Purpose

Outlines policies and procedures of University personnel when using the Commonwealth of Virginia’s eVA electronic purchasing system.

Definitions

a. eVA users – Individuals within the University community who create requisitions for the purchase of goods and services.

b. Department Managers – Individual assigned by the Department Chair to oversee the eVA program.

c. Security Officer – Individual designated in writing to administer security of eVA for the University.

d. Global eVA Security Officer – Individual designated at the Commonwealth level to administer overall security of eVA. The Global eVA Security Officer is responsible for facilitating and monitoring COVA Entity compliance with the eVA Security Manual, as well as with applicable federal and state statues and policies.

e. DPS Account Executive – Division of Purchases and Supply staff member assigned to the VSU to assist in effectively using and configuring eVA.

Authority, Responsibility, and Duties

Department Manager shall:

1. Determine which employees shall be granted eVA access and monetary limits.
2. Designate a “back-up” individual for delegation purposes when unavailable.
3. Certify that the items called for in the requisition are for official use of the University and that funds are available, or will be made available, to promptly remit payment to the sender upon delivery and receipt of goods or services.

Security Officer shall:

1. Take the necessary steps to activate, deactivate, or reactivate user accounts based on the procedures outlined below.
2. Maintain a list of active accounts.
3. Ensure users have signed the eVA Access Request Form which contains the Acceptable Use Acknowledgement clause and maintain these original documents in a secure area.
4. In accordance with Section 4.2.2.2 of the eVA “Security Manual” dated February 1, 2004, conduct and document quarterly reviews of users accounts to ensure terminated employees or eVA users with changed job responsibilities do not have eVA access, complete the eVA Quarterly Validation Report and maintain original documents in a secure area.

5. Conduct and document an annual audit of users accounts forward to DGS/DP&S as required.

6. Ensure the University is in compliance with the eVA Security Manual.

7. Work with DGS/DP&S to obtain advanced level administration rights by maintaining the basic level criteria, have a Criminal Background Check performed, attend eVA Security Administration Training, submit the VSU eVA Security Plan, and work with the Global eVA Security Officer as needed.

**Human Resource Office shall:**

1. Notify the Security Officer when an employee has given their notice to leave the University.

**Purchasing Director shall:**

1. Ensure eVA users understand and adhere to appropriate policies and procedures and authorized use of eVA.

2. Provide the user all purchasing and eVA training once the user has their eVA logon ID.

3. Work with the Security Officer to ensure workflow roles and data access permissions are appropriate.

The University President or designee may perform any of these functions in the absence of the designate individuals.

**Policy Statements**

**Workflow Criteria:**

1. VSU uses the Commonwealth’s eVA electronic procurement system for the purchase of goods and services.

2. Except in very limited circumstances, all transactions must be processed through eVA including purchases made against your Small Purchase Charge Card.
3. All users, including supervisors (called in eVA “Approvers”), are assigned an user name and password; passwords (8-16 characters in length) must be changed every thirty (30) days.

4. At the present time, eVA does not interface to FRS. Prior to submitting eVA requisitions, end-users must confirm that funds are available to pay the transactions. Purchasing will encumber all requisitions except for orders charged against the Small Purchase Charge Card, which will not be encumbered.

5. The departmental approval process is pre-loaded into the system; it is not necessary to have the Approver to sign the request. Approvers will be contacted by e-mail notifying them that a request is pending. Clicking the “approve” button serves as the signature and a permanent record is built into the system.

6. Workflows can be customized on a department-by-department basis. It is recommended that each department will have one approver authorizing all requests over $1,000. (if the approver prefers, this can be reduced to zero; i.e., the approver will see every requisition).

7. Purchasing will approve all requests over $1,000; in addition, the Vice President for Administration and Finance must approve all requests over $50,000.

8. Certain commodities, including computer hardware/software, telecommunication equipment and services, and facilities management work orders, will require special “commodity approval” before the requisition will be processed.

9. Users can check on the status of their request at anytime by clicking on the “status” button within the SHOP NOW module.

10. Vendors are required to register in eVA by paying an annual subscription fee; they also pay a 1% transaction fee (capped at $500) for each order (the vendor is billed by a third party – users will not see the fee). Users are required to use eVA-registered vendors (there is a search mechanism within eVA for checking if a vendor is registered).

