the eVA Security Policy.

It is a violation of this policy to examine, or attempt to examine, another eVA user’s or COVA Entity’s files or data without authorization. Noted exceptions are personnel who must examine these files or data while performing their assigned duties during the auditing process, DPS reviews, COVA Entity controller reviews, technical reviews to identify or correct eVA problems, or other approved activities to monitor and manage COVA business.

It is a violation of eVA policy to post/send/display defamatory, harassing, pornographic, obscene, or sexually explicit materials. These violations are in addition to items prohibited by any section of the Statutes of the Commonwealth of Virginia, or other federal, state, or local law.

**Reporting of Information Security Violations & Problems**

All eVA users have a duty to report all known information security vulnerabilities -- in addition to all suspected or known policy violations -- in an expeditious and confidential manner to their assigned Entity eVA Security Officer or to the eVA Global Security Officer so that prompt remedial action may be taken.
Possible Sanctions for Misuse

The eVA Global Security Officer may monitor, record and store information about the use of eVA. If such monitoring, recording, and storage reveal possible evidence of inappropriate, unethical, or illegal activity within eVA, the eVA Global Security Officer will contact the COVA Entity’s eVA Security Officer regarding the alleged violations of this policy.

It is not appropriate to use eVA in a way that is detrimental to the normal operation of eVA. Penalties for misuse of eVA may include, but are not limited to, suspension of the use of eVA and referral to the appropriate local law enforcement agency for possible prosecution.

Upon detection of a potential violation, the eVA Global Security Officer will disable the eVA user account. The eVA user account will remain inactive until:

1) The eVA Global Security Officer has determined no violations exist or corrective action has been taken by the COVA Entity eVA Security Officer.

2) The COVA Entity’s eVA Security Officer has notified the eVA Global Security Officer of the correction(s).

3) The remedial actions have been validated by the eVA Global Security Officer.

If corrective action is not taken at the COVA Entity level, the eVA Global Security Officer may:

1) Recommend to the DPS Director that an eVA user be permanently suspended from use of the system.

2) Report to the user COVA Entity’s Director of Purchasing with a recommendation for disciplinary action.

ACKNOWLEDGEMENT

My signature acknowledges that I have read, understood and will adhere to the eVA Acceptable Use Policy. I also acknowledge that I will report violations immediately to the COVA Entity eVA Security Officer, as well as the eVA Global Security Officer at eVASecurity@dgs.virginia.gov.

Signature:

Printed Name:

Agency Name and Number:

Title:

Date:

The eVA Entity’s Security Officer shall maintain a copy of this form (hardcopy or electronic).
APPENDIX C COVA ENTITY eVA DESIGNATION

COVA Entity eVA
Designation Form

COVA ENTITY NAME: ____________________________Agency Code: __________

Date: __________________

- As the Entity Administrative Head for the COVA Entity listed above, I am designating the individual listed below-as the:
  - [ ] Primary Entity eVA Security Officer
  - [ ] Backup Entity eVA Security Officer
- As the Entity Procurement Director for the COVA Entity listed above, I am designating the individual listed below-as the:
  - [ ] Primary Entity eVA Lead
  - [ ] Backup Entity eVA Lead
- The individual designated is: with no known disciplinary actions for security issues.
  - [ ] An employee of my Entity
  - [ ] Is not an employee of my Entity but is authorized to serve as the Entity eVA Security Officer for my Entity.
- I understand that it is recommended that the designated individual have passed a criminal background check.

_________________________ ______________________________
Signature Date

Printed Name & Title

As the Entity eVA Security Officer/Entity eVA Lead, I acknowledge that it is my responsibility to comply with the eVA Electronic Procurement System Security Policies and Standards.

_________________________ ______________________________
Signature Date

Printed Name & Title

________________ (___) __________ ________
eMail Phone Number eVA User ID

eVA Security designation submit electronically or by mail or fax: eVA.Security@dgs.virginia.gov/
Department of General Services; ATTN: eVA Global Security Officer, 1111 E. Broad St, 6th floor Richmond, VA 23219/ Fax: (804) 786-5712

<table>
<thead>
<tr>
<th>Basic Level Security Delegation Granted</th>
<th>Advance Level Security Delegation Granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date eVA Global Security Officer</td>
<td>Date eVA Global Security Officer</td>
</tr>
</tbody>
</table>
APPENDIX D  eVA ANNUAL USER CERTIFIED REPORT

eVA ANNUAL
SYSTEM ACCESS CERTIFICATION

COVA ENTITY NAME: ______________________________Agency Code: ________
Date: __________________________

As the Entity Administrative Head or designee for the COVA Entity listed above, I hereby certify:
- Quarterly reviews have been completed and records are available for review
- Active eVA users for my Entity are valid and in compliance with all the requirements of the eVA Electronic Procurement System Security Policies and Standards.

eVA Annual System Access Certification can be submit electronically or by mail or fax: eVASecurity@dgs.virginia.gov/ Department of General Services, ATTN: eVA Global Security Officer, 1111 E. Broad St., 6th floor Richmond, VA 23219. / Fax: (804) 786-5712

Signatures:

Entity Administrative Head or designee          Date

Printed Name & Title

Entity eVA Security Officer          Date

Printed Name & Title
### APPENDIX E REQUEST FOR eVA USER PROFILE

Name of individual submitting this form ________________________________

Phone number __________________________ Email Address _______________________

<table>
<thead>
<tr>
<th>Agency Number and Abbreviation</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>Required</td>
</tr>
<tr>
<td>Last Name</td>
<td>Required</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>Required</td>
</tr>
</tbody>
</table>

