NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

SEC. VII — E-MAIL 2.0

EMPLOYEE EMAIL USE

University Policy

I. Scope

The purpose of this policy is to ensure the proper use of North Carolina Agricultural and Technical State University's email system used by faculty and staff, contract employees, guests, etc. (All of the preceding groups will be referred to in this policy as "Employees." The employee email system shall be referred to in this policy as "University Email Accounts" and is located on the domain ncat.edu") Electronic Mail is a tool provided by the University to complement traditional methods of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. Violations of policy may result in restriction of access to the University Email Accounts. In the event a University employee holds both a University Email Account and a Student Gmail Account, the more stringent rules of the policy for Employee Email Use shall apply.

II. Policy Statement

A. Account Creation

University Email Accounts are created based on the legal name of the employee as initiated by the Human Resources or Payroll offices. The format of user names will be based on the user's first initial, middle initial (if applicable), and last name. If the generated user name has already been used, a sequential number will be appended to the user name. Requests for mail aliases based on name preference, middle name, nicknames, etc., cannot be accommodated. An existing email username already in use before the change to the standardized format will be kept as an email alias to the new username. Only requests for name changes to correct a discrepancy between an email account name and official University records will be processed, in which case the email account name will be corrected. User id's will remain in the University's system and will not be reused at any time.

B. Ownership of Email Data

The University owns the University Email Accounts and the messages in those accounts. Subject to underlying copyright and other intellectual property rights under applicable laws and University policies, the University also owns data transmitted or stored using the University Email Accounts.

C. Personal Use

Incidental personal use of a University Email Account is acceptable. However, conducting business for profit using a University Email Account is forbidden. Use of a University Email Account for political activities e.g. supporting any person for political office or attempting to influence the vote in any election or referendum, is forbidden. Any use of a University Email Account to represent the interests of a non-University group must be authorized by the Chancellor or his/her designee. Should the employment or student relationship between the University and user terminate, access to personal email located on University servers will be terminated as well. North Carolina Agricultural and Technical State University assumes no responsibility for access to or support of personal email transmitted to or received by a University server.

D. Privacy and Right of University Access

Work related messages on a University Email Account are the property of the University, are a public record, and may be viewed at the discretion of the University. Users of University Email Accounts should not have any expectation of privacy or confidentiality for personal messages in their accounts. Personal email messages in University Email Accounts are not private or confidential, and anyone who sends a personal email through the University email system is hereby deemed to have consented to a search of such

personal emails. Do not use a University Email Account for personal emails if you object to the University having potential access to your personal emails.

Under certain circumstances, it may be necessary for the IT staff or other appropriate University officials to access University Email Accounts; these circumstances may include, but are not limited to, maintaining the system, investigating security or abuse incidents, or investigating alleged violations of this or other University policies.

A & T staff or University officials may also require access to a University Email Account in order to continue University business where the University Email Account holder will not or can no longer access the University Email Account for any reason (such as death, disability, illness or separation from the University for a period of time or permanently). Such access will be on an as-needed basis and any email accessed will only be disclosed to those individuals with a need to know, as determined by the University's legal counsel and/or Human Resources or as required by law.

E. Auto Forwarding

Users of University Email accounts are forbidden from using automated or manual processes to forward or synchronize sensitive data contained in employee email from the University's servers to another email account, server, or storage system. Sensitive data is defined in *The Data Classification Policy (http://www.ncat.edu/legal/policies/sec7-info-tech/data%20classification.pdf)*

F. Data Purging

Messages in University Email Accounts are automatically purged from trash and junk folders as follows:

Trash / Deleted Items – 15 days
Junk / Junk Email – 30 days

Due to finite resources DoIT has the right to determine the amount of space allocated to a University Email Account and revise the above purge policies.

G. Data Retention

The University will retain a copy of all incoming and outgoing email messages for a minimum of 3.5 years for all University Email Accounts.

H. Data Backup

The University Email Accounts are backed up on a regular basis as a way of recovering from a systematic loss impacting the entire email system. User files and folders are not backed up individually. DoIT staff cannot accommodate requests to restore these files or folders.

