Request for Facilities Network Computer Account

With the exception of required signatures, you must type all information on this form before printing.

Prerequisites

Before Computer Services can set up your new accounts, the following prerequisites must be completed:

1. Your information must be in the Human Resources system. To check on the status, please check with the HR liaison in your department.
2. You must set up your eID (consisting of your eName and ePassword). To register for an eID or verify the status, please visit http://eid.colostate.edu. Your supervisor can assist you with this process. To check on the status, please call 970-491-7276.

Computer Services Processing

When the aforementioned prerequisites have been completed, **please complete all parts of Forms A and B on the computer except the signatures. Print the forms and sign them. Then submit them to Dallace Unger in Computer Services, Facilities Service Center North, Room 100F for review and processing. Computer Services requires two business days to set up a new account *after the forms have been completed, signed and received*.**

By submitting the signed Forms A and B, you are agreeing to abide by University and Facilities rules and conditions governing the use of University resources

Other Computer Use Requirements

- Log out of or lock your computer when you are away from your desk during the workday. When you leave work for the day you **must** logoff and leave the computer turned on, the monitor can be turned off. Computer Services does maintenance on the computers during your off hours. This maintenance includes a reboot all workstations in the department. If you are still logged in at the time of the reboot you risk having the files that are open damaged during the reboot.
- You are responsible for anything done with your computer account. Do not share your password(s).
- Avoid storing work files on your local drives (c:\, d:\); drive failure means the files are gone. Network files are placed on a back-up tape each night and can be restored as needed.
- Software has been installed on your computer that allows Computer Services to remotely control your computer to install software, system patches, and virus updates. This software also allows us to watch your computer remotely to help resolve problems. Keep in mind that Computer Services can view whatever may be on your screen.
- Anti-virus and operating systems updates are done frequently to comply with network security situations that arise and to comply with University policies. Keep in mind that you help us keep the system secure by practicing safe computing.
- We have also installed software to monitor the type of software and hardware on each computer. Unlicensed software will be removed from computers without warning.
- Keep your e-mail folders clean and compacted. Empty the Deleted Items folders once a week and always compact afterwards. Delete unneeded messages from all your folders, especially those messages with attachments. If you need to keep the message but not the attachment, you can delete it by right-clicking on the attachment and selecting Remove Attachment. When you close the message, you will be told that the message has been modified and asked if you want to save the modifications. Answer Yes to completely remove the attachment.
- Do not place files on the root directory of the g:\ drive. Any files placed in the root directory will be deleted without notice. You must register all directories on the root of the G: drive and have a person designated as

being responsible for that directory.

- Archive files and e-mail messages to removable media. Any file that you have not used in the last year should be archived. Computer Services will delete any file that has not been accessed for two years.
- Your eID is required for access to computers, programs and to receive pay advice at the University level. All administrative staff will be required to register an eID when employed by Facilities Management.

For access to University systems, you will need to contact the appropriate department to arrange to get a user ID on that system.

Use of equipment on the Facilities computer network

There have recently been some incidents where people connected non-departmental computer equipment to the Facilities computer network. The CSU IT Security Policy states:

> "Personally-owned computers that routinely use University IT resources, including access to University networks, servers, and/or other IT resources, and/or that contain sensitive University information are subject to the same policies as those computers owned and operated by the University."

Effective immediately, all equipment that is going to be connected to the Facilities computer network must be examined and vetted by our Computer Services personnel before the equipment is connected to the network.

Examples of equipment that will need to be vetted include, but are not limited to:

Laptop computers
Printers
Testing equipment
Meters

To vet the equipment prior to connection, you must make an appointment with Computer Services and bring the equipment in for examination. If it is not possible to bring the equipment in, an onsite inspection can be arranged. You can make an appointment by calling the Computer Services help line at 970-567-1009.

In addition, in order to avoid network compatibility problems, all computer equipment purchased by the department must be discussed with, and approved by, Computer Services personnel prior to the purchase. This requirement applies no matter what budget is being used for the purchase.

Maintenance and support costs on equipment purchased with prior approval of Computer Services personnel will be assumed by the Computer Services budget. Equipment purchased without prior approval of Computer Services personnel will not be supported in any way by the section. Non-approved equipment that causes network compatibility problems will be disabled.

June 13, 2016

MEMORANDUM

TO: All Facilities Management Employees

FROM: Tom Satterly, Associate Vice President

SUBJECT: Computing and Data services

For many of us, access to information in any of its varied forms is crucial to completing our jobs successfully. That access may be calling a customer, accessing an on-line manual for the piece of equipment we are working on, finding the status of an order, replying to an email, and many other needs. Because of these needs, we all need access to what the University now calls "Computing and Data services."

What are Computing and Data services? It is the University's way of talking about all electronic devices; computers, cell phones, tablets, and any device that connects to the world in some way. These are tools that most of us use on a daily basis to complete our jobs. It is our responsibility to do everything we can to keep these tools in working condition and safe.

The University provides Computing and Data services so that we can do our jobs successfully. The University realizes that there may be times when a device may be used for personal issues, but these should be kept to a minimum. Personal use of a device should be limited to appropriate usage during breaks and meal times.

Because of the advances in spam/viruses/social engineering we all need to be aware of what web sites we visit and possible phishing communications. Infected equipment, or the compromising of a system, can cost lost time, productivity, money and/or reputation to both yourself and the department depending on how severe the incident is.