#### eVA Applications required

*Only DGS may grant these applications*

- [ ] eMall/Shop Now (Ariba)
- [ ] Logi Reporting
- [ ] Quick Quote
- [ ] VBO Buyer
- [ ] Catalog Administration*
- [ ] Data Management*
- [ ] eProcurement/AdvancedVBO (Full ADVANTAGE)*
- [ ] User Management (Administration)*
- [ ] VSS Administration*

<table>
<thead>
<tr>
<th>eMall/Shop Now (Ariba)</th>
<th>Complete needed fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buysense Org Name</td>
<td>Required</td>
</tr>
<tr>
<td>Catalog controller</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Delegated Purchase Authority Amt** *(Not normally utilized - requires additional setup in Buysense Org approvals)*

Optional

$ amount

- Phone Number
  - Required - format xxx-xxx-xxxx
- Deliver to name
  - Required - Person or location
- Employee Number
  - Optional
  - May be required for some Users
- Expenditure Limit Amt
  - Optional
  - $ amount
- Expenditure Limit Type
  - Required if Exp Limit Amt is indicated
  - Role or User
- Expenditure Limit Approver
  - Required if Exp Limit Amt is indicated
  - Name and eVA User ID
  - or Agency Approval Role
<table>
<thead>
<tr>
<th>Standard Roles needed by User:</th>
<th>Required</th>
<th>eVA-Rpt-Hier, Axxx-AgencyQueryAll, and eVA-CreateRequisition (if user is to create requisitions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Roles needed by User:</td>
<td>Optional</td>
<td>Any approval roles and/or special roles (i.e. agency security)</td>
</tr>
<tr>
<td>Ship to Address – Ship to Address Code</td>
<td>Required - eVA Address ID</td>
<td></td>
</tr>
<tr>
<td>eVA Supervisor User ID</td>
<td>Required - Name and eVA User ID</td>
<td></td>
</tr>
</tbody>
</table>

**Report and Resource Center (Logi)**

<table>
<thead>
<tr>
<th>Entity Access Value/ Agency Number</th>
<th>Required</th>
<th>XXXX,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Threshold Limit</td>
<td>Optional</td>
<td>System default is 5k.</td>
</tr>
<tr>
<td>Advanced reporting needs (i.e., agency management, technical, security, audit)</td>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>

**Quick Quote**

<table>
<thead>
<tr>
<th>Additional Buysense Orgs QQ this user should be able to view and/or approve</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does this user approve Quick Quote requests?</td>
<td>Optional</td>
</tr>
<tr>
<td>Does this user require approvals?</td>
<td>Optional</td>
</tr>
<tr>
<td>Reverse Auction Access</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**VBO Buyer**

<table>
<thead>
<tr>
<th>VBO Home Unit</th>
<th>Required</th>
<th>VBO</th>
</tr>
</thead>
<tbody>
<tr>
<td>VBO Fax Number</td>
<td>Optional - Format XXX-XXX-XXXX</td>
<td></td>
</tr>
</tbody>
</table>

**Additional Applications – ONLY COMPLETED BY DGS**

| Data Management - ONLY COMPLETED BY DGS - may not be done by Entity Security Officer | Yes or No |
| User Management - ONLY COMPLETED BY DGS - may not be done by Entity Security Officer | Yes or No |
| eProcurement/Advanced VBO/ Contract Management - ONLY COMPLETED BY DGS - may not be done by Entity Security Officer | Yes or No |
| VSS Admin Setup ONLY COMPLETED BY DGS - may not be done by Entity Security Officer | Yes or No |

**Additional eVA Applications required - Additional forms are required to be completed**

<table>
<thead>
<tr>
<th>Check all that is required</th>
<th>ACP</th>
</tr>
</thead>
<tbody>
<tr>
<td>eVA Billing Dashboard</td>
<td></td>
</tr>
<tr>
<td>Future Procurements</td>
<td></td>
</tr>
</tbody>
</table>

**Authorized signature required if mailed or faxed**

| Signature | |
**APPENDIX F REQUEST eVA USER DEACTIVATION**

Name of individual submitting this form ________________________________

Phone number _____________________ Email Address ______________________

<table>
<thead>
<tr>
<th>Field</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency Number and Abbreviation</td>
<td>Required</td>
</tr>
<tr>
<td>First Name</td>
<td>Required</td>
</tr>
<tr>
<td>Last Name</td>
<td>Required</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>Required</td>
</tr>
<tr>
<td>PCARD - Does the user have a PCard that needs to be removed from their account?</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Custodial Care - Does this user account need to be assigned to someone to complete Receiving or change orders?</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Custodial Care may not occur until account has been deactivated for 24 hours</td>
<td>Yes or No</td>
</tr>
<tr>
<td>List below the first name / last name / email of the individual being granted custodial care of the account.</td>
<td>Required</td>
</tr>
<tr>
<td>Is this user an Expenditure Limit Approver for other eVA users?</td>
<td>Yes or No</td>
</tr>
<tr>
<td>If yes - Must submit request to update users that are impacted and change the Expenditure Limit Approver to an active eVA account</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Is this user a Supervisor for other eVA users?</td>
<td>Yes or No</td>
</tr>
<tr>
<td>If yes - Must submit request to update users that are impacted and change the Supervisor to an active eVA account</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Does this user have any Approval Roles assigned?</td>
<td>Yes or No</td>
</tr>
<tr>
<td>If yes - Must submit request to update user(s) that should be assigned the Approval Roles</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Additional eVA Applications that may require deactivation.</td>
<td>Check all that is required</td>
</tr>
<tr>
<td>If yes - Additional forms are required to be completed</td>
<td>ACP</td>
</tr>
<tr>
<td>Authorized signature required if mailed or faxed</td>
<td>Signature</td>
</tr>
</tbody>
</table>