LOUISIANA STATE UNIVERSITY AGRICULTURAL CENTER

AG CENTER PS-47

Effective Date: July 18, 2006 Version: 0

USE OF AGCENTER INFORMATION TECHNOLOGY RESOURCES

The AgCenter provides as part of its technology platform an electronic mail system, internet access, and access to various other information technology resources for use by employees in order to enhance the timeliness, quality and performance of their work. These tools are provided to employees for the accomplishment of their work as AgCenter employees.

Appropriate Use

Use of information technology resources, including but not limited to email and internet access, is governed by Louisiana Revised Statutes and the Regulations of the LSU Board of Supervisors (Sections 5-8 and 5-9). These laws and regulations prohibit use of AgCenter resources for non-business reasons. Further, any activity or purpose that is in conflict with any AgCenter policy or procedures, such as the Sexual Harassment, EEO, or Violence-Free Workplace policy, is considered a violation of policy. Further, employees may not transmit personal comments or statements or post information to newsgroups or Usenet that may be mistaken as the position of the AgCenter.

The most serious violations of policy include use for any illegal activity or purpose; access to pornographic information; use of AgCenter property for an employee's outside employment or other personal activities/businesses, including personal farms, conducted for personal gain; and usage that is threatening or intimidating. As is the case with other forms of communication (telephone, written, meetings, etc.), employees are expected to use electronic forms of communication in a manner that is professional and is not demeaning, offensive, or disruptive. As a condition for access to and use the AgCenter information technology resources, each user is personally responsible for ensuring that each and all of these guidelines are followed.

Appendices to this document, which will be updated periodically, contain further specifics regarding acceptable and unacceptable uses along with best practices and recommendations for the most effective use of IT resources.

Privacy

All computers and the data stored on them, including but not limited to email messages, databases, documents and spreadsheets, are and remain at all times the property of the AgCenter. All user network accounts and mailboxes require private passwords although this does not guarantee data privacy, nor should privacy be expected by anyone. The AgCenter reserves the right to retrieve and read any message stored, composed, sent or received; and to reset passwords and access user data at the discretion of management. An employee's use of AgCenter information technology resources constitutes the employee's consent to the AgCenter's access to, and waiver of the employee's privacy interest in, all data on the system. While the AgCenter does not monitor email and internet access as a routine matter, the AgCenter reserves the right to access and disclose this information in its sole discretion and/or for any business purpose.

Additionally, federal regulations such as the Gramm-Leach-Bliley Act and HIPPA impose restrictions on the access and dissemination of AgCenter data. AgCenter personnel with access to AgCenter data must be familiar with data privacy concerns and act accordingly when utilizing this data. As examples, AgCenter personnel with access to confidential data may only use the data in the manner for which intended, may not share the data with others not authorized to have access to the data, and must maintain the data in a manner appropriate to the level of confidentiality required.

Responsibility

It is each individual user's responsibility to maintain the integrity of their network IDs and passwords. An individual's ID and password is their "key" to the system as well as their "signature" when accessing AgCenter resources. Proper protection of passwords and access to computers, laptops, cell phones and handheld devices is the responsibility of each employee. Additionally, it is the responsibility of each employee to ensure that they are operating with valid software licenses and that their machine is properly patched and protected with updated virus software. Employees may not obtain or use another's logonid or password, or otherwise access computer resources for which authorization has not been validly given. Employees also may not copy, impair or remove any software located on any computer resource or install any software on any computer resource that unreasonably impairs the function, operation and/or efficiency of any computing resources. Finally, employees learning of any misuse of AgCenter systems by any user or other individual or violations of this Policy are required to notify their Unit Head and/or HR. Guidelines accompany this policy in order to give further clarification with respect to requirements and user responsibility in this area.

Only certain people within the AgCenter are authorized to access another individual's computer, electronic media, electronic communications, or other electronic resources without the employee's permission. These individuals are the unit head, a person authorized by the unit head or higher level line administrator, and computer personnel in the course and scope of their responsibilities solely for the purpose of maintaining computers.

Violations

AgCenter employees who participate in inappropriate and/or unauthorized use of AgCenter information technology resources or are otherwise in violation of this policy shall be subject to discipline as appropriate under the circumstances up to and including termination.

Appendix A – Email Usage

Mandatory Requirements

- Email messages should be limited to the conduct of AgCenter business and/or AgCenter sponsored activities.
- Email may not be used for: illegal activity; activity that is in conflict with any AgCenter policy or procedure; activities related to a personal business or for personal gain.
- Email messages shall not contain content that may be reasonably considered demeaning, offensive or disruptive to any employee. Demeaning, offensive or disruptive content would include, but would not be limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of his or her age, sexual orientation, religious or political beliefs, national origin, or disability. Employees should also refrain from using vulgarities, obscenities, sarcasm or exaggeration in e-mail messages.
- All employees must use updated virus software and exercise caution when downloading files.

Guidelines

Email has quickly become one of the most important methods of communicating with each other and with our colleagues and constituents. The following guidelines are not intended to discourage your use of email, but rather to ensure that email is used responsibly, appropriately and with discretion.

You should never consider your electronic communications to be either private or secure. Email may be stored indefinitely on any number of computers, including that of the recipient. Copies of your messages may be forwarded to others either electronically or on paper. In addition, email sent to nonexistent or incorrect user names may be delivered to persons other than the intended recipient.

THINK before sending a message. It is very important that you use the same care and discretion in drafting email as you would for any other written communication. Anything created or stored in the computer may be reviewed by others. Before sending a message, ask yourself the following question: Would I want a judge or jury to see this message?

