UADA Policy 910.1
Division Acceptable Use Policy

Purpose

Establish the Acceptable Use of Computers and Networks Policy for the University of Arkansas System Division of Agriculture (UADA). UADA expects that all users of its information technology resources 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 UADA to maintain its network and computer systems in a manner that supports its missions while also complying with legal, policy, and contractual obligations. This includes appropriate use and procedures for use of official email, use of non-UADA assets to further UADA business as well as UADA owned resources. Furthermore, this policy is designed to prevent viruses, malware, or malicious code from infecting the University of Arkansas Systems, Division of Agriculture (UADA) computing devices and networks.

Scope

This policy applies to all UADA 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 UADA or connected to UADA 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. This policy applies to all computers that are connected to the UADA network via a standard network connection, wireless connection, or virtual private network connection. This includes both UADA-owned computers and personally owned computers attached to the UADA network. UADA discourages storing, processing, or transmitting UADA information using personally owned computers that are connected to UADA resources. This policy is intended to co-exist with computer use policies that may be in place for the various campuses at which UADA faculty may be located/associated. As such, the policies herein shall be the controlling policy 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 Senior Associate Vice President or their designees.

Definitions

Authentication: The process of verifying that someone who holds an account on an IT system is who they purport to be.

Confidential Data: Data for which restrictions on the accessibility and dissemination of information are in effect. This includes information whose improper use or disclosure could adversely affect the ability of the institution to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), Health Insurance Portability and Accountability Act (HIPAA), PCI standards.

Devices: Devices include smartphones, tablets, laptops, desktops, and mobile storage devices such as USB drives, external hard drives, etc.

DIT: The employee with the title of Director of Information Technology (AES or CES).

High-Risk Data: Data assets that are classified as being of high risk as defined in UADA Administrative Policy, *Information Security: Data Classification and Protection*.

Information Resources: UADA information and related resources, such as equipment, devices, software, and other information technology.

Information System: A major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

Level of Assurance: The degree of confidence that someone who holds an account on an IT system is whom they purport to be.

Low-Risk Data: Data assets that are classified as being of low risk as defined in UADA Administrative Policy, *Information Security: Data Classification and Protection*.

Moderate Risk Data: Data assets that are classified as being of moderate risk as defined in UADA Administrative Policy, *Information Security: Data Classification and Protection*.

Multi-Factor Authentication: Multiple forms of authentication are used to increase the likelihood that the login credentials are from the individual to whom they were assigned. The types of credentials typically fall into three categories: something you know, such as a PIN or password; something you have, such as a one-time passcode generator, token, or smart card; or something you are, such as a fingerprint or other biometric.

Personal Device Use: Refers to employees taking their own personal device to work, whether laptop, smartphone, or tablet, to interface with the internal/participant organization's network resources. This also refers to mobile storage devices such as USB drives, external hard drives, etc.

Public Data: Data elements that have no access restrictions and are available to the public. This data can also be designated as unrestricted data.

Prior Approval: A process by which all users must gain approval prior to working with, utilizing, or implementing a process or procedure.

Sensitive Data: Data for which users must obtain specific authorization to access, since the data's unauthorized disclosure, alteration, or destruction will cause perceivable damage to the participant organization. Examples: personally identifiable information, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) PCI standards.

Use: Use includes accessing, inputting, processing, storing, backing up, or relocating any UADA or client-specific data, as well as, connecting to a network.: Individual or group that interacts with a system or benefits from a system during its utilization. Users include but are not limited to staff, faculty, students,

contractors/subcontractors, visiting scholars, media representatives, guest speakers, and non-UADA entities granted access. All such "users" are required to be familiar with and comply with this policy.

Computers and Networks

Maintaining access to UADA IT resources is necessary for the 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 UADA 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.

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

1) Manage computing resources so that members of the UADA community benefit equitably from their use.
2) Protect UADA computers, networks, and information from destruction, tampering, and unauthorized inspection and use.
3) Communicate UADA policies and the responsibilities of individuals systematically and regularly in a variety of formats to all parts of the UADA community.
4) Establish and support security standards for electronic information that community members produce, use, or distribute.
5) Monitor policies and propose changes in policy as events or technology warrant.
6) Maintain and manage software licenses.
7) Track hardware as needed.

