# Acceptable Use Policy

**Purpose**

The purpose of IT Services is to further the research, education, and administrative functions of ASMSA. To achieve this purpose, these policies intend:

- To ensure the integrity, reliability, and performance of ASMSA IT systems and network.
- To ensure that the ASMSA community of IT users utilize the campus IT facilities in a fair and equable manner with respect for the rights of the community at large.
- To ensure that IT systems and network are used for their intended purposes.
- To establish sanctions and processes for addressing violations.
- To provide a secure and safe computing environment.

**Scope and Applicability of This Policy**

Anyone using or accessing ASMSA IT Systems is subject to the provisions of this policy. ASMSA faculty, staff, registered students, alumni, and approved guests, contractors, consultants are permitted to use ASMSA's computing and networking services but are subject to the terms of this policy during that use. Individuals who use personally owned equipment while connected to the school network are subject to the provisions of this policy while connected to the network. Other responsibilities of users are detailed in "Use of IT Systems" below.

**Definition of Terms**

Sensitive Data: Sensitive data is a blanket term used to designate classes of data with a high level of security that the school is legally or contractually required to protect. Sensitive data refers to any element of data that is uniquely or in aggregate protected by federal regulations (ex: HIPAA, FERPA), categorized as PII or PHI, or any other data that has been identified as business critical or business-sensitive data, such as financial records or intellectual property of ASMSA.

**Policy**

**Introduction**

It is the policy of the school to provide and maintain computing, networking, and telecommunications technologies to support the education, research, and work of its students, faculty, and staff. The school respects the rights of users to express their own opinions in their personal communications using the computer systems. To preserve the security, availability, and integrity of ASMSA computing resources, and to protect all users' rights to an open exchange of ideas and information, this policy sets forth the responsibilities of each member of the ASMSA community relative to the use of these resources. To accomplish these ends, this policy also supports the resolution of complaints raised under this policy.

Every user of ASMSA IT Systems must be aware that violations of this policy may result in revocation of access, suspension of accounts, disciplinary action, or prosecution, and that evidence of illegal activity

will be turned over to the appropriate authorities. It is the responsibility of each member of the ASMSA community to read and observe this policy and all applicable laws and procedures.

Campus units that manage their own computers may add, with the approval of the Director and reviewed by the IT Manager, individual guidelines which supplement, but do not change, the intent of these policies.

The computing, networking, and telecommunications technologies established or maintained by ASMSA are the property of ASMSA, as are any software licenses purchased with School funds. The computer records created or maintained by employees and contained in these systems – including documents, email, listserv archives, text messages, and voice mail are the property of ASMSA. Exceptions to ASMSA ownership of such records include those addressed through a grant or contractual relationships with external agencies or those in which ownership rights are transferred through other ASMSA policies.

The policies described herein are those that the school uses in the normal operation of IT facilities and network. This document does not waive any claim that ASMSA may have ownership or control of any hardware, software, or data created on, stored on, or transmitted through ASMSA IT systems and network.

**Privileged Access and Investigation**

ASMSA Information Technology staff who are specifically hired to maintain ASMSA's computing and networking resources have special privileges and special responsibilities under this policy. These staff are required to keep confidential any personal information that they come in contact with in the course of performing their duties but are also required to report any known misuse or abuse of computing and network resources. They have been granted extraordinary powers to override or alter access controls, configurations, and passwords, which they must exercise with great care and integrity. In addition to following the tenets of this policy, ASMSA IT Staff are expected to abide by the code of ethics identified and maintained by the USENIX Association, which is the primary professional organization of systems administrators.

**Use of IT Systems**

Access to ASMSA IT Systems is a privilege granted on the presumption that every member of the school community will exercise it responsibly. Because it is impossible to anticipate all the ways in which individuals can damage, interrupt, or misuse ASMSA computing facilities, this policy focuses on a few simple rules.

