University of Arkansas System Division of Agriculture
Computer and Network Use Policy

Summary: Establishes policy governing use of Division of Agriculture computer and network resources.

(1) The Division of Agriculture (Division) encourages the use of computers and electronic communications to enhance efficiency and productivity and to allow the sharing of information and knowledge in support of the Division's missions of research, extension, and education. To this end, the Division provides and supports IT resources which it owns. The Division expects that all users of its information technology shall do so in a responsible and ethical manner while abiding by all applicable laws, policies, and regulations. The purpose of this policy is to establish practices for the Division in order to maintain its network and computer systems in a manner that supports its missions while also complying with legal, policy, and contractual obligations.

(2) This policy applies to all Division IT resources, whether individually/departmentally controlled, shared, stand-alone, or networked. It applies to all computers and communication facilities owned, leased, operated, or otherwise provided by the Division or connected to Division IT resources. These include, but are not limited to: networking devices, tablets, telephones, wireless devices, computers, workstations, and any associated peripherals and software, whether used for administration, research, extension, education, or other purposes.

(3) This policy is intended to co-exist with computer use policies that may be in place for the various campuses at which Division faculty may be located/associated. As such, the policies herein shall be controlling unless specifically in conflict with a policy of such campus. In such cases, the applicability of the correct policy shall be decided by the appropriate Associate Vice President or their designees.

(4) In cases where Division-owned computers, phones, and other devices have been issued, the Division discourages storing, processing, or transmitting Division information using personally owned devices.

(5) Maintaining access to Division IT resources is necessary for maintenance of computers, networks, data, and storage systems; to maintain the integrity of the computers, networks, and storage systems; and/or to protect the rights and property of the Division and its users. Authorized personnel may use management tools to routinely monitor and log hardware/software inventory information, usage data such as network session connection times, CPU and disk utilization for each user, security audit trails, and network loading. In all maintenance cases, the privacy rights of users shall be protected to the greatest extent possible.

(6) "Users" include but are not limited to staff, faculty, students, contractors/subcontractors, visiting scholars, media representatives, guest speakers, and non-Division entities granted access. All such allowable users should be provided, familiar with, and comply with this policy.

(7) The Division has the responsibility to administer, protect, and maintain its computers, software, and networks. The purposes of the Division's information technology management are to:

(a) Manage computing resources so that members of the Division community benefit equitably from their use.
(b) Protect Division computers, networks, and information from destruction, tampering, and unauthorized inspection and use.
(c) Communicate Division policies and the responsibilities of individuals systematically and regularly in a variety of formats to all parts of the Division community.
(d) Establish and support security standards for electronic information that community members produce, use, or distribute.
(e) Monitor policies and propose changes in policy as events or technology warrant.
(f) Maintain and manage software licenses.
(g) Track hardware as needed

(8) Programs should not be installed or run on any of the Division's computers without prior approval by the appropriate Division IT department.

(9) Division computers are required to use anti-virus software with current virus profiles. Virus scans should be run on a regular basis.

(10) All computers are required to have an automatic password protected screen saver set to a maximum of 20 minutes except for instances where the computer is located in a secure location or when the computer is used for research or monitoring in which such protection could hinder the operation. In these instances, alternative security controls may be necessary to ensure adequate protection.

(11) Personnel connecting to networks outside the Division local area networks must conform to the acceptable use policies governing those connecting networks.

(12) Disability accessibility – all computer and communications devices used for academic and administrative tasks of the Division shall be accessible to allowable users with disabilities in compliance with law and these policies. The Division shall make all reasonable accommodations including providing assistive technology, technical assistance, and necessary training.

