IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

| | |
|---|---|
| Chalmers Eugene Troutman, III,<br><br>Plaintiff,<br><br>vs.<br><br>Leon J. Hendrix, Jr., J.J. Britton, M.D., Bill L. Amick, Thomas C. Lynch, Jr., Louis B. Lynn, Patricia H. McAbee, Leslie G. McCraw, E. Smyth McKissick, III, Thomas B. McTeer Jr., Robert L. Peeler, William C. Smith, Jr., Joseph D. Swann, all in their individual capacities and in their official capacities, the Clemson University Board of Trustees, James F. Barker, Doris R. Helms and Clayton D. Steadman, all in their individual capacities and in their official capacities,<br><br>Defendants. | CIVIL ACTION NUMBER: 3:08-cv-449-MJP<br><br>**AFFIDAVIT OF PETER T. TROUTMAN** |

PERSONALLY APPEARED BEFORE ME, PETER T. TROUTMAN, who upon being duly sworn, deposes and states as follows:

1. I am the son of Chalmers Eugene Troutman, III, the Plaintiff in this lawsuit. In the Fall of 2005, I enrolled as a full time student at Clemson University, where I am currently in my junior year.

2. In June of 2007, I became employed by Clemson University in the Clemson Computing and Information Technology (CCIT) office as a laptop technician. I was professionally proficient with the installation and configuration of computer software and I had a working knowledge of computers when I took the job. Since being employed, I have received significant on the job training and I have also been trained in several workshops for CCIT laptop

technicians to enhance our skills with Macintosh computers and the Ubuntu operating system. There are approximately twenty students, all part time, who work as laptop technicians at CCIT as do I.

3. My primary job at CCIT is to render laptop computer support to all Clemson computer users which includes students, faculty, staff and administration. I attempt to diagnose and repair software problems for all those who request help with their laptops. If I determine the problem relates to hardware, I send the laptop to our hardware department.

4. One of the most common procedures practiced by all laptop technicians to solve software problems is to overwrite all existing software and essentially reinstall CCIT's standard operating system, device drivers, and software by a process called "reimaging." The reimaging process takes approximately five to ten minutes while to accomplish the same results without reimaging would take about three hours as it would involve manually reinstalling and configuring the computer's operating system, device drivers, and software. Before reimaging a computer, all customer files must be copied to a backup medium such as a compact disk (CD) or another hard drive in order to retain and save them.

5. Many laptop users request a reimage as a form of routine maintenance to speed up their laptop, or to get rid of any viruses and spyware that their laptop may contain. CCIT customers routinely ask that we backup copies of their files onto a disk before the reimaging process is started, because the reimaging process will erase their data. Approximately 10 to 15% of the people who come into CCIT bring their laptop in for reimaging.

6. The reimaging process itself varies depending on the computer model. If it is an IBM, a hard drive containing IBM images and the image transfer program is attached to the laptop needing a reimage. If it is a Dell, the reimage transfer program is run off a compact disk,

and the image is downloaded off a networked computer in the CCIT office through an Ethernet cable plugged into the laptop. In both cases, the content of the "Clemson" image completely replaces the contents of the computer being reimaged with the content of a brand new Clemson issued laptop. It is my understanding that one of the reasons why Clemson University prefers to apply the reimaging process is so that all the computers used by students and others on the campus will be set up in the exact same manner upon issuance.

7. To the best of my knowledge and belief, it is University policy for all university owned computers to be reimaged or destroyed when they are returned to the university. The Clemson University website found at www. clemson.edu /ccit/aboutpolicies/userid password.html, under the heading General Guidelines (third paragraph) states as follows:

> "Any computer tape, disk (hard drive, CD or floppy) or other storage medium used to store sensitive university data must be totally erased or rendered unreadable before it is discarded or disposed of through property transfer or surplus. Employees should contact departmental Technical Support Providers (TSPs), College Consultants or CCIT personnel for assistance if necessary."

