North Carolina Agricultural and Technical State University
Information Security Plan

I. Summary

The information security plan defines acceptable use to University resources including but not limited to computer systems, networks, software, hardware, and data in electronic or printed format. The plan helps protect the integrity, reliability, availability, and confidentiality of applicable resources. Compliance with federal, state, and University system level and institutional level laws, regulations, policies, standards, processes, procedures, guidelines, and practices govern the policy and promote the mission and goals of the University. The plan applies to personnel, students, alumni, retirees, guests, vendors, consultants, and applicable University affiliates.

II. Responsibilities of Users

The responsibility of users is vital to the integrity, reliability, confidentiality, and availability of the University's information technology resources. User responsibilities include but are not limited to the following:

- Comply with federal, state, and University system level and institutional level laws, regulations, policies, standards, processes, procedures, guidelines, and practices.
- Adhere to account management best practices.
    - Don't share account(s) information with another person.
    - Secure account information if it's in written or printed format. Account(s) information that is attached to a computer hardware device or that is easily accessible to others is prohibited.
    - Use the following password strategies: upper and lower case letters, letters and numbers, and/or special characters.
    - Select a password that you can remember but one that can't be easily figured out by someone else.
- Don't access an account not assigned to you regardless of whether the account information was given directly to you or obtained by mistake.
- Log off and/or secure your workstation(s) and workspace when the workstation(s) and/or workspace are not in use.
- Be mindful of your office surroundings especially if you are in an open space area with little privacy; someone may be looking over your shoulder without you realizing it.
- Report actual or suspected abuse of information technology resources to the system administrator, Aggie Tech Support, and/or IT Security and Audit.
- Use the University's information technology resources for the purposes for which they are intended.
- Backup data.
- Help eliminate vulnerabilities and system functionality issues by keeping your computer updated by routinely checking your software vendors' websites for patches. Use tools such as spyware and anti-virus software to help protect your computer as well.

- Utilize a firewall. A firewall can be hardware or software that can prevent unauthorized access to your computer. A firewall must be configured properly in order for it to be effective. Beware that firewall restrictions may prevent access to system and/or network resources if its not configured correctly.

III. Responsibilities of System/Data Custodians and Administrators

Besides participating in the planning and implementation stages, system/data custodians and administrators must exercise due diligence with the following responsibilities:

- Be compliant with federal, state, and University system level and institutional level laws, regulations, policies, standards, processes, procedures, guidelines, and practices.
- Ensure the integrity, reliability, and availability of the resource(s).
- Consult with system/data owners on user access and privileges while using the principles of least privileges and separation of duties as a guide.
- Make sure resources have adequate physical security.
- Plan for threats and have documented threat management strategy defined.
- Maintain data confidentiality.
- Implement an account management strategy.
    - Require password to be a minimum of six (6) characters with a password strategy of upper and lower case letters, letters and numbers, and/or special characters.
    - Require password changes. A user should change his or her password(s) every 45 days at a minimum. Depending on which system a user has access to may dictate his or her password reset frequency. System administrators must reset high security accounts every 30 days.
- Reduce access to information technology resources when the granted privileges are no longer necessary.
- Terminate resource access when employment ends. The Benefits Office will have to notify the Division of Information Technology (DoIT) on a retiree's behalf in order for a retiree's e-mail account to remain active. A person who is no longer employed by the University but is enrolled as a student at the University may maintain access to resources that are necessary for the person to function as a student (i.e. e-mail, academic lab access). In a University environment, in order to address the issue of former employees being rehired by the University, do the following:
    - Disable instead of deleting resource access for twelve (12) months upon termination of employment or University affiliation.
    - Delete resource access after resource access has been disabled for twelve (12) months.

IV. Responsibilities of Data Owners

Data owners are responsible for the data integrity. Data owners play a critical role in the layered security strategy from the standpoint that a data owner decides who and what a user(s) can access. Data owners must be prudent with the following responsibilities:

- Disclose to the users relevant legal requirements and ethical obligations for the release of information.
- Publish any departmental policy on the release of information.
- Implement a data classification system whereby data is rated according to sensitivity, confidentiality, proprietary value, and/or other criteria.
- Maintain a list of authorized users.
- Develop procedures related to the granting of, modification of, and denial of access for new, existing and terminated/transferred employees.
- Exercise the principles of least privileges and separation of duties.
- Review methods for safeguarding information from unauthorized use, improper disclosure, accidental alteration and accidental or intentional destruction.
- Develop an electronic records retention and disposition policy.
- Provide users with sufficient training in the use and protection of information.

V. Network Security

Network security protects the integrity, reliability, and confidentiality of the University's network, data resources, and the computer systems attached to the network. Access to the University's wired and wireless network is for legitimate use by authorized users.

A. Device Connectivity and Configurations

1. All devices connected to the University network must be properly registered. Dynamic Host Configuration Protocol (DHCP) is the standard configuration for automatic IP address distribution. Connecting a device to the network with static information is prohibited unless approved by Division of Information Technology (DoIT).
2. All devices approved for use at NC A&T SU must be properly protected from system vulnerabilities (e.g. latest operating system patches, anti-virus software with the latest virus definitions, spyware, password protection etc.).
3. Network connectivity devices, whether software or hardware, must be approved by DoIT before they are connected to the University network. These devices include devices such as hubs, switches, routers, bridges, and modems. A network interface cards (NIC) is usually an integrated component of a computer's configuration. Users are responsible for making sure that they use NICs compatible with the University's network.
4. Switch and router configurations affect the way data is transmitted and devices are connected to the University network. The configurations are maintained by DoIT and are reviewed regularly. Configuration change requests must be

reviewed by the Change Control Board (CCB) where a decision will be made to either approve or deny the request.

5. Physical access to University networking equipment (routers, switches, hubs, etc.) must be approved by DoIT.

B. Perimeter Firewall & Intrusion Detection and Prevention

The intrusion detection system prevents vulnerabilities from negatively impact the network. The University perimeter firewall filters inbound and outbound network traffic. The ability of computers to communicate with each other or to access network services (i.e. the Internet) is made possible through ports. Select ports are opened while others are closed. The decision to open or close a port is based on network security. The necessity for University patrons to conduct academic and administrative business is also taken into consideration.

A request to open a port on the firewall must be submitted to the Aggie Tech Support. Each request will be reviewed by the Change Control Board (CCB) where a decision will be made to either approve or deny the request.

C. Network Monitoring and Maintenance

Intrusion logs and data traffic are monitored regularly in order to detect abnormal network activity. Noncompliant devices will be disconnected from the network. The Division of Information Technology (DoIT) reserves the right to access computer systems and review information when there is reasonable cause to suspect state, federal, or University violations. Port scanning or network monitoring tools cannot be used to access University resources without DoIT's permission.

Users can report suspicious or inappropriate network behavior to the Networking Services, Aggie Tech Support, or the IT Security and Audit department.

VI. Security Contact and Incident Response

The Department of IT Security & Audit is the point of the contact for information technology security related issues. Users can contact Aggie Tech Support or IT Security and Audit in order to report an incident. Incidents, notifications, and violations will be handled accordingly and may necessitate third party participation.