ADA University

Technology Resources Acceptable Use Policy

Contents

1. Introduction

This Acceptable Use Policy (AUP) for university technology resources outlines the acceptable and prohibited use of all university technology resources, including hardware, software, network, and data, and applies to all authorized users. The purpose of this policy is to promote responsible and ethical use of university technology resources and to protect the university's systems and data from unauthorized access, misuse, or abuse.

Definitions

"University technology resources" refer to all hardware, software, network, and data owned, operated, or maintained by the university, including but not limited to computers, laptops, mobile devices, servers, databases, applications, websites, and internet connectivity.
"Authorized users" refer to individuals who have been granted access to university technology resources, including students, faculty, staff, adjuncts, contractors, guests, and other affiliated personnel.

2. Purpose

The purpose of this AUP is to promote responsible and ethical use of university technology resources and to protect the university's systems and data from unauthorized access, misuse, or abuse. By following this AUP, users can help ensure the security and integrity of university technology resources and help maintain a safe and productive computing environment for all members of the university community.

3. Scope

This AUP applies to all users of university technology resources, including faculty, staff, students, contractors, and guests – generally a person, who is using University technology resources.

4. Acceptable Use

Authorized Use of University Technology Resources

University technology resources are provided to support academic research, teaching, learning, administrative, and other university-related activities. Use of all University technology resources should be for purposes that are consistent with the educational mission and not for commercial purposes. Authorized uses of university technology resources include (but are not confined to):

- Conducting academic research, course-related work, and university administrative tasks.
- Accessing and using university resources for educational purposes and authorized university business.
- Storing, processing, and transmitting data related to academic research, coursework, and university-related activities.
- Engaging in electronic communication with other members of the university community, external organizations, and individuals on behalf of the university. This could include sending emails, making phone calls, or participating in video conferences with external stakeholders

such as other educational institutions, government agencies and other organizations while representing University.
- Using university facilities to host events authorized by the university and its affiliates.
- Complying with applicable laws, regulations, and university policies.

University technology resources may be used for purposes other than those explicitly stated in this policy, provided that such use is justified and approved by the University leadership (Office of Rector, Office of Vice-Rectors, Office Of COO). Any exceptions to this policy must be properly documented and maintained by the mentioned university authorities. Justified submission for exceptions should include a clear explanation of the need for the exception and how it aligns with the university's mission and values. Exceptions should be reviewed periodically to ensure they remain justified and in compliance with university policies and applicable laws and regulations.

Personal use of University information technology resources should be limited and kept incidental to work duties. Authorized users may engage in non-work-related activities, provided such use is reasonable, does not impede work efficiency, incur additional costs, or hinder others from utilizing shared resources.

Prohibited Use of University Technology Resources

The following activities are strictly prohibited:

- Unauthorized access or use of university technology resources, including attempting to bypass access controls or security measures.
- Using university technology resources for non-University authorized commercial purposes of personal and other institution related nature, political objectives (such as but not limited to political campaigning, lobbying, or advocacy, as well as any activities related to political parties, candidates, or causes) or other non-university related activities, especially to the point that excessive or inappropriate personal use of technology resources can have negative consequences, such as draining network resources, compromising system security, or violating acceptable use policies.
- Sending, requesting others to send to University owned technology resources or storing illegal, threatening, discriminatory, harassing, or abusive messages or content.
- Disclosing or sharing confidential or sensitive information without authorization.
- Installing or using unauthorized software, hardware, or devices on university-owned or operated technology resources.
- Engaging in any activity that could harm or disrupt university technology resources or networks, including sending spam, viruses, or malware.
- Violating copyright or intellectual property laws, including unauthorized reproduction or distribution of copyrighted materials.

Security and Privacy

Users of university technology resources are responsible for ensuring the security and privacy of university data and resources. Users must:

- Follow IT best practices and other applicable policies, guidelines and procedures introduced by respective vendors (for example: Ellucian (Banner), Anthology (BlackBoard Learn)) and/or Information Technologies and Services department (IT&S).
- Report any suspected security breaches or incidents to the university's IT&S and Security and Logistics division of General Administrative Services department.
- Protect university-owned or operated devices from theft, loss, or damage.
- Comply with the applicable University policies and/or other applicable state laws and government regulations.

5. Protection of University Technology Resources

Data Privacy and Confidentiality

The university is committed to protecting the privacy and confidentiality of data stored on university technology resources. Please refer to "**Personal Data Usage and Public Information Policy**", p. 4.4, "**Data Privacy and Data Classification**", section "**f**" for details on data classification.

Users must:

- Only access and use data that is necessary for their authorized university-related activities.
- Protect confidential and sensitive information from unauthorized access, disclosure, or use.
- Effectively utilize available tools and methods for securing data
- Comply with applicable state laws, regulations, and university policies regarding data privacy and confidentiality (such as "**Personal Data Usage and Public Information Policy**")

Information Security Incident Reporting

Users who suspect a security incident or breach must report it immediately to the following departments/functions:
If an incident is related to a violation of the requirements for data usage and protection as outlined in Personal Data Usage and Public Information Policy – to Data Protection Officer.
If an incident is related to information security / information system breach – to IT & S department.

To ensure timely and effective response, users should provide as much relevant information as possible when reporting a security incident or breach.
Users should refrain from discussing or sharing details of the incident with unauthorized individuals or external parties until directed to do so.

