APPENDIX B *eVA ACCEPTABLE USE ACKNOWLEDGEMENT*

eVA Acceptable Use Acknowledgement

Revised November 16, 2018

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 e*VA* 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.

F. As an authorized COVA Entity e*VA* 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 shall not be stored on the user's personal or work computer.

Password Requirement

The minimum password length required by the system must be 8 characters. The system checks password history to ensure that passwords cannot 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 a 90-day 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.

To learn more about the Information Security Standards, go here: http://vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandardSEC52501.pdf

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. Return this form to your Entity *eVA* Security Officer.

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 *eVA*Security@dgs.virginia.gov.

Signature: .....

Printed Name: .....

Agency Name and Number: Longwood University A214LWU

Title: .....

Date: .....

The *eVA* Entity's Security Officer shall maintain a copy of this form (hardcopy or electronic).