CEE Computing Policies and Procedures

1.0 Introduction

This document describes the computing policies and procedures of the Via Department of Civil and Environmental Engineering with regards to responsibilities of CEE faculty, research and administrative staff, and graduate students as well as the services provided by the CEE Computer Systems Administrators (CSA). The goal of the CSA is the development and maintenance of a safe, effective computing environment for the pursuit of the departmental mission.

2.0 Services and Responsibilities

All computer users are responsible for:

- Following the VT Acceptable Use Guidelines (Policy 7000: Acceptable Use and Administration of Computer and Communication Systems - http://www.policies.vt.edu/7000.pdf) as well as the CEE Computing Policies within this document. The important points of Policy 7000 are attached as Appendix A to this document.
- Maintaining computer security by, for example, using discretion in opening email attachments or clicking on embedded links in emails.
- Reading the VT Policy on Computer Privacy (Policy 7035: Privacy Policy for Employees' Electronic Communications – http://www.policies.vt.edu/7035.pdf). The important points of Policy 7035 are attached as Appendix B to this document.
- Ensuring that all software is updated regularly, including the operating system and MS Office products, which may not have an automatic update option.
- Ensuring that updating of antivirus software is enabled and functioning.
- Ensuring that all research data files are backed up on a regular interval, ideally including a personal secondary backup to the departmental free backup service.
- Scanning their computers for personally identifying information (PII) at least once per semester and removing or encrypting any sensitive data found.

Helpdesk

Requests for assistance made through the Helpdesk (helpdesk.ce.vt.edu) will receive priority. During a (local) computer outage, please call the Helpdesk phone at 1-7037. Requests made through the Helpdesk are considered official, time stamped, reviewed in the order in which they are received, prioritized, assigned to a technician, and resolved. Repair and maintenance of printers is not provided by the CSA, but attempts will be made to alleviate printing problems.

Services and responsibilities of the CSA include:

- Setting up and configuring new and recycled computers (See Section 7.0 for Computer Inventory Control Procedures).
- Configuring automatic critical updates for the operating system (OS) and antivirus software.
- Ensuring antivirus protective measures are installed and activated on each computer.
- Installing research and instructional software as needed.
- Providing backup services for educational and research files.
- Responding to Helpdesk requests.

- Providing training for faculty, research and administrative staff, and graduate students on best practices for safe and effective computer use.
- Sending alerts to the CEE Department related to CSA service changes and security concerns.
- Setting up and maintaining all departmental computer labs.
- Reading and abiding by the VT Policies for Information Technology and Computer Privacy (Appendix B).
- Ensure that domain requirements for passwords match those of the university.

To achieve the goal of safe, effective computing in the CEE Department, the only Microsoft operating system that will be installed is Microsoft Windows 7 or later. However, the CSA will also support computers using Apple OS X and the Redhat Linux operating systems.

3.0 User Categories and Computer Types

The following subsections describe responsibilities of the computer user or computer type according to categories, delineating particular issues that apply, and specific computer user responsibilities or the CSA services that are pertinent.

1. Administrative Staff – Accounts for full and part time administrative CEE staff will be configured as "standard" user accounts on their desktop computers unless their job requires an "administrator" account. Please refer to the previous section on user responsibilities. All software and updates are installed by the CSA.

2. Faculty/Research Staff - Desktop Computing – Two accounts for faculty will be configured, the first based on VT PID with a "standard" user account, and the second as a local login "administrator" user account on their desktops/laptops by default to be used to perform system updates, configurations and installations. Please refer to the previous section on user responsibilities.

3. Faculty/Research Staff - Managed Servers – (Note: a server is defined as a computer that is not necessarily in the CE domain, but is providing services other than individual academic or research productivity.) The CSA will initially setup Faculty Managed Servers in cooperation with the faculty/staff person assigned as the manager. However, the PI is directly responsible for maintaining operating system (OS) patches and application updates as released by vendors in a timely manner (1-3 days is considered timely). Planning for systems support and maintenance are the responsibility of the PI. The CSA should be notified in advance of the purchase and arrival of these systems in order to plan for initial setup time. The standard set up for Faculty/Research Staff Managed Servers does not include membership in the CE domain.