(13) Restrictions: Division's IT resources may not be used for:

(a) Unlawful activity
(b) Violation of Division or Board of Trustee policy
(c) Commercial purposes or personal gain not approved by the Division (see PMGS-95-3)
(d) Breach of confidentiality
(e) Unauthorized access to or use of IT resources
(f) Use of false identity (except in cases where an employee is instructed by a supervisor to use the supervisor's identity to conduct Division business)
(g) Copyright and license infringement
(h) Sexual and other forms of harassment
(i) Dissemination, hosting, and/or posting of child pornography or obscene material

(j) Initiating a denial-of-service attack or releasing a virus, worm, spyware, or malware
(k) Fraud, phishing, or spamming
(l) Improper use of the Division name or logo
(m) Intentionally seeking information on, obtaining copies of, or making modifications to data, applications or passwords belonging to other users

(14) Personal use – users of Division IT resources may use these resources for incidental personal purposes provided that, in addition to the constraints and conditions herein, such use does not:

(a) Interfere with the Division's operation of IT resources, or
(b) Interfere with the user's employment or other obligations to the Division, or
(c) Burden the Division with noticeable incremental costs. The Division is not responsible for any loss or damage incurred by an individual as a result of personal use of Division IT resources.

At no time shall the Division or any Division personnel be responsible for loss, damage, or retrieval of personal data stored on Division equipment or for any loss or damage incurred by the user as a result of personal use of the Division's IT resources.

(15) Where available, the IT management unit(s) shall provide users with designated storage areas for work-related data/information. These areas will be defined and clearly communicated in writing to the user. IT management unit(s) will regularly back-up these storage areas. Users must store all work-related data/information necessary to fulfill contractual obligations in these defined areas. Data/information stored in places other than these defined areas are at risk of loss. However, personal data and other information should be stored elsewhere. Where designated centrally managed storage areas are not available, users are responsible for properly backing-up work related data/information necessary to fulfill contractual obligations. In these instances, IT management unit(s) will assist users in securing and utilizing appropriate storage mechanisms.

(16) AES-supported computers will generally be set up with non-administrative user account access. In rare instances, a user may have a need for administrative account access to a computer. In those instances, an account may be requested using form PMGS 14-1-1. This request shall explain the nature of the need and requires the approval of the supervisor, the unit head, and the appropriate Associate Vice President. In cases where an administrative access account is issued, the user must use that account only in those specific instances where administrative access is required and not as their routine logon account. Additionally, the user must notify the IT management unit if any addition/deletion/modification to software/hardware is performed. Failure to comply with these policies will result in revocation of the administrative access account.

(17) The Division desires to provide the highest level of privacy possible to its users. Privacy, however, cannot be guaranteed. In addition, privacy and confidentiality must be balanced with the need for the Division to manage and maintain networks and systems against improper use and misconduct.

(18) The general right to privacy is extended to the electronic environment to the extent possible. Privacy is mitigated by the Arkansas Freedom of Information Act, necessary computer system

administration, required audits, and other exceptions noted herein. Contents of electronic files will be examined or disclosed only when authorized by their users, or in an emergency situation or as approved by an appropriate Division official under provisions as noted herein, or as required by law.

(a) The Division may preserve, access, or disclose information without the users consent in the following instances:

(1) Required by or consistent with law.
(2) There is a substantiated reason to believe that violations of law or policy have occurred.
(3) There are compelling circumstances in which failure to act may result in significant bodily harm, irreplaceable property loss or damage, loss of significant evidence, or the loss of critical data.
(4) Time-dependent, critical operations, programs, or projects are threatened.

(b) In cases where prior consent is not obtained (except in the cases of subpoenas, search warrants, or extreme emergency), a request must be made in writing and prior written authorization must be received from the Vice President for Agriculture or the appropriate Associate Vice Presidents or their specified designees. In cases of extreme emergency when circumstances are such that time is of the essence and any delay for prior authorization will result in a high probability of critical harm or loss, a full report as soon as practicable must be provided to the Vice President for Agriculture or the appropriate Associate Vice Presidents or their specified designees following any access or retrieval of data or equipment. In any event, such emergency action must include the least invasive action necessary to resolve the emergency situation.