- All systems, devices, users connected to ASMSA information technology resources must use system security and management tools (patch management tools, antivirus, etc.) provided by IT Services to protect ASMSA infrastructure and the Exceptions to this policy should be made in writing to the IT Manager. Written exceptions are not required for the instruments, control devices, and other systems or devices using embedded operating systems. To have a safe and secure cyber environment, the following rules must be followed or implemented:

- Every system, device, or user connected to the school resources and using School resources must be part of the Active Directory System, Hybrid Active Directory/Azure, or Azure Active Directory joined.
- Every user must have a unique account to use School resources.
- Every device and system owned by School, used for research purposes, and used by faculty or staff to perform School business must contain an endpoint security solution provided and managed by IT Services.

**Use of ASMSA IT Systems must be consistent with the school priorities:**

- Private, restricted, Personally Identifiable Information (PII) or confidential information shall not be stored on user devices, including workstations, laptops, servers outside of the data center, removable media, and portable hard drives at any time. Private, restricted, PII, or confidential information can only be stored encrypted.
- Although the minimum personal and incidental use of ASMSA IT resources is permissible within the guidelines of the policy, users should not abuse this privilege. Furthermore, users should not use campus IT resources, including but not limited to servers, storage systems, network devices, or cloud-based applications to save or host non-campus related data or personal information.
- ASMSA technology team will attach the greatest priority to uses that support the academic, research, and business functions of the school. The use of the network for entertainment purposes constitutes the lowest of its priorities and may be preempted should diversion of resources to a higher priority be deemed necessary. To maintain these priorities, the school reserves the right to limit the number of resources an individual user consumes.

**Several actions are specifically forbidden:**

- Engaging in illegal peer-to-peer file-sharing or other illegal downloading.
- Selling access to ASMSA computing resources.
- Malicious activities, intentionally denying or interfering with any network resources, including spamming, bombing, jamming, and crashing any computer.
- Using or accessing any ASMSA IT System, or reading or modifying files, without proper authorization.
- Sending chain letters.
- Users must respect the purpose of and abide by the terms of use of online media forums, including but not limited to social networking websites, mailing lists, chat rooms, and blogs.
- School information resources must not be used for partisan political activities were prohibited by federal, state, or other applicable laws, and may be used for other political activities only when in compliance with federal, state, and other laws and in compliance with applicable School policies.
- School information resources should not be used for activities unrelated to appropriate School functions, except in a purely incidental manner.
- School information resources should not be used for commercial purposes, including advertisements, solicitations, promotions, or other commercial messages, except as permitted under School policy. Any such permitted commercial use should be properly related to School activities, consider proper cost allocations for government and other overhead determinations,

and provide for appropriate reimbursement to the school for taxes and other costs the school may incur by reason of the commercial use. The Director of Finance and Administration will determine permitted commercial uses.

**No Impersonations**

- Using ASMSA IT System to impersonate someone else is forbidden.
- Users must use their own login ID and password. Access to any ASMSA IT System using another user's logon credentials is fraudulent and prohibited by this policy.
- Mail or postings from ASMSA IT Systems must not be sent anonymously. Users must not conceal their identity under any circumstance when using ASMSA IT Systems.
- Users are responsible for the use of their logon credentials and are presumed to be responsible for any activity carried out under their IT system accounts.

Most ASMSA IT Systems are designed so that log on credentials create an audit trail for important business processes. Sharing logon credentials with others circumvents this vital aspect of system integrity. For this reason, and to forestall potential abuse, users must keep their credentials private and not allow others to use them. IT Services maintains a process for obtaining temporary access to required functionality across its systems. Requests for extended functionality must be directed to ASMSA tech support.

**Proper Authorization:**

- Use of ASMSA IT systems is restricted to authorized ASMSA faculty, staff, alumni, and students.
- The administrator of ASMSA IT Services is the responsible authority, which grants authorization for system use and access.
- Users must not permit or assist any unauthorized person to access ASMSA IT systems.
- Guests of ASMSA may use the guest wireless network.
- Users must not access or attempt to access data on any ASMSA IT system they are not authorized to access.
- Users must not make or attempt to make any deliberate, unauthorized changes to data on an ASMSA IT system.