4. Program Area Labs - Computer Labs designed to support the research mission of the department are the responsibility of the CSA. No local computer administrative rights will be granted to faculty, staff, or students and software installation or maintenance requests are to be made through the departmental Helpdesk (helpdesk.cee.vt.edu).

5. Research Computing – CEE Department-owned computers assigned to graduate students for research use are maintained by the CSA by default. Software installation requests are to be made through the Helpdesk (helpdesk.cee.vt.edu). Accounts for graduate students on computers that are purchased by CEE faculty will be configured as "standard" user accounts by default. Local administrative rights will be granted to each student for a specific computer upon the nomination of a faculty member responsible for that computer (The Custodian). The graduate student must first: 1) complete an online seminar on best practices for safe and effective computing provided by the CSA (security.cee.vt.edu), 2) pass an online proficiency exam, and 3) sign a Student Administrative Computer Responsibilities form (see Appendix C) and return it to the CSA.

Faculty should exercise good judgment before petitioning for an escalation of administrative rights for any student and should consider whether it is necessary in order to accomplish specific research goals. Such administrative privileges to any student will be revoked if the student fails to abide by the signed form or when the student completes specific research goals.

6. Personally-owned computers - Personally-owned computers are not supported by the department and are not insured by VT in the event of loss, theft, or destruction while on campus. Users should obtain OS patches, and are referred to the antivirus.vt.edu website, the answers.vt.edu website, and the computing.vt.edu website, as well as some simple instructions for maintaining the integrity of personally-owned computers. Beyond that, users with personally-owned computers may contact the VT Computer Support Center (4-Help) by phone or by website (4help.vt.edu) for technical assistance. Personally owned computers cannot be connected by Ethernet cable to the network within Patton or Durham Halls, but must instead be networked using wireless hardware if a connection is desired. Refer to the wireless.cns.vt.edu website for more information.

4.0 Educational Opportunities

Faculty and students within the CEE Department make extensive use of computer resources on a daily basis. The reality is that most faculty, staff and students have received little or no training experience to maintain a safe computing environment. According to the Computer Emergency Response Team at Carnegie Mellon University, the number of computer security vulnerabilities has increased five-fold. Unfortunately 99% of these vulnerabilities apply to the common Microsoft Windows operating system prevalent in our department.

There is a persistent threat that departmental computing resources will be compromised. Faculty, staff and students have little or no time to become security experts in this ever-expanding field. However, it is believed that the use of existing educational opportunities at the University and training within the department to better manage computers will pave the way for a better use of CEE Departmental computing resources.

1) Faculty, staff and students should be encouraged to attend a computer management course once every year. The University offers courses in various computer topics throughout the year as part of the Faculty Development Institute (FDI). These courses are available to faculty, staff and graduate students. A complete list of courses is available at: https://www.fdi.vt.edu/.

2) The CEE Department CSA will offer short courses that target specific topics of interest to CEE Department users. Areas judged to be critical to better utilize CEE computing resources include: a) basic operating system management and practices, and b) computer security. Certain of these courses would be taught live during the year, and others would be available via video-streaming on the departmental website.

3) The security and operating system management short courses will be mandatory for graduate students and faculty/staff who need to manage computer systems in program area labs. To ensure adequate preparation for managing computer systems, an online quiz will be administered by the CSA that tests for sufficient grasp of modern threats and defense to information systems. This short-course and quiz will be housed within Scholar with access granted to CEE users by PID. All graduate students who use department computing resources must pass the online quiz before making a support request for CSA assistance.

4) It is important to further educate users to relevant departmental policies and computing systems operations near the time that they enter the CEE Department. To meet this goal, all new faculty and staff, including graduate research team members, will be given a copy of the current CEE Department Computing Policies (this document) during their initial orientation to the department. The CSA will offer an introductory education session at the beginning of each academic semester, with the expectation that faculty, staff and graduate students who have recently joined the department will be in attendance. This session will provide

information on all aspects of departmental policies, review CSA services provided to users, and answer questions from participants.

