6. GENERAL POLICIES

6.1 INCLEMENT WEATHER AND EMERGENCY CLOSINGS
If the UA System Office officially closes due to inclement weather or other emergency reasons, employees will be granted administrative (paid) leave. Otherwise, if the UA System Office remains open, employees are expected to report to work as usual. Each campus will notify local media sources and post announcements on their websites as determinations are made regarding closings.

The UA System Office operates in multiple locations. Emergency closures, including closures due to inclement weather, may differ by location:

- Campus-based employees should follow campus procedures and advice.
- Montgomery-based employees should follow state office procedures and advice.
- Sid McDonald Hall and other System-only locations in Tuscaloosa should follow UA campus procedures and advice, except for additional advice, updates, and directives that will be communicated by official employee email, by phone, or the UA System Office’s website from the Chancellor or his/her designee.

Leave Procedures for Emergency Closings

1. Administrative (paid) leave will be granted during emergency closings.
2. Regardless of location, if an employee experiences undue travel or other difficulties, but his/her office is open, the employee may request annual or personal leave from his/her supervisor.
3. Non-exempt employees must seek prior supervisor approval before performing work during official closings.
4. Non-exempt employees who are required to work during inclement weather and emergency closings will be paid for time worked at a rate of 1.5 times the hourly rate in addition to administrative leave pay.

6.2 UA SYSTEM OFFICE PROPERTY
Private or personal use of UA System Office property without proper authorization is prohibited. Employees are prohibited from discarding UA System Office property. Employees should contact Human Resources for disposition of property that is no longer needed. Equipment should be turned into the respective campus’s IT group or UAS IT to properly wipe any data from the system to avoid any possible retrieval. Devices that will no longer be used should also be wiped and the hard drive properly destroyed prior to surplus. Equipment that is obsolete or has been rendered useless must be transferred to the relevant campus Surplus Property for disposal by Property and Inventory Management regardless of the dollar value.

Employees separating from service are prohibited from retaining and/or removing any UA System Office property. UA System Office property includes, but is not limited to, work-related files of any kind, office
keys, supplies, computers, credit cards, parking permits, furniture, office décor, etc. Employees should contact Human Resources for instructions on returning all UA System Office property upon separation from service.

6.3 **RESPONSIBLE USE OF ELECTRONIC RESOURCES**

All electronic media systems, including, but not limited to, voicemail, electronic mail, the Internet, voice and video networks, fax machines, hardware, software, local area networks, files, and all information composed, transmitted, accessed, received, or stored in these systems are the property of the UA System Office. These systems are to be used primarily for conducting UA System Office business. Only limited, occasional, or incidental use of electronic media resources (sending or receiving) for personal, non-business purposes is allowable as is the case with personal calls.

These systems are not to be used in ways that violate UA System Office mission or policies or local, state or federal laws or other legislation. They should not be used for soliciting outside business ventures, nor for soliciting for non-System Office related purposes.

The UA System Office reserves the right, at its discretion, to review any employee’s electronic files and messages and usage to the extent necessary to ensure that electronic media resources are being used in compliance with applicable guidelines, policies, and laws.

The UA System Office may exercise its right to review, audit, intercept, access and disclose all matters on its systems at any time, with or without employee notice, during or after working hours. Employees should have no expectation of privacy in connection with the use of these systems. In addition, the UA System Office may be required to provide information stored in its electronic media resources to someone other than the user as a result of a court order or a civil, criminal or internal investigation or an open records request.

Employees shall always respect intellectual property rights when obtaining information over the Internet or using e-mail. Illegal or unauthorized downloading, uploading, copying or distribution of copyrighted works as defined under the Digital Millennium Copyright Act is strictly prohibited. Employees should be aware that such infringement could result in legal liability for the employee and the System Office and may result in disciplinary action to the employee.

**System Office Electronic Accounts**

Users of UA System Office electronic accounts are granted access to System Office information through authorized and approved System Office provided accounts. All UA System Office information, and especially all sensitive and restricted information as defined in the UA System Office Security Procedures, will be accessed through computer accounts established for an individual based on their role and job responsibility. Detailed procedures define the account management processes for access to all System Office information and will include account request, account modification or termination based on the individual’s change in role or job responsibility, and termination of accounts based on separation or retirement.

UA System Office accounts include the individual’s identification (user ID), the authentication process (password, PIN, multi factor, token, biometric, etc.), and the authorization (access rights to information). Authorization or access rights to System Office accounts shall be provided in accordance
with the concept of “least privilege” meaning that an individual shall be granted access to information required to perform their job and nothing more where technically possible.

Upon employment, most users are given access to a UA System Office email account and a single sign-on account. For most job roles, wireless access is available using single sign-on.

Individuals are responsible for the protection and privacy of their electronic accounts. Each account is for the exclusive use of the individual to whom it is assigned. Any unauthorized use of System Office accounts should be reported as an incident to the UA System Office IT team. No individual should be allowed access to any other individual’s account unless authorized to do so from IT, Human Resources, Office of Counsel, law enforcement, or another defined authority. Sharing of accounts is prohibited. However, employee passwords will be disclosed to appropriate System Office personnel, such as IT, Human Resources, Office of Counsel, law enforcement, or another defined authority, when necessary.