Unapproved (and unlicensed) software is not to be installed or run on any of UADA's computers without prior approval by the appropriate UADA IT department. UADA computers are required to use anti-virus software with current virus profiles. Virus scans should be run on a regular basis.

All computers will have an automatic password-protected screen saver set to a maximum of 15 minutes except for instances where the computer is 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. Contact UADA IT for an exception. Respect for privacy is required. Users shall not intentionally seek out information on, obtain copies of, or make modifications to data, applications, or passwords belonging to other users.

Personnel connecting to networks outside the UADA local area networks must conform to the acceptable use policies governing those connecting networks.

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

UADA's IT resources may not be used for:

- Unlawful activity
- Violation of UADA or Board of Trustee policies
- Commercial purposes or personal gain not approved by the UADA (see PMGS-95-3)
- Breach of confidentiality
- Unauthorized access to or use of IT resources
- Use of false identity (except in cases where an employee is instructed by a supervisor to use the supervisor's identity to conduct UADA business)
- Copyright and license infringement
- Sexual and other forms of harassment
- Dissemination, hosting, and/or posting of child pornography or obscene material
- Initiating a denial-of-service attack or releasing a virus, worm, spyware, or malware
- Fraud, phishing, or spamming
- Improper use of the UADA name or logo
- Intentionally seeking information on, obtaining copies of, or making modifications to data, applications, or passwords belonging to other users

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. 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 is 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.

UADA computers will be set up with non-administrative user account access. In rare instances, a user may need administrative account access to a computer. In those instances, an account may be requested using these request forms: AES or CES. (Attachment 1) This request shall explain the nature of the need and requires the approval of the supervisor, the unit head, and the appropriate Senior 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 login 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 the revocation of the administrative access account.

Personal use by users of UADA IT resources is allowable for incidental personal purposes provided that, in addition to the constraints and conditions herein, such use does not interfere with UADA's operation of IT resources, the user's employment or other obligations to UADA, burden UADA with noticeable incremental costs. While incidental and occasional personal use of such systems is permissible, personal communications and data transmitted or stored on UADA information technology resources are treated as business communications. Company electronic resources exist for business purposes; therefore, all content contained therein belongs to the organization and is accessible at any time by the organization. In the event of termination, an employee's access to his/her computer, network and system access, e-mail accounts, and any

personal material within these accounts is immediately terminated. Storage of non-work-related data and information on UADA equipment is discouraged. Please note that UADA is not responsible for any loss or damage incurred by an individual as a result of the personal use of UADA IT resources.

UADA 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 UADA to manage and maintain networks and systems against improper use and misconduct. The general right to privacy is extended to the electronic environment to the extent possible under the law and in the interest of the University and UADA. 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 UADA official under provisions as noted herein, or as required by law. The UADA may preserve, access, or disclose information without the user's consent in the following instances:

1) Required by or consistent with the 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.

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

Recognized limits to the general right of privacy are:

1) Information requests – UADA employees shall comply with UADA 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 UADA personnel shall not intentionally search communications and information for violations of law or policy. However, if, in the regular course of their duties, UADA 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. Users shall be provided with information on such services upon request.

All information gathered by UADA personnel under procedures and authorizations noted herein is restricted to official UADA use.

UADA reserves the right to deny the use of its IT resources when necessary to satisfy these restrictions and constraints noted herein. 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 UADA.

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

Use of personal devices

In the instances in which use of an employee's personal device is required or permitted under UADA policy, the employee will take the following actions to ensure the security of the device and any data contained on the device.

1) Employees and authorized users must appropriately secure the device to prevent data from being lost or compromised, reduce the risk of spreading viruses, and mitigate other forms of abuse to UADA computing infrastructure by following security guidelines. The user should at minimum employ some sort of device access protection such as, but not limited to, strong passcode, facial recognition, card swipe, fingerprint, etc.; set an idle timeout that will automatically lock the device if misplaced; keep the device's software (operating, anti-virus, security, encryption, etc.) up to date and enroll your device in "Find my phone" or similar services and/or label your device with some identifying information (work or home phone number, name, and or UADA address) to make the device easy to return if lost or stolen(this may be done via your locked screen).
2) Users should report immediately to your manager any incident or suspected incidents of unauthorized data access, data, or device loss, and/or disclosure of system or participant organization resources as it relates to personally owned devices. Managers will immediately report such incidents to the DIT.
3) At the time that use of the personally owned device for UADA business is no longer required the employee will provide documentation to their manager acknowledging and confirming that the device does not contain any UADA sensitive data.