The CSA will establish an educational component to the CEE Department website, where relevant and timely information will be posted regarding departmental computing resources, new University computing information, and other items important to keeping faculty, staff and graduate student users informed on such matters.

5.0 Departmental Backup Requirements and Resources

The overall guiding policy in the CEE Department regarding backup of important data files and documents is that it is ultimately the users' responsibility to back up their own data and critical documents to a secondary media. The CEE Department does provide an option for backup of faculty and staff computers as well as selected graduate research computers (as described below). Some Faculty take advantage of this service, which is provided for free, while others employ their own backup systems. However, the faculty member is ultimately responsible to address financial losses that may occur on a research grant or contract if they have not taken steps to insure appropriate data and document backup in support of that grant or contract.

Faculty and Staff Computers

The CEE Department through the CSA offers targeted directory backups of faculty and staff computers. For Windows computers, this includes the user's email files for Outlook and Eudora, the My Document folders on the desktop, and any user profile folder within Documents and Settings. These partial system backups are provided at least three times a week and are then backed up again remotely to the Virginia Tech Campus's Tape Backup system. Due to network bandwidth and internal storage limitations there are some file types that are excluded from this backup program. These include pictures, music, and video files of any kind. Image files such as ISO's and executables (.exe) are not backed up; likewise, ZIP and TAR files are not backed up. The CSA can also backup Apple and Linux clients with similar limitations.

CEECL, Program Area Labs, and Research Computers

There are currently no backups provided for the departmental computer labs. Data on these machines can be lost at any time either due to hard drive failure or user corruption. CSA will post notices to this effect in all departmental computer labs. It is highly recommended that all users make sure that they are performing some type of personal backup on a regular basis.

Computers that are used by graduate students and purchased by faculty in support of research grants/contracts are not automatically backed up; rather, it remains the student's responsibility to maintain backups of their research data and associated documents, and for faculty members to insure that this is taking place in some manner. Faculty members who employ students using research computers may request that a research computer be placed into the departmental backup system. The faculty member should request this through the Helpdesk and the particular research computer(s) will be placed in the backup queue and will have the same file exclusions as described above in the Faculty and Staff computer section above.

Other backup options

There are networked computers on campus that the University offers for data transfer and storage:

Filebox.vt.edu is freely available to all current students, faculty and staff wishing to store data. This service is available from any networked computer making is useful for transferring files. There is an initial limitation of 25 MB, however users may request more storage if needed.

Network attached storage (NAS) is available for faculty and staff to use. Additional information can be found at http://www.computing.vt.edu/infrastructure_services/nas

More information about Virginia Tech's Network Backup System can be found here:
http://www.computing.vt.edu/security_and_viruses/network_backup/

6.0 Department Cluster Computing Policies

The CSA resources provided by the CEE Department are insufficient to provide full or substantial system support for cluster computing systems that may be developed by selected CEE faculty in support of their research activities. In such instances it will ultimately be the responsibility of the faculty to maintain and support any cluster computing systems that they establish. The following criteria are offered to define expectations in cluster situations.

1) Cluster computing systems in CEE will be used mainly for "number crunching," for prototyping parallel computer programs before installation on Advanced Research Computing systems, and for research on scaling and porting of parallel codes in different systems. A CSA will assist with installation of the operating system, text editors, compilers and parallel programs developed for the cluster but is not expected to install other software.

2) To avoid potential security problems, the faculty responsible for a cluster should have robust firewall security protection activated in the cluster to minimize intrusions. Whenever possible clusters should not be directly connected to the internet. However, there are instances where large file transfers make this situation unacceptable. The firewall (software and hardware) activation is the responsibility of the faculty member(s) who are responsible for the cluster. Whenever possible, the transfer of files from clusters to other computer systems should be done manually through DVD-Rs and external hard drives.

3) Faculty who establish cluster computing systems are responsible for seeing that local back-up systems are installed to insure safe storage of computer programs and data.

4) Maintenance and support of clusters, including maintenance of the operating system and hardware components, will be the sole responsibility of the faculty member who is in charge of the system. Departmental CSA will be available to handle the initial installation of software and establishment of the cluster system configuration.