The Security Officer and/or Purchasing Director may request, from DGS/DP&S, new access, access change, or access termination of users in eVA. Once advanced security access is authorized by DGS/DP&S, the VSU Security Officer will complete all DGS/DP&S authorized functions on behalf of the University.

All request for new security access or changes to existing security access for eVA must be made on the Access Request Form, which includes the Appropriate Use Clause. Terminations may be made via the Access Request Form or by sending an email to the Security Officer.

**Activating a New Account**

1. The Department Manager will work with the Purchasing Director to determine the appropriate access required in eVA. The user will complete the eVA Access Request Form and sign the Appropriate Use Clause.
2. The Department Manager will review the form for accuracy and sign the form.

3. The Purchasing Director will review the form for accuracy, complete the appropriate areas and sign the form.

4. The VSU Security Officer will complete the form electronically and forward it to eVASecurity@dgs.state.va.us with any additional information required.

5. The Security Officer will receive via email, from DGS/DP&S, the user name and temporary password of the user. The Security Officer will notify the user via email their user-id and initial password.

6. The Security Officer will notify the Purchasing Director that the user has been activated in eVA and is ready for training.

7. The Security Officer will maintain the original VSU Access Request Form with the signed Acceptable Use Acknowledgement clause in a locked file.

**Changing an Account**

1. The Purchasing Director will work with the Security Officer to review the user’s current eVA access and determine if any current roles will need to be changed based on the users move to another position.

2. The user and Department Manager will complete the VSU eVA Access Request Form for access required in the new position. All signatures must be original and no copies or facsimiles will be accepted.

3. The Security Officer will complete the users new form electronically and forward it to eVASecurity@dgs.state.va.us and indicate it is a change in access due to a change in position.

4. DGS/DP&S will confirm that the change has been completed per the request.

5. The Security Officer will attach the new eVA Access Request Form to the users original Access Request Form which contains the original signed Acceptable Use Clause.

**Terminations**

1. The Human Resource Office will notify the Security Officer by e-mail when an employee has given their notice to leave the University and give the exact date of departure.

2. The Purchasing Director will work with the Security Officer to review the user’s current eVA access and determine if any current roles will need to be changed based on the users departure.

3. The VSU eVA Security Office will notify eVASecurity@dgs.state.va.us to deactivate the user’s account.
4. The Security Officer will attach all departure paperwork received to the user’s original VSU eVA Access Request Form.

**Reactivating an Account**

1. The Department Manager that has had an employee change or terminate will work with the Purchasing Director to determine if a deactivated account needs to be reactivated so that the individual who is assigned those duties may access orders and receipts as needed. The account may remain active for up to 9 months. No reactivation request will be approved if the user’s initial deactivation from eVA has exceeded 9 months.

2. The Purchasing Director will notify the Security Officer via email when an account needs to be reactivated to allow an individual who has assumed duties of the changed or terminated eVA user to access the deactivated account. The request must include the date of activation, the responsible users full name for the account, the responsible users email address and phone number, the group profile and the user id of the deactivated account. Only roles required to process a change order will be assigned to reactivated users accounts.

3. The Security Officer will email the DPS Account Executive to request the account be reactivated.

4. The Security Officer will notify the responsible user, Department Manager and Purchasing Director when the account has been reactivated.

**eVA Security Awareness**

**Passwords**

The user is responsible for any activities associated with their login and password. The following password guidelines are provided:

- Do not use simple, obvious or predictable passwords
- Do not use names or nicknames of people, pets, places, or personal information that can be easily found out, such as your address, birthday or hobbies
- EVA requires the password to be eight to sixteen characters in length. The password should include a combination of alphabetic and numeric characters. Common English words should be avoided.
- Create passwords that are easy to remember but hard to guess.

Protect your security codes and passwords

- Do not share your passwords with anyone (Anyone means your coworker, spouse, friends, etc.)
- Do not write down your passwords
- Do not use the automatic password storage feature on your computer
- eVA forces the user to change their password immediately after a password reset and every thirty days. eVA validates the new password to ensure it is not identical to the previous password.
- If you think your password has been compromised, change it immediately.