What is phishing? Phishing is where the cybercriminal sending the email offers you some type of bait – money, free gift, etc. – in order to get some personal information back from you – credit card number, Social Security Number, log on id and password, etc. Phishing attempts are often easy to spot because the criminals send the email out to a large number of people, so it tends to be fairly generic. This is not the case with a newer version of phishing called spear phishing. This type of email is specifically designed for you. The criminal researches you and uses this information to create an email that (they hope) is more likely to get you to click on the link or open the attachment. (A recent spear-phishing attack against an accounting team at a company that designs and manufacture aircraft parts got the company to transfer $54 million to the cyber criminals involved.)

In December 2015, we were infected with a virus that started encrypting files on the G drive. Fortunately, the user realized what was happening and turned off his computer and only 8400 files were encrypted. To undo the infection cost Computer Services 60 man-hours to correct the issues and make sure everything was cleaned up. And, this does not account for any lost

productivity for people outside of Computer Services. The FBI says that Ransomware (where a virus infects a computer and then encrypts all the files it can find on the computer, including any server files) alone cost businesses $209 million in the first quarter of 2016. (This number only includes cases reported to the FBI.) And, this number does not account for lost productivity only for the ransoms paid.

Please do your best to use devices in a safe and prudent manner. If you are suspicious of an email, a web page or a link, do not click on it. Contact Computer Services immediately as you can limit the damage. Remember, if a device is found to have been used inappropriately, that information will be passed on to the supervisor.

If you have any questions, please contact Computer Services at 970-567-1009.

Thank you for your support.

FORM A

Request for Facilities Network Computer Account

With the exception of required signatures, you must type all information on this form before printing.

Hand written forms will be returned.

Please note: Employee's name must be in all capital letters and include their middle initial. Please provide a phone number where the employee can be contacted. If the employee does not have a phone, please provide the supervisor's number. Any form that cannot be read or is not signed by the supervisor will be returned.

A new account automatically includes a login to the Facilities Management network. Access to other resources must be requested below on this form.

Employee Name: _____ Section: _____

eName: _____ CSU Email address: _____

Phone number: _____ CSU ID #_____

Are you a student? Yes ☐ No ☐

Do you need access to Microsoft Outlook for your job? Yes ☐ No ☐

Are you a supervisor? Yes ☐ No ☐

Do you need access to the FAMIS system? Yes ☐ No ☐

If yes, to which role should you be assigned:

☐ CSU Employee ☐ RCS or Construction Services Employee

☐ Building Svcs. Supervisor ☐ RCS Manager

☐ Construction Svcs. Supervisor ☐ District Energy Supervisor

☐ Trades Supervisor

☐ Other, please specify: _____

If applicable, select the email distribution list(s) to which you need access:

☐ Trades Maintenance ☐ Building Services ☐ Outdoor Services

☐ Construction Management ☐ Supervisor's (must be approved by Dallace Unger)

Dallace Unger: _____

All employees have **read** access to the K: drive, if you need write access to the K: drive you must get permission from Kristi Buffington and have her sign below authorizing you to have write permissions.

Kristi Buffington: _____

Software

The following software is installed by default on all computers in Facilities Management: Windows OS; Microsoft Office Suite (Word, Excel, PowerPoint, Access); Adobe Reader; QuickTime; Internet Explorer; Mozilla Firefox. If you require specific software not included in the default list, **please attach a separate sheet** listing the software packages, along with a brief explanation of their purpose.

Employee Signature: _____ Date: _____

Supervisor Signature: _____ Date: _____

Supervisor Name (Printed): _____

Facilities Management Addendum to the "Acceptable Use Policy for Computing and Networking Resources at Colorado State University" (Policy ID#: 4-1018-001)

Electronic devices and data services provided by Facilities Management are for University business use. Personal use of the electronic devices and/or data resources shall not interfere with business, nor should it violate acceptable business practices or standards.

Unacceptable business practices include, but are not limited to:

- Viewing, creating or sending pornographic materials.
- Downloading, viewing or copying copyrighted materials such as movies, music, or software.
- Using any electronic device to send or forward discriminatory, questionable or inappropriate jokes, messages, pictures, video or comments.
- Giving my username and password to someone else, even temporarily.
- Accessing or removing files, e-mail or other electronic material belonging to another person, without their explicit permission.
- Accessing, sharing or storing personal identification information. This includes Social Security Numbers, Driver's License Numbers, Credit Card numbers, and any information that violates the expected standard of confidentiality. Only the University Information Technology Executive Committee (ITEC) grants access to such information.
- Using University (or State of Colorado) property or equipment to run a personal business.

Users violating any of these policies will be subject to disciplinary action up to and including termination.

The University's "Acceptable Use Policy for Computing and Networking Resources" (Policy ID#4-1018-001) outlines the University's expectations. By signing this document, you agree to abide by the University and Department policies regarding the use of computing resources.

Employee Signature: _____ Date: _____

Employee Name (Printed): _____

Witness Name: _____ Date: _____

Witness Name (Printed): _____

The full text of policy 4-1018-001 is on the Office of Policy and Compliance web site (http://opc.prep.colostate.edu/) at http://policylibrary.colostate.edu/policy.aspx?id=704.

Modified: 8/19/2019