All suspected incidents will undergo a thorough investigation, and the responsible department (utilizing collective effort of Information Technology and Services, Safety and Security, Asset Management functions) will promptly take appropriate action, utilizing all available controls, resources, and solutions to address the incident and minimize the possibility of future occurrences. It is crucial that all users fully cooperate with any investigation conducted by the University.

User Responsibilities

Users of university technology resources are responsible for:

- Protecting university technology resources from unauthorized access, use, or disclosure.
- Avoiding usage of third-party tools/solutions if not provided by University.
- Complying with this AUP and all other applicable university policies and procedures.
- Reporting any suspected security incidents, violations of this AUP, or other policy violations to the appropriate authorities as described in this and other applicable University policies and other governing documents.
- Using university technology resources in a manner that does not interfere with other users' ability to access and use those resources.
- Completing any mandatory training on the use of university technology resources is required. Failure to participate in University-organized technology training on a repetitive basis may result in reporting the individuals who have not attended the trainings to their respective management and/or University leadership.

6. University Technology Resource Guidelines

Access to University Technology Resources

Access to university technology resources is granted based on the individual's role, including job duties, status (such as contractor, guest, student, etc.), assigned responsibilities, academic program requirements and other parameters.
Users of university technology resources may not share their access credentials (if provided by the University), or other access information with others or use another person's access credentials to gain unauthorized access.
Access to university technology resources is granted based on the individual's job duties or assigned responsibilities. Users may not share their access credentials, passwords, or other access information with others or use another person's access credentials to gain unauthorized access.

Users are responsible for maintaining the security of their passwords and accounts. Passwords must be kept confidential and should not be shared with others. Users should select strong passwords that are difficult to guess and should change their passwords periodically.

Intellectual Property Rights

Users must respect the intellectual property rights of others and comply with applicable laws and regulations governing copyright, trademarks, and patents. Unauthorized reproduction or distribution of copyrighted materials is strictly prohibited.

7. Monitoring of University Technology Resources

The university reserves the right to monitor university technology resources to ensure compliance with this AUP and applicable laws and regulations.
Computer activity may be monitored by authorized individuals for the purposes of maintaining system performance and security. In instances where individuals may be suspected of abuse of University technology resources, the contents of the individuals' user files may also be inspected by the university.

All information stored on or transmitted through the University's technology resources is subject to the University policies and regulations. The University has the legal right to access, preserve and review all information stored on or transmitted through its technology resources.

8. Protection of Intellectual Property Rights

Ownership of Intellectual Property Created Using University Technology Resources:

Any intellectual property created using university technology resources is owned by the university, subject to applicable laws and regulations. Users may not use university technology resources to create intellectual property for personal gain or commercial purposes.

9. Policy Review and Revision

This AUP will be reviewed periodically and may be revised as necessary to reflect changes in technology, laws, regulations, or university policies.

The University is committed to keeping users informed about any changes to policies. When updates are made to policies, users will receive prompt notifications through various communication channels. These notifications will clearly indicate that a change has occurred and provide a summary of the key updates. The University believes in maintaining transparency and ensuring that users are aware of any modifications that may affect their obligations or rights. The goal is to foster clear communication and promote a shared understanding of the University's policies and any subsequent changes.

Feedback collection will be carried out utilizing various tools, including but not limited to MyADA portal, email, surveys, and other tools.

10. Cultural and Ethical Considerations

In our diverse university community of faculty, staff and students, it is important to respect cultural differences in online communications and collaborations. Users should avoid language or content that might be offensive or exclusionary to others.

11. Policy Enforcement

Users are responsible for familiarizing themselves with this AUP and complying with its provisions.

Violations of this Acceptable Use Policy will be investigated and addressed according to the procedures outlined in the Employee Handbook for staff, the Student Code of Conduct for students, and the Faculty Handbook for faculty members. For other University-affiliated persons, including contractors, vendors, and visitors, violations will be handled in accordance with the University's policies and guidelines applicable to their status. Disciplinary actions for policy violations will be determined based on the relevant policies and guidelines outlined in these respective documents.

12. Contacts

Users may contact the Information Technologies and Services department for assistance with university technology resources and for reporting violations, incidents and breaches described by the current policy.

Email: itservicedesk@ada.edu.az
Phone:

- If calling from outside the ADA Campus or from mobile phone:
  +994 12 437 32 35 and then follow the interactive voice menu prompts and dial internal extension **111**.
- If calling from ADA University provided deskphone or wireless phone:
  Dial internal extension **111**.

13. Acknowledgement

By using university technology resources, users acknowledge that they have read, understand, and agree to comply with this AUP and all other applicable university policies and procedures.

14. Conclusion

In conclusion, this Acceptable Use Policy (AUP) establishes the guidelines for the responsible and ethical use of university technology resources. By adhering to these guidelines, users help ensure the security and integrity of our technology resources and contribute to a safe and productive computing environment for the entire university community.

It is essential for all users to familiarize themselves with this AUP and comply with its provisions. Failure to comply may result in disciplinary action, including suspension or termination of access to university technology resources, as well as legal action if the violation involves criminal activity.

For any questions or concerns about this AUP or its application, please contact the Information Technologies and Services department (see Section 12 – Contacts).