**Honor the Privacy of Others**

- Personal e-mail and electronic files maintained on School equipment and personal Web pages are part of a comprehensive electronic information environment. This environment creates unique privacy issues that involve federal and state laws as well as School policies.
- Users have the right to expect that their legitimate uses of ASMSA IT Systems are confidential. ASMSA users who invade the privacy of others may have their access suspended and may also be subject to School disciplinary action through appropriate channels and legal procedures.
- Users must not access the contents of files of another user without authorization from that user.
- Users must not intercept or monitor any network communications not explicitly meant for them.
- Systems administrators will identify categories of data, which will be managed as confidential on a particular IT system, and they will make all reasonable efforts to maintain the confidentiality of that data. However, limited risks do apply to confidentiality, for example to IT

limitations, software bugs, and system failures. Systems administrators will take reasonable steps to inform users of the limits to confidentiality for their respective ASMSA IT systems. Users are expected to become familiar with those limits and risks of confidentiality and to manage their confidential data accordingly. Confidentiality of data must comply with the State of Arkansas Freedom of Information Act.

- Unauthorized users must not create or use programs, hardware, or devices that collect information about other users without their knowledge and consent. Software on ASMSA IT Systems is subject to the same guidelines for protecting privacy as any other information-gathering project at the school. Further, users may not disclose private information that they discover while accessing ASMSA IT Systems, even if that access is for legitimate use.
- Caution must be taken if the transmission of sensitive data is required. Sensitive data must be encrypted before transmission via email or other forms of digital transmission.

**No Threats to Infrastructure**

- The ASMSA IT Department is authorized to investigate alleged or apparent violations of ASMSA IT policy or applicable law involving IT systems and/or network using whatever means appropriate. The IT Department will maintain a log and incident reporting of all such incidents.
- Users must not extend the ASMSA network without explicit permission from the IT Department. The unauthorized use of routers, switches, modems, wireless access points, and other devices can impact the security and stability of the network and is strictly prohibited. All use of network addresses or other address spaces as contracted by the school must be registered with IT Services
- Users must not use ASMSA IT Systems to attack computers, accounts, or other users by launching viruses, worms, Trojan horses, or other attacks on computers at ASMSA or elsewhere.
- Users must not perform unauthorized vulnerability scans on systems.
- Anomalous (unusual or unexpected) computing activity that is illegal or wasteful of ASMSA IT Resources or that violates the terms of use of the licenses and agreements through which ASMSA obtains or uses ASMSA IT Resources is prohibited.
- Users who have extraordinary bandwidth needs should work with ASMSA IT Department to address these needs.
- Because of the rapid pace of technological change, ASMSA IT Department has extraordinary powers to interpret this rule and may apply it to any activity not identified here that threatens 1) the health of the ASMSA network, systems, or applications or 2) the integrity of data including personal information about users.

**No Violation of Federal, State Laws or School Policies**

- Users must adhere to licensing agreements that the school has with its vendors. All use of ASMSA IT systems and network must be consistent with all contractual obligations of the school, including limitations defined in software and other licensing agreements. Users are not authorized to download and install unapproved software without prior authorization and approval from IT Services. Approved software can be located and installed via the Company

Portal. It is always incumbent on each ASMSA user to ensure that their use of the software remains in compliance with the ASMSA license.

