South Carolina
DEPARTMENT OF AGRICULTURE
HUMAN RESOURCES DEPARTMENT
1200 Senate Street, Wade Hampton Bldg 5th Floor, Columbia, SC 29201

Hugh E. Weathers, Commissioner

INFORMATION TECHNOLOGY POLICY

THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY. THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENTS OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.

I. POLICY STATEMENT

Access to and utilization of information technology (IT) resources (e.g., cell phones, e-mail, electronic devices, video communication, facsimile, and future technologies), computer systems, and networks owned or operated by the South Carolina Department of Agriculture (SCDA) impose certain responsibilities and obligations on SCDA employees (hereinafter termed "users") and are subject to state government policies and local, state, and federal laws. Acceptable use is always ethical and reflects honesty. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual's right to freedom from intimidation, harassment, and unwarranted annoyance.

SCDA utilizes the principle of least privilege for systems access, as such, users may be subject to limitations on their access to and the use of the networks as determined by the appropriate supervising authority. In order for users to gain additional systems access, an access change form will need to be completed by supervisors and processed through the IT department.

Users are advised that allowing others to access their IT resources, computer system, or network account, constitutes a violation of this Policy, which may result in access being restricted or withdrawn. Where relevant, all SCDA policies — including but not limited to those governing harassment, discrimination, ethics, confidentiality, and security — apply to Internet, network, and electronic mail use and content.

By participating in the use of networks and systems provided by SCDA, users agree to be subject to and abide by this policy for their use.

Willful violation of the principles and provisions of this policy may result in disciplinary action up to and including termination of employment.

This policy shall be reviewed, at minimum, annually.

II. ACCEPTABLE USE, MONITORING, AND PRIVACY

A. Acceptable Use

Access to the Internet and SCDA network is provided as a tool for the SCDA stated business activities. The IT resources, computers, mobile devices, associated files, associated software, and attached systems are all property of the SCDA. As such, any work product, files, etc. created using SCDA assets automatically becomes SCDA property and users should have no expectation of retention of files upon separation from the agency. No personal files should be stored on SCDA systems, any files stored on SCDA systems become SCDA property.

Users should make every effort to ensure that work product files (documents, data files, etc.) are saved to OneDrive or to network drives. This will help ensure that all SCDA data is backed up. Files stored locally may be lost in the event of a catastrophic failure or damage.

Only in rare instances, approved by supervisor, should a user place SCDA files on removable media. In the event that it becomes necessary, removable media should be obtained from the IT department, and, upon the ending of said event, media should be returned to the IT department for deletion and sanitization.

Users must ensure that any Personally Identifiable Information (PII) sent via electronic mail is sent encrypted. Additionally, IT staff must utilize encryption if they transmit temporary passwords via electronic mail.

B. Monitoring

Use of network services provided by SCDA is subject to monitoring for security, network management, or other purposes deemed appropriate by SCDA management. SCDA has software and systems in place that monitor and record all Internet usage. Its security systems are capable of recording each website visit, each chat, newsgroup or electronic mail message, and each file transfer into and out of our internal networks, and the SCDA reserves the right to do so at any time.

C. Privacy

No employee should have any expectation of privacy as to system, Internet, or electronic mail usage. Employees are therefore advised of this potential monitoring and of the fact that there is no expectation that any system, Internet, or electronic mail usage is private. SCDA may suspend access to its network and the Internet at any time for technical reasons, policy violations, and other concerns.

III. PERSONAL RESPONSIBILITY

By accepting your user credentials and password and related information, and accessing the SCDA network or Internet, users agree to adhere to this policy. Users also understand that they have a duty to report any network or Internet misuse or abuse to their Division Deputy Commissioner, or to the SCDA Information Technology Department. Misuse includes policy violations that harm another employee or another individual's property.

A. System Integrity

Users are responsible for ensuring the integrity for any and all system credentials (to include, but not limited to, network account, electronic mail, computer access, mobile device access) to which they are given access. To this end, users understand that **password sharing is strictly prohibited**. At no time, nor for any purpose, should they give, communicate, or allow their password to be seen, whether verbally or in writing, by others. In the event that another user needs access to an SCDA system, they will need to request access through the appropriate channels. This policy should not be construed to prohibit IT staff from giving or communicating a temporary password to a user for the purpose of establishing or restoring access to systems to which that user has been given access.

Additionally, users understand that they have a duty to ensure that any system to which they are given access is secured whenever they are not actively utilizing them. Computers, mobile devices, etc., should be screen locked whenever a user steps away from or puts down a device that they were accessing.