5) Departmental CSA personnel will be allowed access to cluster computing systems when necessary in the conduct of their duties and responsibilities. Such access should be coordinated with the faculty member(s) responsible for a specific cluster computing system.

6) Faculty are asked to notify CSA personnel at the time computers are purchased with the intent to establish a new cluster computing system. This will allow the CSA to anticipate time commitments necessary to accomplish the initial setup and configuration of the cluster computing system.

7) CEE faculty are encouraged to make appropriate use of the Advanced Research Computing resources (http://www.arc.vt.edu) that have been established by the University.

7.0 Departmental Computer Inventory and Tracking

The CEE Department has approximately 1000 computers that are used in departmental facilities as well as by faculty, staff and students. Such a large number of computers present a variety of logistical challenges in

relation to inventory management and tracking needs. CSA personnel should be made aware of the ordering and pending arrival of new computing resources so that they may schedule time for initial set up and inventory of these new resources upon arrival. The following procedures will be implemented to improve inventory control efficiency and enhance the servicing of new computing resources:

1) All computers and related equipment and software will now be ordered by the CSA personnel.

2) CSA personnel will be notified by Main Office personnel upon the arrival of any computer here in Patton 200. They will relocate the computer to their workspace as quickly as possible to minimize the possibility for the computer to be picked up and relocated elsewhere.

3) CSA personnel will ensure that the computer is processed and delivered to its CEE location within 2-3 business days. Processing will involve appropriate software installations and initial checkout of system. CSA personnel will also make the request at this time to Property Control for an equipment inventory tag.

4) All FDI and BANNER computers received in the CEE Department are to be likewise delivered to Patton 200 and handled in the same manner as described above.

5) The Department Head will notify CSA personnel and Main Office fiscal personnel each year as to the faculty members who have been selected to participate in the FDI Program. Those faculty members will be expected to work with the Department Head and CSA personnel regarding the fate of any computers that are being replaced by new FDI computers.

6) Whenever a desktop computer is to be relocated, the faculty member responsible for the computer is to see that a request is submitted to the Helpdesk to obtain assistance with the relocation. If this relocation procedure is bypassed, the computer may not have the latest software or updates for the operating system and could very easily be vulnerable to remote exploit in a short time period.

Appendix A: Key Components of University Policy 7000

http://www.vt.edu/about/acceptable-use.html

In making acceptable use of resources you must:

- Use resources only for authorized purposes.
- Protect your userid and system from unauthorized use. You are responsible for all activities on your userid or that originate from your system.
- Access only information that is your own, that is publicly available, or to which you have been given authorized access.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

In making acceptable use of resources you must NOT:

- Use another person's system, userid, password, files, or data without permission.
- Use computer programs to decode passwords or access control information.
- Attempt to circumvent or subvert system or network security measures.
- Engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to university data.
- Use university systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates.
- Make or use illegal copies of copyrighted materials or software, store such copies on university systems, or transmit them over university networks.
- Use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or userid.
- Waste computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
- Use the university's systems or networks for personal gain; for example, by selling access to your userid or to university systems or networks, or by performing work for profit with university resources in a manner not authorized by the university.
- Engage in any other activity that does not comply with the General Principles presented above.

Appendix B: Virginia Tech Privacy Policy for Employees' Electronic Communications

1. Purpose

This policy defines the balance between the university's business needs and respect for employees' freedom of inquiry and expression with regard to electronic communications and computer resources owned or provided to employees by the university.

As noted by the 2001 Virginia Tech Strategic Plan, "The core values of Virginia Polytechnic Institute and State University are freedom of inquiry, personal integrity, mutual respect, promoting personal and professional growth, fostering a lifelong commitment to learning, and contributing to society." The core values section of the Strategic Plan also emphasizes the importance of the university as a "community of scholars" embedded in an environment that protects and nurtures freedom for intellectual inquiry.

The Commonwealth of Virginia's Human Resource Policy 1.75 ("HR policy") contains the following statement: "No user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the Commonwealth's equipment and/or access." The HR policy further states that Virginia agencies, including its institutions of higher education, have "the right to monitor any and all aspects of their computer systems" and may do so "at any time, without notice, and without the user's permission." While the policy grants Virginia Tech the right to monitor its computer systems, it does not require it to do so, and states that, "Agencies may supplement this policy as they need or desire, as long as such supplement is consistent with this policy."