I. Expiration of Accounts

Individuals who separate from the University, e.g. to take other employment, retire, transfer to another college, or simply go on to other activities, will have their University Email Account purged. There are many situations at the University where the expiration of accounts will differ, as set forth below. Notwithstanding the guidelines below, the University reserves the right to remove email privileges at any time.

Employees are extended an account as part of their employment. Upon separation of an employee from the University, an employee's e-mail access is terminated. During the exit interview process conducted by Human Resources, terminated employees have the opportunity to provide a third party email address for the purpose of receiving university email related to the termination process. Human Resources updates the Banner system with the separated employee's third party e-mail address as the preferred email address to receive University related communications.

J. Appropriate Use

When using email as an official means of communication, employees must apply the same professionalism, discretion, and standards that they would use in written business communication. All email is subject to public records/disclosure laws. Users of email shall not disclose information about students and/or employees in violation of University policies or laws protecting the confidentiality of such information.

The Data Classification Policy (http://www.ncat.edu/legal/policies/sec7-info-tech/data%20classification.pdf) is applicable to all users that have University issued e-mail accounts. Emailing restricted data is subject to protective governance including but not limited to federal and state statutes/regulations, industry standards, and University policies. University divisions, offices, and organizations that collect employee, student, alumni, vendor, and guest data are responsible for understanding and abiding by email regulations, standards, and policies that pertain to restricted personnel, medical, financial, University business, and research data.

- University business processes that require restricted data such as social security numbers, banking information, credit card numbers, and birth dates to be emailed must be documented and approved by senior management, and must be sent encrypted. Otherwise, such restricted data cannot be emailed.
- An identification number must be truncated if it is not necessary to transmit the full identification number. If the full identification number must be emailed, the transmission must be encrypted.
- Encryption is required for the transmission of access controls.

No technical data with potential for military defense application or otherwise subject to export control or other international trade control laws may be transmitted or stored in an

unencrypted format. Users who use email communications with persons in other countries should be aware that they may be subject to the laws of those other countries and the rules and policies on others systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, regulations, rules, policies, contracts, and licenses applicable to their particular uses.

Approval and transmission of email containing essential University announcements to students, faculty, or staff must be obtained from the responsible University official noted as follows:

- for sending to all faculty, approval from the Provost and Vice Chancellor of Academic Affairs,
- for sending to all staff, approval from the Vice Chancellor for Human Resources,
- for sending to all students, approval from the Vice Chancellor for Student Affairs.
- for sending of information technology communications, Vice Chancellor for DoIT.

Use of distribution lists or 'reply all' features of email should be carefully considered and only used for legitimate purposes as per these guidelines. In some cases where email messages generate a high number of responses due to the subject matter, it may be appropriate to utilize the University's survey software available through the Department of Institutional Research.

K. User Responsibility

A & T DoIT maintains the University's official email system. Employees are expected to read email on a regular basis and manage their accounts appropriately. An email message regarding University matters sent from an administrative office, faculty, or staff member is considered to be an official notice.

Sharing of passwords is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is deemed to be authored by the account holder (unless proven to the contrary), and it is the responsibility of that holder to ensure compliance with these policies. Users must change their passwords every 90 days. Detailed information can be found at: http://www.ncat.edu/divisions/doit/dept/ats/change-password.html

L. Departmental and Organizational Accounts

Requests for shared departmental accounts will be accommodated, but require a designation of an account holder, who will administer the addition, deletion, or modification of names within the account, as well as manage the account consistent with these policies. These accounts will be created with an expiration date of one (1) year, at which time the holder can request a renewal, which will be granted pending verification of identity and the member list. Shorter expiration dates will be given where appropriate,

to accommodate specific time-sensitive needs. Supported types of shared accounts are designated as:

Type 1 – This id will be able to receive mail from anywhere on the Internet, but will have no direct reply capability. The group/organization utilizing this type of generic id will be required to utilize their own University email id to respond to the originators of any mail received by this generic id. These accounts will only be granted for SGA or Faculty/Staff recognized activities or organizations with approval from the faculty advisor of the organization (for SGA).