**Don’ts**
• Don't reveal a password over the phone to ANYONE
• Don't reveal a password in an email message
• Don't reveal a password to the boss
• Don't talk about a password in front of others
• Don't hint at the format of a password (e.g., "my family name")
• Don't reveal a password on questionnaires or security forms
• Don't share a password with family members
• Don't reveal a password to co-workers while on vacation

**Securing your computer**

All workstations must be secured when unattended or when unauthorized individuals are in an employee’s workspace and may have an unauthorized view of the users work data. This may be accomplished by hitting Ctrl, Alt, Delete and clicking “Lock Computer”.

Users will be formally reprimanded for all password and security violations and the written reprimand made a part of the employee’s file to be used in the yearly employee evaluation. Severe violations will be handled under the Commonwealth of Virginia human resource policies and procedures.

**Procurement card (SPCC)**

All purchasing cardholders will adhere to the current VSU Purchasing Charge Card Policy. Listed below are some general guidelines for credit card security.

• To protect yourself against loss or theft of credit, sign your credit card immediately so no one else can use it.
• Always protect your credit cards as if they were cash. Just like cash, credit card numbers can be stolen.
• Keep your account number to yourself. Give your credit card number or expiration date over the telephone only if you know you are dealing with a reputable company.
• Never put your account number on the outside of an envelope or on a postcard.
• Draw a line through blank spaces on charge slips above the total so the amount cannot be changed.
• Keep copies of sales slips and compare charges when your monthly statements arrive.
• Make a record of your credit card numbers, their expiration dates, and the telephone number for each credit card company in case of an emergency such as reporting lost cards.

• Carry only those credit cards you regularly need, especially when traveling.
• Never give out additional personal information when you use your card for purchases. Merchants cannot ask for a driver's license number or phone number as a condition for accepting your card. All that's required is your signature.
• Never use a credit card as personal identification. Your credit privileges and history are too precious to risk.
**Appropriate Use of eVA**

Valid uses of eVA include but are not limited to 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.
- Follow all Commonwealth of Virginia, Virginia State University, and eVA policies and procedures, as well as all local, state, and federal laws and policies.

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 to promote 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 VSU statutes or policies, including the eVA Security Manual.
- It is a violation of this policy to examine, or attempt to examine, another eVA user's or VSU'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, 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.

Possible Sanctions for Misuse

- The Global eVA 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 Global eVA Security Officer will contact the 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, referral to the
University President, and/or referral to the appropriate local law enforcement agency for possible prosecution.

- Upon detection of a potential violation, the Global eVA Security Officer will disable the eVA user account.

**Review & Audit Schedule**

1. **Regular Reviews**
   The Security Officer will work with the Purchasing Director to conduct required reviews and audits of user accounts. The Security Officer will maintain all audits on file in a secure environment. The annual review will be sent or emailed by the President or Designee with a copy sent or emailed to the Security Officer to maintain on file in a secure environment.

2. The Security Officer will review all VSU eVA accounts on a quarterly basis at a minimum. The purpose of this review is, but not limited to the following:

   - Determine whether accounts assigned to any eVA users that have a change of responsibilities are appropriately modified.
   - Determine whether accounts assigned to eVA users that have left Virginia State University have been locked out and in a timely manner.
   - Determine that every active user has a signed acceptable use policy on file.
   - Initiate a review of the eVA approval chain for each eVA user account to check if all accounts in the eVA approval chain are still active and appropriate.
   - Monitor that account terminations (lock-outs) are timely and followed procedures.
   - Identify and report to the global eVA Security Officer any self-identified violations of the policy and the actions Virginia State University plans to implement to prevent further violations.

3. By July 1st of each year, The University President or designee will submit to the Global eVA Security Officer a listing of all active eVA user accounts. The Security Officer shall run the “Agency Security User Setup Information” report or the “Bulk Load” report and will review the report for accuracy before providing the list to the University President or designee. This list will then be attached to the Annual User Accounts Report and forwarded to:

   Department of General Services
   Information Systems & Services
   ATTN: eVA Global Security Officer
   805 E. Broad St  6th floor
   Richmond, VA 23219 or submitted via email by the University President or designee using his/her email account to eVASecurity@dgs.state.va.us.

4. By November 1st each year, the University President or designee will submit to the Global eVA Security Officer an update of Virginia State University’s eVA Security Officer status.
Reference

VSU Policy 507, “Procurement of Goods and Services”.

Approved by: Eddie N. Moore, Jr., President
Date: September 29, 2006