The University may exercise its right to review, audit, intercept, access, and disclose all matters on its systems and networks at any time, with or without notice to the user, during or after working hours. Individuals should have no expectation of privacy in connection with the use of System Office accounts.

User accounts may not be used in an inappropriate manner such as, but not limited to:

- Activities that violate any UA System policy
- Accessing information for which the user is not authorized or making attempts to circumvent or defeat account usage restrictions
- Use must not result in commercial gain or benefit to the user and cannot constitute consulting for a business or running a business
- Use that promotes commercial activities or displays paid advertising
- Use that violates state or federal laws or UA System policies on the use of UA System Office equipment, resources, email listservs or time including, but not limited to, engaging in political activities in their individual capacities as private citizens
- Use that violates any copyright or license agreements
- Use that includes the following forms of communication, which are prohibited
  - Obscenity
  - Defamation
  - Advocacy directed to incite or produce lawless action
  - Threats of violence against person(s) or property
  - Disruption of the academic environment
  - Discrimination or harassment due to race, sex, religion, disability, age, or other protected status
  - False information about academic or administrative policies or issues
- Use that attempts to create a sexually or racially hostile work or academic environment
- To send, view, download, or forward abusive, threatening, obscene or harassing material
- Use that may access, destroy, endanger, or divert another’s research, writing, data, or other work product without permission of the owner
- Use that may involve the intentional introduction of destructive software, such as programs known as computer viruses, trojan horses, ransomware, or worms, crypto currency mining software, distributed computing software, or penetration testing software into any UAS computer, computer system, or network without prior approval
• Use that may involve disclosure of passwords or identifying data that attempts to circumvent system security or in any way attempts to gain unauthorized access
• Use that misrepresents oneself or the UA System Office or to otherwise violate explicit workplace policies mandated within the UA System or within a particular department or division.

For voluntary separation, electronic account access will be removed the day after separation. For involuntary separation, electronic account access will be removed immediately upon receipt of notification instructions from Human Resources and the department.

6.4 **TELEPHONE USE**
The UA System Office recognizes there may be times when employees must make or receive personal calls during business hours. However, such calls should be held to a minimum and should not interfere with the employee’s work. Employees are encouraged to handle such calls during their breaks or lunch time.

Use of personal cell phones and other electronic devices should also be held to a minimum and must not interfere with the employee’s work. Employees are prohibited from using their cell phones and other electronic devices while driving on UA System Office business.

Supervisors are expected to address excessive or inappropriate use of UA System Office telephones or personal electronic devices during employee work hours.

Any emails accessed, stored and sent on system servers and Internet access on UA System Office-owned computers are the property of the UA System Office. Employees are discouraged from sending or receiving personal emails from their system email addresses. Upon termination from employment, it is within the discretion of the UA System Office to forward personal emails to individuals who have terminated their employment.

**Wireless Device Security**
As a security measure, the employee acknowledges the UA System Office may be called upon to “wipe” all data from the phone, in the event that the device is lost, stolen, or the employee is terminated. Employee consents to such a “wipe” and waives any claims related to the same. The UA System Office IT recommends the use of Microsoft’s Outlook app for email and calendar usage. In the event of a request for a “wiping” of a device, the following data subjects may be included:
  • If using Microsoft’s Outlook app, all data stored within the app is subject to the “wipe”.
  • Native phone email and calendar apps, a “wipe” may include data beyond the data stored on the email and calendar apps. This would include personal photos, communications, etc.

6.5 **VISITORS IN THE WORKPLACE**
There are occasions when individuals will visit UA System Office employees in the workplace. While we seek to provide an environment open to work and families, it is important that visits not become disruptive to work routines. Frequent or extended presence of visitors during work hours may result in decreased employee productivity and effectiveness. The quality and integrity of UA System Office confidential data, services and resources may also be affected.
Further, the UA System Office believes that frequent or extended presence of visitors in the workplace has the potential to result in the risk of harm to the visitor and possible liability to the UA System Office.

It is not appropriate for children to be in the workplace on a regular basis. No child with an infectious disease should be brought to the workplace under any circumstances. If UA System Office employees must attend to their children, they should take sick or annual leave as appropriate to accommodate their children during working hours.

Situations that result in excessive or inappropriate workplace visitors will be addressed and may result in disciplinary action.

If a visitor is injured while visiting an employee in the workplace, employees should report the incident or injury to their supervisor and the UA System HR Department, which will provide the appropriate forms for reporting.

6.6 **WORKFORCE REORGANIZATION**

In times of business and/or financial necessity, the administration of the UA System Office has authority to determine the priority of retaining services and combining and/or eliminating positions or programs.

Employees who are impacted by a workforce reorganization should contact the UA System HR Department for assistance in locating other employment and for guidance regarding pay and benefit matters.