ANDERSON UNIVERSITY

ACCEPTABLE USE POLICY

CONTENTS

1.0 PURPOSE

Anderson University's technology infrastructure exists to support the institution and administrative activities needed to fulfill the institution's mission. Access to these resources is a privilege that should be exercised responsibly, ethically and lawfully.

The purpose of this Acceptable Use Policy is to clearly establish the University's position relating to the acceptable use of its technology and the role each member of the institution has in protecting its information. Fulfilling these objectives will enable Anderson University to implement a comprehensive system-wide Information Security Program.

2.0 SCOPE

This policy applies to all users of computing resources owned, managed or otherwise provided by the institution. Individuals covered by this policy include, but are not limited to all workforce members, service providers, students, and anyone else with access to the institution's computing resources and/or facilities. Computing resources include all Anderson University owned, licensed or managed hardware and software, email domains and related services and any use of the institution's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

3.0 PRIVACY

Anderson University will make every reasonable effort to respect a user's privacy. However, employees and other users as identified above, do not acquire a right of privacy for communications transmitted or stored on the institution's resources. Additionally, in response to a judicial order or any other action required by law or permitted by official Anderson University policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the institution, the President may authorize an Anderson University official or an authorized agent, to access, review, monitor and/or disclose computer files associated with an individual's account. Examples of situations where the exercise of this authority would be warranted include, but are not limited to, the investigation of violations of law or the institution's rules, regulations or policy, or when access is considered necessary to conduct Anderson University business due to the unexpected absence of an employee or to respond to health or safety emergencies.

4.0 POLICY

4.1 PERSONAL USE

Activities related to Anderson University's mission take precedence over computing pursuits of a more personal or recreational nature. Personal use of the University's information technology and digital resources, except for students enrolled at the University, should be incidental and kept to a minimum. Any use that materially disrupts the institution's mission or its day-to-day business activities is prohibited without an explicit exception.

Following the same standards of common sense, courtesy, and civility, but subject to the right of individuals to be free from intimidation, harassment, and unwarranted annoyance. All users of Anderson University's computing resources, whether via personally-owned and/or institution-owned and managed devices, must adhere to the requirements enumerated below.

4.1 FRAUDULENT AND ILLEGAL USE

Anderson University explicitly prohibits the use of any information system for fraudulent and/or illegal purposes. While using any of the institution's information systems, a user must not engage in any activity that is illegal under local, state, federal, and/or international law. As a part of this policy, users must not:

- Violate the rights of any individual or company involving information protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by Anderson University.
- Use in any way copyrighted material including, but not limited to, photographs, books, or other copyrighted sources, copyrighted music, and any copyrighted software for which the institution does not have a legal license.
- Export software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Issue statements about warranty, expressed or implied, unless it is a part of normal job duties, or make fraudulent offers of products, items, and/or services.

Any user that suspects or is aware of the occurrence of any activity described in this section, or any other activity they believe may be fraudulent or illegal, must notify his/her manager immediately.

If any user creates any liability on behalf of Anderson University due to inappropriate use of the institution's resources, the user agrees to indemnify and hold the institution harmless, should it be necessary for Anderson University to defend itself against the activities or actions of the user.

4.2 CONFIDENTIAL INFORMATION

Anderson University has both an ethical and legal responsibility for protecting confidential information in its possession and to which it has been entrusted by its constituencies in order to pursue its missions and daily activities, in accordance with its Data Classification Policy. To that end, there are some general positions that the institution has taken:

