AURORA UNIVERSITY

POLICY:
ACCEPTABLE USE

DOCUMENT #: ITS-POL-0002
EFFECTIVE: 05-26-2022
OWNER: ITS

CONTENTS

1.0 PURPOSE

Aurora 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 each member of the institution's role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives will enable Aurora 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 faculty, staff, student workers and service providers with access to the institution's computing resources and/or facilities. Computing resources include all Aurora 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

Aurora University will make every reasonable effort to respect a user's privacy. However, faculty, staff and student workers 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 Aurora University policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the institution, the President of the institution may authorize an Aurora 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 Aurora University business due to the unexpected absence of faculty, staff or student workers or to respond to health or safety emergencies.

4.0 POLICY

Activities related to Aurora University mission take precedence over computing pursuits of a more personal or recreational nature. Any use that disrupts the institution's mission is prohibited.

Following the same standards of common sense, courtesy and civility that govern the use of other shared facilities, acceptable use of information technology resources generally respects all individuals' privacy, but subject to the right of individuals to be free from intimidation, harassment, and unwarranted annoyance. All users of Aurora University's computing resources must adhere to the requirements enumerated below.

4.1 FRAUDULENT AND ILLEGAL USE

Aurora 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 Aurora 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 direct supervisor immediately.

If any user creates any liability on behalf of Aurora 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 Aurora University to defend itself against the activities or actions of the user.

4.2 CONFIDENTIAL INFORMATION

Aurora University has both an ethical and legal responsibility for protecting confidential information in accordance with its Data Classification Policy. To that end, there are some general positions that the institution has taken:

- Transmission of confidential information by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is prohibited.
- 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 faculty, staff, student workers and service providers will use approved workstations or devices to access institution's data, systems, or networks. 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 institution 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 the trunk of an automobile) when not in use.
- Photographic, video, audio, or other recording equipment will not be utilized in secure areas.
- All confidential information stored on workstations and mobile devices must be encrypted.
- All faculty, staff and student workers who use institution-owned workstations will take all reasonable precautions to protect the confidentiality, integrity and availability of information contained on the workstation.
- Institution faculty, staff, student workers 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 activate their workstation locking software whenever they leave their workstation unattended or will log off from or lock their workstation when their shift is complete.

4.3 HARRASSMENT

Aurora University is committed to providing a safe and productive environment, free from harassment, for all faculty, staff and student workers. 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, in writing, to his/her supervisor or any department head.

4.4 INCIDENT REPORTING

Aurora 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 institutional 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 Service Desk.
- No faculty, staff or student worker will prevent another member from reporting a security incident.

4.5 MALICIOUS ACTIVITY

Aurora 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 Aurora 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 Aurora University accounts as for other non-Aurora 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 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 Aurora 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 Aurora 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 the Office of Information Technology, 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 users, unless this activity is a part of the user's normal job functions.

4.6 OBJECTIONABLE CONTENT

Aurora University strictly prohibits the use of institution 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

Aurora University strictly prohibits the use of any hardware or software that is not purchased, installed, configured, tracked, or managed by the institution. Users must not:

- Install, attach, connect or remove or disconnect, hardware of any kind, including wireless access points, storage devices, and peripherals, to any institution information system without the knowledge and permission of Information Technology;
- Download, install, disable, remove or uninstall software of any kind, including patches of existing software, to any institution's information system without the knowledge and permission of the institution;
- Use personal flash drives, or other USB based storage media, without prior approval from their manager; or
- Take Aurora University equipment off-site without prior authorization.

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 REMOTE WORKING

When working remote, the user must:

- Be given explicit approval from Human Resources.
- Safeguard and protect any institution-owned or managed computing asset (e.g., laptops and cell phones) to prevent loss or theft.
- Not utilize personally-owned computing devices for Aurora University work, including transferring Aurora University information to personally-owned devices. Third party vendors and/or contractors will be required to reapply for VPN access annually. Prior to June 30 every year they will be notified to reapply for access, if the application is not received by July 1, access will be revoked.
- Take reasonable precautions to prevent unauthorized parties from utilizing computing assets or viewing Aurora University information processed, stored or transmitted on institution-owned assets.
- Not create or store confidential or private information on local machines unless a current backup copy is available elsewhere.
- Not access or process confidential information in public places or over public, unsecure networks.
- Only use approved methods for connecting to the institution (e.g. VPN).
- Explicit approval from ITS must be obtained prior to VPN Access being granted.

4.9 OTHER

In addition to the other parts of this policy, users must not:

- Stream video, music, or other multimedia content unless this content is required to perform the user's normal business functions;
- Use the institution's information systems for commercial use or personal gain; or
- Use the institution's information systems to play games or provide similar entertainment.

5.0 ROLES AND RESPONSIBILITIES

Aurora University reserves the right to protect, repair, and maintain the institution's computing equipment and network integrity. In accomplishing this goal, Aurora University IT 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 IT 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 Aurora 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 institution resources and may be subject to penalties and disciplinary action both within and outside of Aurora 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 Aurora University from liability.

Users are subject to disciplinary rules outlined in the Employee Handbook, and other policies and procedures governing acceptable workplace behavior. The University reserves the right to impose discipline up to and including immediate termination, whenever management deems it appropriate to do so.

7.0 EXCEPTIONS

Exceptions to the policy may be granted by the Chief of Information Technology, 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)
- Illinois State Information Security Breach and Notification Act (need to review)
- NIST 800-53
- 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 RESPONSIBLE DEPARTMENT

Information Technology Services

11.0 POLICY AUTHORITY

This policy is issued by the Chief Information Officer for Aurora University.

12.0 REVISION HISTORY

Version	Date	Author	Revisions
1.0	03-07-2022	GreyCastle Security	Initial Draft
1.1	05-26-2022	Aurora University Team	Approval/Effective

13.0 APPROVALS

Executive	Chief Information Officer
Name Jeff King	Name Hurstel Howard
COO	CIO
Date 05/24/2022	Date 5/26/2022
Signature Jeff King	Signature Hurstel Howard