8. I am advised that a computer consultant to Clemson University claims that when I reimaged my father's computer, approximately 18,000 files were deleted. I do not believe that is an accurate statement. In my opinion, after a computer has been reimaged, determining an accurate number of files and differentiating a portion of the files from the mass of total files on a hard drive cannot be done with accuracy. The process of the reimage overwrites a large portion of the hard drive's files. Any number produced would have to be an extremely rough estimate, and cover a large range of possible files deleted, not a specific number. I believe any estimate of the number of files deleted as a result of reimaging would have a margin of error of

approximately 35-40%. The margin of error comes from not knowing what portion of the hard drive got replaced with the 7.5 gigabytes of completely new information on a 40 gigabyte drive.

9. When my father asked me to assist him, I did so not because he was my father, but because I am employee of the CCIT office, he was an employee of the university, and the help requested was a routine part of my job. The downloading of his files and the reimaging of his computer occurred on August 6, 2007, while he was still an employee of the University. I reimaged his computer immediately after backing up his files, and the date the files were backed up is date stamped on the original back up disk. I did not believe I was doing anything improper whatsoever. I know my father well enough to say that if there was any hint of impropriety involved in the process, he would never have asked me to download the contents of his computer and reimage it for him. I also assisted him in backing up his computer files when he retired from the Fluor Corporation.

10. During the backup and reimaging process of my father's laptop, no files were deliberately deleted. To the best of my knowledge, all of my father's personal files which were on his laptop were downloaded onto the disk. I do not believe all of my father's emails were backed up onto the disk. I copied the folder that I believed contained his e-mails, entitled, "Eudora," but I did not successfully back up his e-mails because emails are stored in a different part of the computer. Those emails should nevertheless be available to the University because they should still be on the Clemson University server.

11. Attached to this Affidavit is a copy of the complete Clemson University policy regarding reimaging. To the best of my knowledge and belief, this is the process that was followed each time I reimaged a computer at Clemson. In addition to the reimaging of my father's computer, I have reimaged hundreds of others during the time I have been an employee

of the CCIT office at Clemson University. No one has ever claimed this was improper or that it caused a problem.

FURTHER, YOUR AFFIANT SAYETH NAUGHT.

Peter Troutman

PETER T. TROUTMAN

SWORN to and SUBSCRIBED before me
This 30 day of December 2008
Connie N Simpson (L.S.)
NOTARY PUBLIC for South Carolina
My Commission Expires: 9/29/2016

# ATTACHMENT 1
# To Affidavit of Peter T. Troutman
# dated December 30, 2008

Printed from Clemson's Website from the "A to Z" Index" under "Policies and Procedures

Acceptable Use Policy For Employees
print | feedback | text size

# Executive Summary

Computing is an integral part of the academic and business functions of the university. Many university functions that an employee encounters in carrying out their job functions and duties will require that employee to interact with the computing infrastructure and available resources. The computing resources at Clemson University are the property of Clemson University. Clemson University reserves the right to take all necessary measures either proactively or in reaction to an event or the possibility of an event to protect those computing resources.

This document outlines the basic expectations of Clemson University on how each employee will interact with the campus computing systems. Each employee is expected to conduct their computing needs in a manner that in no way jeopardizes the availability of the campus system or any connected system whether owned by the university or some other entity. Additionally, Clemson University strictly prohibits the use of its computing facilities to engage in, participate in, or be party to any illegal activity. The university will monitor its systems in order to protect against such activity. Additionally, university employees are exposed to and have access to sensitive data resources and information, it is expected that the employee will take every known action to protect the privacy and sensitivity of those resources and information.

Any violation of this policy will result in corresponding disciplinary action by the university. Employees suspected to be in violation of this policy will be reported to the appropriate investigative unit, including but not limited to the Office of Human Resources or the University Police Department.

All employees of Clemson University are expected to be familiar this policy and agree to adhere to it prior to using any computing related facilities. Acceptance will be considered as a condition of employment with the University.

# Purpose

The purpose of this policy is to protect the Information Technology resources and the data that is contained in, or manipulated by those IT resources as used in the daily employment duties of the university employee. The shift of computing resources from a centralized data center to the desktop has resulted in a corresponding shift of some of the responsibility for maintaining and safeguarding those resources to the individual employee. The equipment, software and data used by each employee are expensive and vital assets of Clemson University that it is the duty of every employee to protect. In addition, Federal and State statutes protect the privacy of much of the information available on University computer systems.