If at any time a user observes or suspects that the integrity of the system has been breached, they are required to immediately report the breach to the SCDA IT department and their supervisor. Failure to do so may be interpreted as complicity should their knowledge of the breach be discovered.

B. Physical Security and Protection of Devices

Users are responsible for exercising a reasonable duty of care to keep SCDA IT assets safe. Devices should not be left unattended in public spaces, nor should they be left in a vehicle.

When devices are issued with protective cases, those cases should not be removed, except at the direction of the IT department for the purpose of maintenance.

Users have a duty to report damage or theft immediately to the IT department and their supervisor.

At no time should SCDA IT assets be operated by non-SCDA staff, except in the cases of those systems designated for use by non-SCDA staff (i.e. Presentation computers at Buddy Jennings Training, Wade Hampton Conference Room, Phillips Market Center Conference Room, etc.)

IV. VIOLATIONS

SCDA IT resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, personal business ventures, or for the solicitation of performance of any activity that is prohibited by any local, state, or federal law.

Users are expressively prohibited from using SCDA IT resources, computer systems, and the network for:

A. Engaging in immoral, illegal, or unlawful activities, violating the Policies and Procedures of SCDA, or encouraging others to do so. Examples include (but are not limited to):

   1. Accessing, transmitting, receiving, or seeking unauthorized, confidential information

   2. Conducting unauthorized activities

3. Viewing, uploading, printing, copying, filing, transmitting, downloading, or searching for obscene, pornographic, sexually explicit, illegal, or otherwise objectionable, non-business-related Web content

4. Intercepting communications intended for others

5. Downloading or transmitting SCDA confidential information without proper authorization

6. Downloading unapproved software of any type or visiting malicious websites

B. Using or installing software not licensed or approved by the SCDA.

C. Installing or using hardware or peripheral equipment not specifically approved and authorized by the SCDA Information Technology Department or using approved equipment in a manner inconsistent with the approved purpose for which the equipment was installed. Prohibited equipment examples include any electronic surveillance, audio, or video recording equipment not directly related to functions required by job duties and responsibilities.

D. Vandalizing or using the network to disrupt network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of viruses, harmful components, or corrupted data.

E. Attempting to circumvent or subvert system or network security measures. This includes, but is not limited to, installation of software or hardware designed to intercept, collect, or monitor system data or files, installation of software or hardware designed to simulate activity for the purpose of keeping a screen active (i.e. jiggler devices).

F. Intercepting network traffic for any purpose unless engaged in authorized network administrative duties.

G. Making or using illegal copies of copyrighted software or other mediums, storing such copies on SCDA systems, or transmitting them over SCDA networks. Users who violate any copyright declarations are acting outside the course and scope of their employment or other authority and the SCDA is relieved of any legal responsibility thereof. Users will be personally responsible and liable for such infringing activities.

V. NON-WORKING TIME LIMITED PERSONAL USE

SCDA computer systems and networks are to be used primarily for conducting official state business. It is recognized that employees may occasionally use these systems and networks for limited incidental personal use during non-working time. Such limited personal use may be acceptable as long as other usage policies are followed and the use does not interfere with an employee's work or negatively impact the computer system or network and does not result in additional public expense. These systems are not available or accessible for public speech or any First Amendment expressive activity or for use by the public; further, the systems are expressly declared not to be a public forum.

VI. CYBERSECURITY

Each user of SCDA IT systems and assets bears responsibility for the overall security of SCDA systems in the respect that they are expected to act in a manner with the intent to prevent cybercriminals from gaining access to SCDA data and systems, and to report any activity that may indicate attempts by cybercriminals to access SCDA data or systems (i.e. phishing emails, vishing calls, etc.). To this end, SCDA requires all users to participate in monthly cybersecurity training. Users should be aware that SCDA conducts periodic tests to evaluate the risk of our systems. If a user falls prey to one of these tests, they may be assigned remedial training to complete.

Furthermore, each computer, mobile phone, and mobile device in the SCDA network relies upon periodic network connection to receive patches and updates to software and security. Users are responsible for ensuring that their devices are properly connecting to the network to receive these updates.

VII. ACQUISITION OF IT EQUIPMENT

IT assets (i.e. computers, printers tablets, phones, peripherals, etc.) should either be requested through the IT department or approved by the IT department **prior to purchase**. This will help ensure that all SCDA equipment is safe, secure, and compatible with other network assets.

VIII. ONBOARDING

All incoming staff at SCDA must complete prescribed system access and cybersecurity before being given log on credentials.