Sensitive and private data must not be stored on these devices or on external cloud-based personal accounts, such as Box or OneDrive. At no time shall UADA or any UADA personnel be responsible for loss, damage, or retrieval of personal data stored on UADA equipment or for any loss or damage incurred by the user as a result of personal use of UADA's IT resources.

Employees who utilize their personal devices for UADA business purposes accept all risks and liabilities associated with that use to include, but not limited to, those described in this policy. UADA is not responsible nor does it accept liability for the maintenance, backup, or loss of data stored on an employee's personal device. It is the responsibility of the individual owner to back up all software and data to other appropriate backup storage systems. UADA shall NOT be liable for the loss, theft, or damage of any employee's personal

devices. This includes, but is not limited to, when the device is being used for UADA business, on UADA work time, or during business travel. UADA provides security for the UADA network and at no time does UADA accept liability for the security of an employee's personal device. An employee's personal device may be subject to the search and review as a result of a Freedom of Information Act (FOIA) request and/or subpoena associated with litigation involving UADA. UADA may, without notification, prevent or ban any mobile device which disrupts the UADA network or is used in a manner that violates any UADA policies.

Anti-Virus and Anti-Spyware Management

All computers attached to the UADA network must have anti-virus software installed with current virus definitions. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers. Any activities with the intention to create and/or distribute malicious programs onto the UADA network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited. No student, faculty, staff, or guest should attempt to destroy or remove a virus, or any evidence of that virus, without direction from UADA. Any virus-infected computer will be removed from the network and remain off the UADA network until it is verified as virus-free by UADA.

Department and Individual Responsibilities. The following activities are the responsibility of UADA departments and employees:

1) Departments must ensure that all departmentally managed computers have virus protection that is in keeping with the standards set out in this policy.
2) Departments that allow employees to use personally owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.
3) All employees and students are responsible for taking reasonable measures to protect against virus infection.
4) Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the UADA network without the express consent of the IT department.

Electronic Mail (Email) and Messaging

These policies are applicable to all users (departments, organizations, individuals) of any UADA e-mail system. Users are expected to comply with all applicable laws and university policies affecting the use of e-mail and related systems, including but not limited to responsible use, computer accounts, passwords, information security, and software licensing. The organization reserves the right to limit the size of individual mail messages being transmitted through UADA resources. Additionally, UADA reserves the right to send e-mails to its users.

UADA specifically prohibits the following uses/activities by its employees with respect to the use of UADA's email and messaging system. UADA reserves the right to prohibit additional activities if they have effect of violating laws or other System or UADA policies or result in overburdening the UADA network. Users shall not:

1) Alter electronic communications to hide one's identity or to impersonate another individual is considered misrepresentation and/or forgery and is prohibited under this policy. All e-mails, news posts, chat sessions, or any other form of electronic communication must contain the sender's real name and/or e-mail address. The only exception is with an alias or shared accounts that have been assigned to a user.

2) Initiate or forward "chain letters" or e-mail are prohibited on university e-mail systems and the Internet as a whole. Chain e-mail can be identified by phrases such as "please pass this on to your friends" or similar inducements that encourage the recipient to forward the message.
3) Engage in bombarding someone with a large volume of unsolicited mail to disrupt them or their site is known as "mail bombing." Mail bombs have the effect of seriously degrading system performance and may have legal consequences. This practice is strictly prohibited on UADA systems.
4) Send unsolicited commercial advertisements or solicitations (SPAM) via e-mail is regulated by applicable laws.
    i) Users found in violation of these laws could be subject to criminal prosecution, civil prosecution, administrative action, and/or loss of some or all computing privileges.
    ii) UADA users receiving such messages are responsible for notifying the sender to stop. If the sender refuses to comply or does not provide a valid means for users to be removed from their list, the recipient may take civil action against them.
5) Use electronic communications, including e-mail, to annoy, harass and/or physically threaten other individuals is prohibited.
6) Use State resources, including e-mail, for one's personal or political gain. This includes promoting off-campus sales and services.
7) Operate unofficial e-mail reflectors. An e-mail reflector is automated or otherwise forwarding a mail message to multiple recipients triggered by the content or headers of the mail message being forwarded. Authorized reflectors include uada.edu and reflectors established by the system administrators of the UADA machines affected.
8) Sending messages to large numbers of users except as defined in the procedures accompanying this policy. Official mailings to large numbers of users should conform to the "Large Mailings and Broadcast Messages" section of this policy.
9) E-mail messages that include any person's (users, other users or clients) personal identification numbers (e.g., social security number, driver license, etc.).