In recognition of the complex and unique mission of a land grant university, the Virginia Tech privacy policy supplements the commonwealth's electronic communications policy to tailor it to situations that may arise in a university community, and to further the goals of an academic community expressed in the Strategic Plan. However, it does not create any additional or new legal rights, or new or additional legal expectation to privacy for Virginia Tech employees.

2. Policy

The university does not routinely monitor or access the content of electronic communications, computer files, or voice mail of its employees, whether stored on university equipment or in transit on the university network. Content of employees' electronic communications or files will not be accessed during the execution of systems support, network performance, and related security functions.

However, monitoring or access may be necessary under certain circumstances. This section outlines the legal or administrative circumstances under which access and/or monitoring may occur without further authorization, or when it may occur on a routine basis if specified in an approved departmental policy.

2.1 Legal or administrative circumstances where monitoring and/or access may occur without further authorization are:

- communications or files required to be released by law, by orders of a court, or requested in accordance with the Virginia Freedom of Information Act ;
- approved Internal Audit reviews;
- resolution of technical problems; [Technical staff may inadvertently see or hear potentially illegal content in communications or files while working to resolve technical problems. If so, they are required to report what they have seen or heard to appropriate authorities. Otherwise, the university

expects technical staff to treat inadvertently encountered electronic communications and files of university employees as confidential and not subject to disclosure to anyone.]

- emergency situations involving an imminent threat of irreparable harm to persons or property; and,
- resources assigned to a group or publicly available to any user.

2.2 Routine monitoring and/or access in support of essential departmental operations:

If routine monitoring or examination of employee electronic communications or files are an essential part of the work environment, then the department must develop and maintain a clearly written operating policy that is regularly disseminated to the affected employees. If the policy affects tenure-track or continued appointment track faculty members, then input from the affected faculty members is required before approval. Prior written approval of such departmental policies is required from the relevant dean or senior manager.

2.3 All other cases of monitoring and/or access require authorization as described in the procedures section in part 3.

Virginia Tech requires all employees to obey applicable policies and laws in the use of university computing and communications technologies. Nothing in this policy changes or supersedes these employee requirements.

3. Procedures

Authorization for non-law-enforcement university personnel to monitor or access electronic communications or files of employees will not be granted casually. Such authorization will require justification based on reasonable business needs or reasonably substantiated allegations of violation of law or policy on the part of the employee. In carrying out retrieval of files or information, due respect should be accorded to confidential or personal information and legally protected files.

Explicit consent never constitutes an intrusion. Employees may freely give consent to other individuals to access information stored on equipment or resources assigned to them. No further authorization is required in such instances.

3.1 Investigations of Violations of Law or Policy

Requests for authorization to monitor or review electronic communications or files because of allegations of violations of policy or law by faculty or staff members may originate with supervisors. They may also originate with an investigatory authority such as the Equal Opportunity Office investigating a claim of sexual harassment. Requests must be made in writing and include the rationale for the request, a description of the information or files to be accessed or retrieved, and the proposed handling and disposition of the files. Authorization in such cases may be granted by the relevant dean or senior manager (including vice presidents/vice provosts), or higher level authority if needed.

The senior manager who is asked to consider authorization for monitoring or reviewing the electronic communications or files of an employee must use his or her best professional judgment in determining if there exist reasonable grounds, considering the surrounding circumstances and environment, to grant such authorization. The senior manager is expected to maintain confidentiality in such a situation. He or she may wish to consult with the Office of the General Counsel or Personnel Services in determining whether to authorize monitoring or review, and in determining if the affected employee or anyone else should be notified that the monitoring or review is taking place.

3.2 Business Needs

Where there is a reasonable need for access to routine business or educational documents and the employee is unavailable, authorization to access that employee's electronic communications should be provided by the department head or director, or next higher authority. Whenever possible, the employee should be informed and asked to help in obtaining the needed business materials. If that help is not reasonably available, then other steps should be considered to respect the confidential or personal nature of any other materials present. The employee will be promptly notified of the access and the nature of the documents or communications reviewed or obtained.

