

# COMMONWEALTH OF VIRGINIA



## *eVA* Electronic Procurement System Security Policy

**Department of General Services  
Division of Purchases and Supply**

A handwritten signature in black ink, appearing to read "Ron Bell", written over a horizontal line.

**Ron Bell, Director, DPS  
May 1, 2013**

## **Table of Contents**

<b>PREFACE .....</b>	<b>3</b>
<b>SCOPE.....</b>	<b>3</b>
<b>PURPOSE .....</b>	<b>3</b>
<b>DEFINITIONS.....</b>	<b>3</b>
<b>REGULATORY REFERENCES.....</b>	<b>5</b>
<b>INTERNATIONAL STANDARDS .....</b>	<b>5</b>
<b>GENERAL RESPONSIBILITIES.....</b>	<b>5</b>
<b>STATEMENT OF POLICY FOR <i>EVA</i> PROCUREMENT SYSTEMS SECURITY.....</b>	<b>8</b>
<b>COMPLIANCE .....</b>	<b>8</b>
<b>RESPONSIBLE STAFF DIRECTOR.....</b>	<b>9</b>
<b>CONTACT PERSON FOR INTERPRETATION .....</b>	<b>9</b>
<b>EXCEPTIONS.....</b>	<b>9</b>

## **PREFACE**

### **Publication Designation**

Electronic Procurement Security

### **Subject**

*eVA* Security Policy

### **Effective Date**

05/01/2013

### **Compliance Date**

11/01/2013

### **Supersedes**

*eVA* Electronic Procurement System Security Policy dated June 26, 2007

### **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*.

## **PURPOSE**

The purpose of this policy is to set expectations for authorizing the use of *eVA* by entity personnel, including, but not limited to, managers, administrators, requestors, 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**

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. 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 as buyers and vendors).

**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 § 2.2-1111  
(DGS/DPS Authority and  
Responsibility)**

**INTERNATIONAL STANDARDS**

**ISO 15408, Common Criteria for  
Information Technology Security  
Evaluation, 1999**

**ISO/ECI 17799:2005, International  
Policy, Information technology – code  
of practice for information security  
management.**

**DGS Information Technology  
Security Policy – IS2  
ITRM SEC519-00**

## **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”.

### **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”.

### **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, 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-AMS security standards.
- For business continuity of *eVA*.

## **STATEMENT OF POLICY FOR *eVA* PROCURMENTS SYSTEM SECURITY**

*eVA* is an innovative, web-based, purchasing service solution provided by CGI and administered by the Department of General Services (DGS). *eVA* streamlines and automates government purchasing activities. *eVA* makes purchasing easier and faster for both vendors and employees with purchasing responsibilities. *eVA* users are able to shop from catalogs and statewide contracts, notify vendors of business opportunities, and provide one-stop vendor registration.

The ability to provide a robust, fully hosted electronic procurement solution such as *eVA* is highly dependent on the security of its infrastructure, as well as the security of each and every transaction that takes place on the *eVA* solution. As a service offering, CGI maintains ultimate control and responsibility for providing a consistent service offering that does not compromise data integrity. In execution of this responsibility, CGI has the system access and capability to manage *eVA* production and *eVA* users without detection by the Global *eVA* Security Officer. This is a necessary and acceptable risk. The contractual agreement between COVA and CGI requires notification and acceptance by COVA of any modification or change to the *eVA* production system and/or *eVA* user accounts made by the CGI System Administrator or other CGI employees.

It is the policy of the Commonwealth of Virginia that the e-procurement solution be used only for conducting legitimate and authorized *eVA* business transactions within the approved authority level of the user and in the manner in which it was intended. Although CGI maintains ultimate responsibility for the security of *eVA*, the function of this policy is to protect *eVA* assets from creditable threats, whether internal or external, deliberate or accidental, natural or man made. All entities that are authorized to use *eVA* shall use all reasonable security control measures to ensure that:

- a. e-procurement information will be protected against unauthorized access.
- b. Confidentiality, integrity, and availability of e-procurement information shall be maintained.
- c. Regulatory and legislative requirements will be met.

## **COMPLIANCE**

Compliance with this policy is mandatory. In order to determine compliance, a set of standards are maintained and published by the Virginia Department of General Services, Division of Purchases and Supply (DPS).

A set of standards sets forth the mandatory requirements for the *eVA* Security program. A standard must be followed in order to comply with this policy. A standards statement will always use a verb that has the strong connotation of urgency, usually a word like “shall”, “will”, or “must”. When read, the reader is left with a clear sense of what must be done and there is usually no ambiguity as to the meaning or intent. There is no

deviation allowed unless a specific exception to policy is received from the DGS/DPS Director. All *eVA* Security Standards will be clearly identified as mandatory requirements.

A set of guidelines generally informs the reader that these are things that can be done to meet a given standard. It usually implies that there are options. Guidelines generally identify industry best practices, and procedures. As long as an acceptable option is selected and implemented, the standard is usually met and compliance is affirmed. A guideline will usually use, but not always, a verb like “should”, “can”, or “might”. Before deviating from the guidelines, check with the *eVA* Global Security Officer as to whether following some other procedure other than the options suggested in the guidelines would fulfill any obligations when meeting a standard. All *eVA* Security Guidelines will be clearly identified. Although various options may be provided, the choice of an applicable option is mandatory.

## **RESPONSIBLE STAFF DIRECTOR**

DGS Division of Purchases and Supply Director

## **CONTACT PERSON FOR INTERPRETATION**

Personnel desiring clarifications, explanations or other interpretations should contact the *eVA* Global Security Officer at: [eVASEcurity@dgs.virginia.gov](mailto:eVASEcurity@dgs.virginia.gov)

## **EXCEPTIONS**

Requests for exceptions to this policy shall be submitted in writing by the appropriate Entity *eVA* Security Officer to the *eVA* Global Security Officer for review and subsequent routing to the DGS/DPS Director who is authorized to grant exceptions. Requests for exceptions may be submitted by FAX, E-mail, or conventional paper (hard copy) correspondence.

**Department of General Services**  
**ATTN: *eVA* Global Security Officer**  
**1111 E. Broad Street, 6<sup>th</sup> floor**  
**Richmond, VA 23219**

**FAX Number: (804) 786-5712**

**E-Mail Address: [eVASEcurity@dgs.virginia.gov](mailto:eVASEcurity@dgs.virginia.gov)**