- Possession of a copy of ASMSA-licensed software does not imply personal ownership or unrestricted use of that software.
- Users who leave the school must relinquish any School licensed software, and, consistent with the School's Intellectual Property Policy, all ASMSA-owned data. Questions about the appropriate use of ASMSA-licensed software may be directed to the IT Manager.
- Departing employees are not entitled to remove, destroy, or copy any of the business-related documents entrusted to their care or created by them during their employment unless otherwise permitted by ASMSA.
- Without specific authorization by the system administrator, users must not remove any School-owned or administered equipment or documents from an IT system.
- Users must not violate copyright laws. Such violations include, but are not limited to, illegal peer-to-peer file sharing and unauthorized downloading of copyrighted content (like movies, songs, TV shows, and other broadcasts).
- Users must not use ASMSA computing resources to harass others or to publish libelous statements. Various types of harassment, including sexual or racial, are proscribed by other School policies.
- Users of ASMSA IT Systems are subject to all federal and state obscenity laws. The use of School resources to access pornographic materials for non-work purposes may result in disciplinary action, up to and including termination.
- Users must not use ASMSA email or other technology for Intentional, non-incidental acquisition, storage, and/or display of sexually explicit images or to send unsolicited commercial email or sexually explicit email as defined in Arkansas's Unsolicited Commercial and Sexually Explicit Electronic Mail Fair Protection Act.
- Users must not use ASMSA IT Systems (e.g., e-mail, social media, blogs), without specific authorization, to imply ASMSA support (as opposed to personal support) for any position or proposition.
- Users must observe all applicable policies of external or off-campus data networks when using such networks.

**Access to Data and Data Classification**

ASMSA will exercise its right of access to the digital information of users only in the following circumstances:

- Those instances where the school has a legitimate "need to know." Examples include those where there is reasonable suspicion that: a user is using email to threaten or harass someone; a user is causing disruption to the network or other shared resources; a user is violating School policies, laws, or another user's rights; a student is engaged in academic dishonesty, or a faculty or staff member is in violation of any School policy addressing research misconduct. "Need to know" access will be conducted by ITS staff only after securing the approval of the General Counsel. If access provides evidence of a violation of law, this policy, or other School policies, the results of such access may be shared with other appropriate officials of the school.

- Those instances in which the school must comply with a Freedom of Information Act request, a subpoena, or a discovery request.
- Those instances in which an employee is absent from work and access to specific computer records is critical to continue the work of the school during their absence.
- Those instances in which access to School information is required for IT Staff to carry out their administrative practices – e.g., backing up files, cleaning up trash or temporary files, searching for rogue programs, or conducting routine systems maintenance. This restriction does not apply to the collection of audit trails and usage logs by ASMSA IT Staff. There are times, however, in the regular course of their jobs, when IT Staff may encounter private or personally identifiable information. In this event, ASMSA IT Staff are responsible for keeping that information secure and must not divulge it to anyone unless they believe a breach of law or policy has occurred. IT Staff are regularly reminded of this responsibility.

**Reporting and Compliance**

Incidents that violate this policy may or may not require an immediate response. Those that pose an immediate danger to persons, systems, or property will be addressed by the appropriate School agencies. Whether or not an incident requires an immediate response, violations of this policy may result in revocation of access, suspension of accounts, disciplinary action, or prosecution. Evidence of illegal activity will be turned over to the appropriate authorities.

Any violations of this policy should be reported by e-mail to the ASMSA Tech support at techsupport@asmsa.org or by phone at 501.622.5142.

Users must not conceal or help to conceal or "cover-up" violations by any party. Users are expected to report any evidence of an actual or suspected violation of this policy to the systems administrator of the facility most directly involved. In case of doubt, the report should be made to the ASMSA IT Manager.

**Review**

This policy should be reviewed at least once a year or when required by legal and/or regulatory changes.

**Additional Documents and Policies**

Definitions

Sensitive Data: Sensitive data is a blanket term used to designate classes of data with a high level of security that the school is legally or contractually required to protect. Sensitive data refers to any element of data that is uniquely or in aggregate protected by federal regulations (ex: HIPAA, FERPA), categorized as PII or PHI, or any other data that has been identified as business critical or business-sensitive data, such as financial records or intellectual property of ASMSA.

All Computer Usage policies can be found at https://www.asmsa.org/human-resources/. Federal and state laws and regulations pertaining to computer usage is listed below.

1. USENIX System Administrators' Code of Ethics
2. Arkansas's Unsolicited Commercial and Sexually Explicit Electronic Mail Fair Protection Act
3. State of Arkansas Freedom of Information Act
4. SS-70-001: Arkansas DIS Data and System Security Classification
5. FERPA
6. HIPAA
7. PCI 3.2
8. ISO-27001:2013
9. NIST 800-53A
10. NIST-Cyber Security framework

---