# Policy

It is the policy of Clemson University that: Clemson University computing resources are the property of Clemson University to be used for university-related business. Employees have no expectation of privacy when utilizing university computing resources, even if the use is for personal purposes. The university reserves the right to inspect, without notice, the contents of computer files, regardless of medium, the contents of electronic mailboxes and computer conferencing systems, systems output, such as printouts, and to monitor network communication when:

1. It is considered reasonably necessary to maintain or protect the integrity, security or functionality of university or other computer resources or to protect the university from liability;
2. There is reasonable cause to believe that the users have violated this policy or otherwise misused computing resources;
3. An account appears to be engaged in unusual or unusually excessive activity; and
4. It is otherwise required or permitted by law. Additionally, the userid and computing services of the individuals involved may be suspended during any investigation of misuse of computing resources.

## Communications

- President
- Provost
- Vice Presidents
- Vice Provosts
- Deans
- Directors/Department Heads
- Director of Human Resources
- All Faculty and Staff

## General Guidelines

All data pertaining to student records, University administration, research projects, any Federal or State information, and any other information not explicitly deemed public shall be considered confidential and will be safeguarded by each employee having access to that data. All employees will adhere to Federal and State laws concerning privacy. Official releases of data under Freedom of Information requests are to be routed through the appropriate vice-presidential area and/or the Office of General Counsel.

All University data, public or private, will be stored in such a manner as to reasonably protect it from loss due to equipment failure, fire, theft, sabotage or human error. The University Records Manager establishes data retention periods. Data backup procedures will include remote storage of backup data, written backup and recovery procedures and periodic verification of storage media.

Any computer tape, disk (hard drive, CD or floppy) or other storage medium used to store sensitive university data must be totally erased or rendered unreadable before it is discarded or disposed of through property transfer or surplus. Employees should contact departmental Technical Support Providers (TSPs), College Consultants or CCIT personnel for assistance if necessary.

All employees will safeguard their computer userids and passwords. No employee will allow unauthorized persons access to University data or computing or network resources by sharing their userid and password. Employees should reference CCIT documentation on selecting strong passwords. Departmental servers will use CCIT provided security for access to sensitive data or applications. No server will store userids and passwords on the server.

No employee will knowingly create access into the computing network in such a way as to bypass University security systems. Employees will make reasonable efforts to insure that no software or hardware under their control allows unauthorized access to University data. Administrators of departmental servers will regularly apply operating system security patches and service packs. All unnecessary server services will be turned off.

No employee will attempt to use the University network to gain unauthorized access to other computing resources or data, nor will they knowingly attempt to disrupt the operation of any computer system or network.

No employee will knowingly violate software licenses or copyrights during the course of their job duties or at any time while using University equipment or software. Employees are responsible for producing proof of license for any software installed on their University-supplied computer. Licenses for personally-owned software installed on a university computer should be kept with that computer.

No employee will use University data, computing resources or the network for illegal activities or for personal gain.

All employees will safeguard the software and data resources on their workstation or personal computer by installing University-licensed virus protection software or an equivalent package and running this software at regular intervals. Departmental servers and other shared computing resources will also run virus protection software if it is available. Departmental TSPs or College Consultants can assist in installing and running the virus protection software.

All employees will do their best to ensure all software or data is virus-free before it is installed or loaded on a University computer system. Any detection of a software virus will be reported immediately to the departmental TSP or, if no TSP is available or assigned, the College Consultant, or to the IT Support group in CCIT.

No employee will use the University electronic mail system to falsify the identity of the source of electronic mail messages; send harassing, obscene or other threatening electronic mail; attempt to read, delete, copy, or modify the electronic mail of others without their authorization;

or send, without official University authorization, "for-profit" messages, chain letters, or other unsolicited "junk" mail.

## Disciplinary Sanctions

The university will impose disciplinary sanctions on employees who violate the above policies. The severity of the imposed sanctions will be appropriate to the violation and/or any prior discipline issued to that employee.

## Definitions

References and Related Documents

Userid and Password Policy

http://www.clemson.edu/ccit/about/policies/userid_password.html

## Revisions

January 2009

## Approvals

IT Council