Type 2 – This id will be able to receive mail from anywhere on the Internet, and will be able to respond directly to the sender. The generic id will be unable to access any of the predefined mailing groups that exist within the campus environment. Members of the group/organization utilizing this type of generic id will have to utilize WEB mail to read and respond to any mail sent to the generic id. The WEB interface will allow users to "sign in" to the generic id utilizing the generic id and their own personal LDAP password. Mail sent from the generic id will not reflect the identity of the responder, but will instead carry the identity of the generic id. Due to security concerns given the anonymous nature of email originating from these types of id's, no students will be allowed access to Type 2 accounts. If a student is found to have access to these accounts, the holder will be notified of the impending removal of the student account. Repeated violations will result in deletion of the type 2 account.

M. Supported Mail Clients

The University-supported email client is Lotus Notes and the web portal is located at https://webmail.ncat.edu. The Division of Information Technology will not support alternate email clients. Helpdesk personnel will work with the individual to access email via the supported methods and will verify functionality of the supported environment. The University Division of Information Technology is continually evaluating tools and technologies and reserves the right to modify the list of supported clients with appropriate notification.

N. Inappropriate Use

Inappropriate email usage, examples of which are described below and elsewhere in this policy, is prohibited. Users receiving such email should immediately contact DoIT.

- Generation of email related to any political activities.
- Generation of email for personal financial gain.
- Generation or facilitation of unsolicited bulk commercial email.
- Infringement upon another person's copyright, trade or service mark, patent, or other property right or intending to assist others in defeating those protections.
- Violation of, or encouragement of violation of, federal and/or state laws and/or the legal rights of others.

- Is for any unlawful, invasive, defamatory, or fraudulent purpose.
- Intentionally distributing viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature.
- Interfering with the use of the email services, or the equipment used to provide the email services, by customers, authorized resellers, or other authorized users.
- Altering, disabling, interfering with or circumventing any aspect of the email services.
- Testing or reverse-engineering the email services in order to find limitations, vulnerabilities or evade filtering capabilities.
- Constituting, fostering, or promoting pornography.
- Inciting violence or threatening violence against one or more persons or property, or containing unlawfully harassing content.
- Creating a risk to a person's safety or health, creating a risk to public safety or health, compromising national security, or interfering with an investigation by law enforcement.
- Improperly exposing trade secrets or other confidential or proprietary information of another person.
- Misrepresenting the identity of the sender of an email.
- Using or attempting to use the accounts of others without their express permission.
- Collecting or using email addresses, screen name information or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting).
- Using the service to distribute software that covertly gathers information about a user or covertly transmits information about the user.
- Any conduct that is likely to result in retaliation against the University's network or website, or the University's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS).

These guidelines provide some examples of permitted or prohibited use of email. This list is not intended to be exhaustive but rather to provide some illustrative examples.

O. SPAM & Virus

Incoming email on the University Email Accounts is scanned for viruses and for messages deemed to be 'SPAM', or unsolicited advertisements for products or services sent to a large distribution. Suspected messages are blocked from the user's inbox. Due to the complex nature of email, it is impossible to guarantee protection against all SPAM and virus infected messages. It is therefore incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases viruses appear to be sent from a friend or coworker, therefore attachments should only be opened when the user is sure of the nature of the message. If any doubt exists, the user should contact the Aggie Tech Support Helpdesk at: (336) 334-7195 and forward a copy of the email to spam@ncat.edu

III. Enforcement

Enforcement of this policy includes the following:

- Divisional and departmental assessments
- External and internal audit compliance

University sanctions for a user cited for policy violations include but are not limited to one or more of the following:

- Suspension of information system(s) privileges. [In order to reduce the number of credentials used to access University resources, single sign-on/reduced sign-on identity management solutions are enabling users to access multiple resources with the same credentials. Suspended access will impact a student's ability to complete academic requirements and/or an employee's ability to perform his or her job duties.]
- Misconduct review.
- Discharge of employment.
- Student dismissal.
- Breach of contract/agreement filed against guests.

For University employees and students, sanctions will be administered in accordance with the Student Handbook, the Faculty Handbook, University Policies, and the Office of State Human Resources Policies.

Date Policy is Effective: Upon approval

Approved by the Board of Trustees

First approved: November 22, 2013
Revised: