SOP-I-0018	DELTA Computer Use
SOP Type:	☒Internal SOP - DELTA-level that does not directly affect entities outside of DELTA ☐External SOP - DELTA-level that affects these entities: ☐Unit SOP - DELTA individual unit(s) affected:
Contact:	DELTA Business Office
Effective Date:	November 1, 2009 Last Revision Date: July 16, 2018

1. Introduction

The purpose of this SOP is to help make DELTA staff aware of the university's computer-use and anti-virus regulations, and to highlight or expand upon the regulations where needed.

2. Computer Use Regulation

All DELTA employees shall comply with the NC State University Computer Use Regulation. Additional information can be found under IT Rules, Regulations and Procedures.

DELTA IT staff may install software-auditing utilities on any DELTA-owned computer for the purpose of tracking software licenses.

3. Anti-Virus Software Regulation

All DELTA employees shall abide by the NC State University Anti-Virus Software Regulation and Antivirus Resources.

4. Illegal File Sharing

DELTA employees are reminded of the personal risks and legal consequences of unauthorized distribution of copyrighted materials, including illegal peer-to-peer file sharing. Music, movies, videos, games and other online media are protected by (or subject to) copyright laws. It is usually illegal to share them via peer-to-peer applications. NC State University faculty and staff are expected to respect the intellectual property rights of others and refrain from copyright infringement. For more information, see this memo from the chancellor.

5. Loaner Computers

Any computer loaned to faculty or entities outside of DELTA must have a mechanism by which it will be restored to a known, good state once returned. When a computer is returned DELTA's Desktop Support unit will be responsible for wiping clean and re-imaging. Contact delta-desktop@help.ncsu.edu for any questions or to reserve a computer or laptop for loan.

6. Email Usage Policy

In accordance with NC State University Data Management Procedure, DELTA is committed to protecting University data. As such, this email policy is in place to ensure the proper use of the NC State email system and policies and make users aware of what DELTA deems as acceptable and unacceptable use of the email system. This policy outlines the minimum requirements for use of email within DELTA.

All use of email must be consistent with DELTA policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices. DELTA email accounts should be used primarily for DELTA business related purposes. Occasional, inconsequential personal communication and use of University IT resources is permitted to any users who satisfy the conditions in Section 3 of the University Computer Use Regulation. Users of such resources should do so with no expectation of privacy.

Email is an NC State business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email pursuant to University REG 01.25.12 - University Record Retention and Disposition Regulation. The NC State email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any DELTA employee should report the matter to their supervisor immediately.

Users are discouraged from automatically forwarding DELTA email to a third party email system. NC State OIT recommends keeping work-related email in your official account, but does not require it. Individual messages which are sent or forwarded by the user must not contain data classified as Yellow or above, as defined in University REG 08.00.03 - Data Management Procedures. The official email system to be used is the NC State G Suite and will be used to conduct DELTA business, to create or memorialize any binding transactions, or to store or retain email on behalf of DELTA.

Using a reasonable amount of DELTA resources for personal emails is acceptable as long as the user satisfies conditions mentioned in the Computer Use Regulation.

Sending chain letters from an NC State email account is prohibited.

DELTA employees shall have no expectation of privacy in anything they store, send or receive on the university's email system. DELTA is not obliged to monitor email messages.

The Senior Management Team or their designee may verify compliance to this policy through various methods.

Any exception to the policy must be approved by the Senior Management Team in advance.

An employee found to have violated this policy may be subject to disciplinary action.

7. User Access Controls

In accordance with NC State University Security Standards for Sensitive Data and Systems Rule DELTA ETS shall implement an Access Control Policy for management of access right requests, access authorization and approval and administration of user accounts.

User account management for all systems that store University Data should adhere to the University Rule. Account creation, modification and termination documentation should be stored for each staff member in order to provide evidence of user roles and privileges within University systems.

Once a staff member is onboarded within DELTA, a request for that staff member will be submitted to delta-desktop@help.ncsu.edu in order to have the appropriate access created for the staff member to complete their daily work. Each account will be provided with the minimum necessary privileges to complete their work. Should a user require additional privileges, a request must be submitted from the user's manager via an email delta-desktop@help.ncsu.edu in order to maintain appropriate documentation regarding the user account and assist in the account privilege review processes required by the University Security Standards for Sensitive Data and Systems Rule.

User termination procedures should be completed upon the user's last day of work. As part of the off-boarding process, access should be adjusted to the levels agreed upon by the off-boarding team member, their manager and the DELTA business office. These access level agreements should be discussed and documented before the user's last day.