Do not forward or initiate chain or mass e-mail. Chain or mass email is a message sent to a number of people asking each recipient to send copies with the same message to a specified number of others. Employees should delete all chain email and all non-business related email immediately upon receipt and refrain from forwarding them to any other employees.

E-Mail Retention

Our email system is a key component of being able to conduct business across the state and with all of our colleagues and peers. As such, it is backed up daily and plans are in place for being able to restore the system in the event of failure. This means, also, that backups can be used to retrieve even deleted emails. Backups are maintained for approximately one month, so emails that are deleted would still be on backup systems for another month after deletion. Also, it is important to note that when deleting an email, it goes into your “Deleted” folder which is also backed up. If you do not have your “Deleted” folder set to permanently remove items after a set amount of time, then emails you delete are maintained indefinitely in your “Deleted” folder as well as in the backups.

In a similar vein, emails that you send or forward are also stored in your “Sent” folder. If you forward a message and then delete it, a copy will be in your “Deleted” folder as well as your “Sent” folder. Until the message is deleted from both the “Deleted” folder and the “Sent” folder, it will remain active in the email system.

Finally, many email users use personal email folders and local archive files to maintain old emails for reference purposes. Please be aware that these are considered “official” business documents and can be subpoenaed in any investigations or suits that the AgCenter may be a part of. Please keep this in mind when deciding whether or not to keep any particular email correspondence.

E-Mail Best Practices for Senders

- Do not use email to discuss or solve a sensitive personnel or work-place issue. For those issues and other issues of a complex nature, a phone conversation will have far better results. However, an email follow-up to the phone conversation is often appropriate.
- Avoid emotional overtones or content in your email.
- Avoid sending email that may contain controversial subject matters, once again, a phone call may be more appropriate and secure.
- Be succinct. The most effective email messages are short and to the point.
- Keep the message focused on a single topic.
- Include a subject line that captures the content of the message. This helps recipients prioritize, file and search for messages.
- Tag messages appropriately — do not label messages “High Priority” or “Urgent” unless they really are.
- Do not modify someone else’s message.
- Do not forward someone else’s message without permission.
- Do not **“reply to all”** unless **“all”** need to see your reply.
- Choose the number and size of file attachments with great care. Compress attachments whenever possible.
- Address email according to the expected action—list people in the “To” field if they should respond, and in the “CC” if they should read the message as information only.
- Avoid long dialogues and threads via email. The duration of the thread, too many topics and too many people copied can lead to confusion, and tax the system’s resources. If an email thread is getting long, it may indicate time for an in-person conversation.
- Consider message format because the recipient’s email system may not display the message as intended by the sender. Do not depend on alignments, fonts or colors to make a point.
- Broadcast emails addressed to large groups should be in support of AgCenter business, be used only where large groups of people would have an interest, and where targeting individual addresses would be too labor intensive or prone to error. Such broadcasts should only be made selectively and rarely.
- User mailboxes are not to be used for long-term storage. Retention should be for current topics and message threads. A good rule of thumb is to delete messages more than 90 days old.
- Users can employ a local .PST file to archive important messages.
- E-mail should not be used to move large files among work groups.
- Sensitive information should not be routed through public networks, such as the Internet.
- To avoid proliferation of junk mail, users of the AgCenter’s e-mail system should not reply to junk e-mail or give their e-mail address in Internet chat rooms or discussion groups. Delete all junk mail (spam). Do not respond and ask to be removed from the sender’s list as this often results in additional junk mail (spam).

Appendix B – Internet Usage
Mandatory Requirements

- Accessing information or services on the Internet should be limited to AgCenter business and/or AgCenter-sponsored activities.
- Access to the Internet may not be used for: illegal activities; use for private or personal gain; activities that are in conflict with any AgCenter policy or procedure; access to pornographic and/or other inappropriate materials and/or information.
- Internet access cannot be used for downloading any copyrighted content that has not been appropriately paid for and/or permission granted for its use.

Guidelines

Access to the Internet is made available to employees in order to enhance their productivity in job-related activities. With the proliferation of information and systems available via the internet, many of the AgCenter's employees find themselves using the Internet frequently and many times on unfamiliar sites. The following guidelines will help to keep your machine secure as well as protect you from scams, spyware, viruses and spam.

- Use a browser toolbar that blocks pop-up ads. If you do get pop-up ads, do not click through.
- Create a user account on a “free” site, such as Hotmail. Whenever prompted to enter an email ID that is strictly for registering on a site, use the “free” email ID. This will help to limit your susceptibility to spam.
- When downloading content from the Internet, save it to a local drive and then scan it for viruses. Do not “open” or “execute” the item directly from the website.
- Download and use a spyware tool such as Spybot or Adaware.

Appendix C – Passwords
Mandatory Requirements

- Passwords must be changed every 90 days.
- Passwords cannot be repeated.
- Passwords must be at least 6 characters long and include at least one non-alphabetic character and at least one capital letter.
- Each employee will have his/her own unique network and email ID which is not to be shared. Employees are never to share their passwords with others.
- Employees must utilize a password-protected screensaver.

Guidelines

Passwords are an employee's "keys" to the AgCenter systems. It is vital that they are protected in an appropriate fashion. The following guidelines will help to ensure security while easing the burden of remembering complex passwords.

- Utilize a phrase instead of a word. For example, "We the people of the United States" could be represented by "Wtp0tUS". This password is very difficult to guess but very easy to remember.
- Do not write down passwords and keep them by your computer.

Appendix D – Software Licensing
Mandatory Requirements

- Employees of the AgCenter do not have the right to reproduce software.
- All software being utilized on AgCenter systems must be properly licensed. Documentation for this license is the responsibility of the department for individual computers and of IT for network software.
- AgCenter employees who become aware of misuse of computer software and/or related documentation must notify their supervisor and IT.