(c) After all such actions authorized above, the responsible authority or designee shall at the earliest opportunity that is lawful and consistent with Board of Trustee or Division policy notify the affected user of the actions taken and the reason.

(d) Recognized limits to the general right of privacy are:

(1) Information requests – Division employees shall comply with Division requests for public information in their possession and shall comply with all Freedom of Information requests for which a specific exception is not applicable.
(2) Necessary system reliability, maintenance, and security monitoring – the least invasive degree of inspection required to perform this necessary work shall be performed. In the performance of this necessary work, authorized Division personnel shall not intentionally search communications and information for violations of law or policy. However, if in the regular course of their duties Division personnel inadvertently discover or suspect improper activity, such personnel must report such findings to the proper authorities.
(3) Back-up services – both mandatory and suggested back-up services shall be provided as noted herein. In addition to notification as provided in (15) above, users shall be provided information on such services upon request.

(19) All information gathered by the Division personnel under procedures and authorizations noted herein is restricted to official Division use.

(20) The Division reserves the right to deny use of its IT resources when necessary to satisfy these restrictions and constraints noted herein.

(21) This Policy does not address the ownership of intellectual property stored on or transmitted through Division IT resources. Ownership of intellectual property is governed by law, Board of Trustees policy, and/or Division policy. The contents of all electronic communications or data storage shall conform to laws and applicable Division policies regarding protection of intellectual property, including laws and policies regarding copyright, patents, and trademarks.

(22) In the event of termination, a user's access to his/her computer, network, system access, and/or e-mail accounts shall be immediately terminated (except in cases where continuance is allowed by other policy or written agreement). Personal data not part of an investigation or governmental action may be retrieved at the convenience of the Division.

(23) Violations of any part of this policy will be addressed through appropriate disciplinary actions based upon the severity of the infraction and may include, but are not limited to, suspension of network account, removal of computer equipment, probation, and/or termination of employment.

PMGS 14-1-1
Administrative Rights Agreement - Division of Agriculture

1.0 Overview
This Administrative Rights Service Level Agreement (SLA) is between the University of Arkansas System Division of Agriculture and the faculty and staff using an administrative account on an AES-supported computer. If administrative rights are required, unit head approval and business justification must be presented prior to approval.

2.0 Administrative Rights Use
You are to use the administrative account only when installing or updating software or hardware. Use your primary account at all other times. Your administrative account details should not be shared with anyone.

The administrative account should only be used if the request cannot be fulfilled using normal operating procedures. The IT Group is available on campus from 8am to 5pm, Monday through Friday.

The Division of Agriculture IT Group must be notified within 48 hours of any software installed or reconfigured using your administrator account. An email (agritech@uark.edu) or ticket (agritechhelp.uark.edu) to the helpdesk identifying the software or hardware installed or reconfigured and attaching proof of license (if applicable) is mandatory. Proof can be a license certificate, paid invoice, or other official document.

3.0 Accepted Risk
When logged in with Administrative rights, the computer is increasingly susceptible to viruses since the virus can have full control of the computer. The IT Group is not responsible for data loss, viruses, or system corruption due to the granting of administrative rights.

4.0 Cancellation/Termination
Violation of this agreement may result in revocation of your administrative account privileges. Examples include but are not limited to:

- The account is used in an abusive manner
- There is cause to believe that you are not complying with Division of Agriculture policies, or state or federal law or regulations
- Your computer becomes infected by a virus while using the administrative account
- Software or hardware is installed or reconfigured on your computer without the required subsequent notification and/or license verification

_____ _____ _____
Employee Name (print) E-mail Address Phone

Justification: _____

_____

Computer Description and Location: _____

Serial Number and/or Service Tag number (Required): _____

_____ Date: _____
Employee Signature

_____ Date: _____
Supervisor Approval (please sign and print)

_____ Date: _____
Unit Head Approval (please sign and print)

_____ Date: _____
Associate VP Approval