- Transmission or recording of confidential information by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, audio recordings, etc.) is prohibited.
- The writing or storage of confidential information on mobile devices (phones, tablets, USB drives) and removable media is prohibited. Mobile devices that access confidential information will be physically secured when not in use and located to minimize the risk of unauthorized access.
- All workforce members and service providers will use approved workstations or devices to access institution's data, systems, or networks. Unapproved non-institution owned workstations that store, process, transmit, or access confidential information are prohibited. Accessing, storage, or processing confidential information on home computers is prohibited.
- All company portable workstations will be securely maintained when in the possession of workforce members. Such workstations will be handled as carry-on (hand) baggage on public transport. They will be concealed and/or locked when in private transport (e.g., locked in a secure area of an automobile) when not in use.
- Photographic, video, audio, or other recording equipment will not be utilized in secure areas, without specific exceptions addressing what is recorded and how recordings are to be performed from ITS.
- All confidential information stored on workstations and mobile devices must be encrypted.
- All workforce members who use institution-owned workstations will take all reasonable precautions to protect the confidentiality, integrity and availability of information contained on the workstation.
- Institution employees and affiliates who move electronic media or information systems containing confidential information are responsible for the subsequent use of such items and will take all appropriate and reasonable actions to protect them against damage, theft and unauthorized use.
- Institution workforce members will log off or lock their workstation whenever they leave their workstation unattended or at the end of their shift.

4.3 HARRASSMENT

Anderson University is committed to providing a safe and productive environment, free from harassment, for all employees. For this reason, users must not:

- Use institution information systems to harass any other person via e-mail, telephone, or any other means, or
- Actively procure or transmit material that is in violation of sexual harassment or hostile workplace laws.

If a user feels he/she is being harassed through the use of the institution's information systems, the user must report it to their supervisor, any department head, or otherwise in accordance with the formal Sexual Harassment policy, the Sex/Gender Misconduct Policy and Title IX, and any associated procedures.

4.4 INCIDENT REPORTING

Anderson University is committed to responding to security incidents involving personnel, institution-owned information or institution-owned information assets. As part of this policy:

- The loss, theft or inappropriate use of institution access credentials (e.g. passwords, key cards or security tokens), assets (e.g. laptop, cell phones), or other information will be reported to the IT Help Desk.
- An institution workforce member will not prevent another member from reporting a security incident.

4.5 MALICIOUS ACTIVITY

Anderson University strictly prohibits the use of information systems for malicious activity against other users, the institution's information systems themselves, or the information assets of other parties.

4.5.1 DENIAL OF SERVICE

Users must not:

- Perpetrate, cause, or in any way enable disruption of Anderson University's information systems or network communications by denial-of-service methods;
- Knowingly introduce malicious programs, such as viruses, worms, and Trojan horses, to any information system; or
- Intentionally develop or use programs to infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.

4.5.2 CONFIDENTIALITY

Users must not:

- Perpetrate, cause, or in any way enable security breaches, including, but not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access;
- Facilitate use or access by non-authorized users, including sharing their password or other login credentials with anyone, including other users, family members, or friends;
- Use the same password for Anderson University accounts as for other non-Anderson University access (for example, personal ISP account, social media, benefits, email, etc.);
- Attempt to gain access to files and resources to which they have not been granted permission, whether or not such access is technically possible, including attempting to obtain, obtaining, and/or using another user's password; or
- Make copies of another user's files without that user's knowledge and consent.
- All encryption keys employed by users must be provided to Information Technology Services if requested, in order to perform functions required by this policy.
- Base passwords on something that can be easily guessed or obtained using personal information (e.g. names, favorite sports teams, etc.).

4.5.3 IMPERSONATION

Users must not:

- Circumvent the user authentication or security of any information system;
- Add, remove, or modify any identifying network header information ("spoofing") or attempt to impersonate any person by using forged headers or other identifying information;
- Create and/or use a proxy server of any kind, other than those provided by Anderson University, or otherwise redirect network traffic outside of normal routing with authorization; or
- Use any type of technology designed to mask, hide, or modify their identity or activities electronically.

4.5.4 NETWORK DISCOVERY

Users must not:

- Use a port scanning tool targeting either Anderson University's network or any other external network, unless this activity is a part of the user's normal job functions, such as a member of Information Technology Services, conducting a vulnerability scan, and faculty utilizing tools in a controller environment.
- Use a network monitoring tool or perform any kind of network monitoring that will intercept data not intended for the user's, unless this activity is a part of the user's normal job functions.