The preferred e-mail signature will resemble the UADA business cards and include the UADA mission statement or a link to the mission statement. The following items are permitted in the e-mail signature:

- UADA Logo, Business Card Layout, Employee's Name, Job Title, Address, Office Location, Phone Numbers, E-Mail Address, UADA Social Media Icons and/or links for UADA (homepage, portal, blow, twitter, etc.), and UADA Mission Statement.
- Signature may include all the above items or any portion. No other items including pictures and quotations are permitted in the signature.

All UADA employees will not use quotations (no matter how innocent they may seem) that are personal, political, religious, racist, jokes, or other viewpoints that might be considered offensive by other individuals. Signatures should look professional and represent the UADA and the University of Arkansas System, not personal viewpoints.

Large group mailings are permitted only if sent via authorized distribution methods to reduce the system load.

1) Mailings exceeding the number of addressees specified in the procedures must use system aliases, public distribution lists (PDLs), or a system-operated utility. This applies to all inter-machine e-mail as

well as organization-wide e-mail systems. Examples of system aliases and PDLs include department lists, location lists, committees, clubs, other official UADA organizations, and specific discussion/topic groups.

2) System aliases and PDLs are to be used only for the purpose for which they were created. All other aliases are for use by specific units or members to disseminate or share information. The use of such aliases by non-authorized personnel constitutes a violation of this policy. Official aliases may not be used to broadcast unofficial and/or unauthorized messages. Aliases established to broadcast information may not be used without the express permission of the owner of the list.
3) For other large group mailings, the use of system-authorized distribution methods is encouraged, especially when extremely large numbers of users are involved or when the speed with which the message is being delivered is not critical. Messages being "broadcast" to organization-wide groups (e.g., all faculty, staff, and/or students) must use an approved broadcast method and meet the following criteria:
    a. Other means of communication are not timely, and the nature of the event was such that timely announcement via other methods could not be accommodated.
    b. An appropriate target audience can be determined.
    c. Could be of significant benefit to all the targeted audience.
    d. Must comply with applicable UADA policies on the use of state resources.
    e. Prevents significant inconvenience that the lack of information would cause to the targeted audience.
4) Broadcast messages should originate from a departmental or unit account, e.g., human resources, rather than an individual or personal account.
5) The organization reserves the right to perform broadcast mailings that are related to emergencies and facilities conditions or activities for which urgent notice is required and that will potentially affect most of the recipients.

E-mail should be avoided as a means of communicating confidential or sensitive material since confidentiality cannot be guaranteed on the Internet. It is against UADA policy for system administrators to monitor the contents of files or messages unless necessary to preserve either system integrity or continued e-mail delivery. Moreover, copies of messages are kept on system backups and may be retained for periods of time and locations unknown to you. In addition, e-mail messages can be intercepted, copied, read, forged, destroyed, or misused by others for mischievous purposes.

E-mail, whether created or stored on UADA equipment or not, may constitute an organization record subject to disclosure under the Freedom of Information Act or other laws, or because of litigation. This includes email-related data stored on a machine's hard drive, regardless of machine ownership. Copies of the e-mail must be provided in response to a public record request or legally issued subpoena, subject to very limited exceptions, as with all other documents created and retained at the organization.

Authentication

UADA is committed to a secure information technology environment in support of its mission. This policy is designed to help ensure strong and consistent authentication standards throughout the computing

environments of the organization. Authentication methods for medium and high-risk data shall meet the standards outlined in the *Information Security: Authentication Procedures.*

Access to view low-risk data does not require authentication. However, access to modifying low-risk data shall use authentication methods that meet the requirements for accessing medium-risk data.

The required levels of assurance, the associated authentication requirements, and the procedures to implement this policy are outlined in *Information Security: Authentication Procedures*.

Reference Documents

Data Classification: Data Classification and Protection
Systems & Networking: Authentication Procedures
Request for admin access (AES)
Request for admin access (CES)