4. Definitions

Employees include all persons directly employed by Virginia Tech in their capacity as employees. The policy also covers anyone to whom the electronic communications and computing resources of employees have been extended. These include (but are not limited to) recently terminated employees whose communications and computing resources have not yet been terminated, deleted, or transferred, consultants that may be hired, and individuals whose electronic communications and computing resources continue between periods of employment. This also includes student workers, volunteers, and other individuals who are using state-owned equipment and carrying out university work.

5. References

Department of Human Resources Policy 1.75
http://www.dhrm.state.va.us/hrpolicy/policy/pol1_75.pdf

Virginia Freedom of Information Act Title 2.2, Chapter 37
http://legis.state.va.us/Laws/CodeofVa.htm

University Strategic Plan 2001
http://www.unirel.vt.edu/stratplan/01MVV.html

Administrative Data Management and Access Policy—University Policy 7100
http://www.policies.vt.edu/7100.pdf

Acceptable Use and Administration of Computer and Communication Systems—University Policy 7000
http://www.policies.vt.edu/7000.pdf

Acceptable Use Guidelines
http://www.policies.vt.edu/acceptableuse.html

Management of University Records—University Policy 2000
http://www.policies.vt.edu/2000.pdf

Policy on Intellectual Property—University Policy 13000
http://www.policies.vt.edu/13000.html

Campus Security—University Policy 5615
http://www.policies.vt.edu/5615.pdf

Government Data Collection and Dissemination Practices Act, Sec. 2.2-3800 et seq.
http://legis.state.va.us/Laws/CodeofVa.htm

6. Approval and revisions

Information system technology is characterized by rapid evolution and the development of innovative, novel applications. It is the intent of this policy to establish basic principles that will endure through many evolutions of information systems.

The Vice President for Information Systems is charged with the responsibility to periodically review the policy and propose changes as needed for consideration by university governance.

Appendix C: Student Privileged Computer Use & Responsibilities Form

By these marks and signature of this form, you the student (I) and your faculty advisor attest to the following statements:

- ✓ I have attended or reviewed a Civil & Environmental Engineering seminar on best practices for a safe and effective computing environment and have passed or scheduled to take the system proficiency examination.
- ✓ I have read and will abide by the **CEE Departmental Computing Policies**.
- ✓ I have read, and will abide by, the **VT Acceptable Use Guidelines** also known as Virginia Tech Policy 7000: Acceptable Use and Administration of Computer and Communication Systems viewable at http://www.policies.vt.edu/7000.pdf
- ✓ I have read and will abide by the VT Policy on privacy of electronic communications.
- ✓ I will not install, store or download files that are not required for academic purposes without the direct approval of my faculty advisor. This includes, but is not limited to any other client or server applications that provides peer to peer file sharing programs services or connections, for the purpose of storing, moving, copying, compressing, or distributing pictures, text, binaries, hidden files, alternate data streams, movie files, music files, or any other non-academic file format or application data. I also understand that peer-to-peer file sharing programs such as BIT Torrent, Kazaa, Music Match, Jnutella, or any software or hardware device that may share unauthorized network, processor or memory storage using any network services or local devices directly or in-directly connected to department computers is prohibited and therefore monitored. I further understand that I may *not* install or store illegally-obtained or copy-righted material or software or data files, including peer-to-peer file sharing programs containing such material on any department computer.
- ✓ I will not create or alter any user accounts on any computer owned by the CEE Department without explicit permission from your faculty advisor or a department system administrator.
- ✓ I will insure that automatic updating of the operating system and antivirus software is enabled and working as designed to the best of my ability.
- ✓ I will insure that my research data files are backed up on a regular interval and that my restoration process is tested and successful.

By signing below all parties understand that abusing this policy may cause forfeit of student access to any account on any CEE Departmental computer.

STUDENT INFO: Printed name:_____ VT PID: _____

Student signature:_____Date:_____

FACULTY INFO: I (print name):_____ recommend that this student be granted software installation rights on the assigned research computer owned by the department.

Faculty advisor signature:_____Date:_____