4.6 OBJECTIONABLE CONTENT

Anderson University strictly prohibits the use of institutional information systems for accessing or distributing content that other users may find objectionable. Users must not post, upload, download, or display messages, photos, images, sound files, text files, video files, newsletters, or related materials considered to be:

- Political
- Racist
- Sexually-explicit
- Violent or promoting violence

4.7 HARDWARE AND SOFTWARE

Anderson University strictly prohibits the use of any unapproved hardware or unlicensed software. All software on institutionally-owned and managed systems must be approved, installed, configured, and tracked, by the Information Technology Services Dept. or other institutional department management, as appropriate. Users must not:

- Install, attach, connect or remove or disconnect, hardware of any kind, including wireless access points, storage devices, and peripherals, to any institutional infrastructure or similar core network information systems without the knowledge and permission of Information Technology Services;
- Download, install, disable, remove or uninstall unlicensed software of any kind, including patches of existing software, to any institutional information system without the knowledge and permission of the institution;
- Use personal flash drives, or other USB based storage media, without prior approval from Information Technology Services Department to back up institutional information.
- Use personal USB devices, if enabled, that have been used on other systems without first running a manual scan on the device to ensure it is malware or virus free
- Take Anderson University equipment off-site without prior authorization.

Departments must track any software purchased or downloaded and retain this information for potential management and assessment needs.

4.8 MESSAGING

The institution provides a robust communication platform for users to fulfill its mission. Users must not:

- Automatically forward electronic messages of any kind, by using client message handling rules or any other mechanism;
- Send unsolicited electronic messages, including “junk mail” or other advertising material to individuals who did not specifically request such material (spam);

- Solicit electronic messages for any other digital identifier (e.g. e-mail address, social handle, etc.), other than that of the poster's account, with the intent to harass or to collect replies; or
- Create or forward chain letters or messages, including those that promote "pyramid" schemes of any type.

4.9 OTHER

In addition to the other parts of this policy, except for students enrolled at the University, users must not:

- Stream video, music, or other multimedia content unless this content is required to perform the user's normal business functions if these activities negatively impact Anderson network performance.
- Use the institution's information systems to play games or provide similar entertainment.

No users should:

- Use the institution's information systems for commercial use; unless a specific exception is granted.

5.0 ROLES AND RESPONSIBILITIES

Anderson University reserves the right to protect, repair, and maintain the institution's computing equipment and network integrity. In accomplishing this goal, Anderson University ITS personnel or their agents must do their utmost to maintain user privacy, including the content of personal files and Internet activities. Any information obtained by ITS personnel about a user through routine maintenance of the institution's computing equipment or network should remain confidential, unless the information pertains to activities that are not compliant with acceptable use of Anderson University's computing resources.

6.0 ENFORCEMENT

Enforcement is the responsibility of the institution's President or designee. Users who violate this policy may be denied access to the institutional resources and may be subject to penalties and disciplinary action both within and outside of **Anderson University**. The institution may temporarily suspend or block access to an account, prior to the initiation or completion of disciplinary procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the institution or other computing resources or to protect **Anderson University** from liability.

Users are subject to disciplinary rules described in the appropriate Employee Handbook or other appropriate Student Handbook or other policies and procedures governing acceptable workplace behavior.

7.0 EXCEPTIONS

Exceptions to the policy may be granted by the Executive Director of Information Technology Services or by his or her designee. All exceptions must be reviewed annually.

8.0 REFERENCES

- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- NIST 800-53
- NIST 800-171
- FIPS-199
- PCI DSS 3.1
- Code of Ethics of the American Library Association

9.0 RELATED POLICIES

- Information Security Policy
- Data Classification Policy
- Data Classification and Handling Procedure

10.0 POLICY AUTHORITY

This policy is issued by the Information Technology Services Department for Anderson University.

11.0 REVISION HISTORY

Version	Date	Author	Revisions
1.0	March 2021	Anderson University ITS, GreyCastle Security	Initial Draft