7.5 - Acceptable Use of University Computing Resources Policy

Effective Date: January 1, 2003
Revision Date: February 3, 2016

Purpose and Scope

The Embry-Riddle Aeronautical University Acceptable Use Policy and the Information Security Policy are the overarching policies upon which all University technology resources are governed. These documents provide the foundation for other Information Technology APPMs (Section 7) and internally-scoped Information Technology policies, standards, guidelines, and procedures.

The Acceptable Use Policy (AUP) defines responsibilities for the use of University computing resources, and is applicable to faculty, staff, students, contractors, vendors, and any other individual utilizing University-provided technology resources. Use of these resources is a privilege granted by the University, and access to these resources may be revoked if their use is in violation of the AUP. This technology is provided to support the educational mission of the institution, to enrich student learning, and to facilitate the free exchange of ideas and information between the University and the communities in which it operates.

Policy

Use of any University technology resources constitutes acceptance of and compliance with this policy. All users of these resources **shall**:

1. Comply with all federal, state, local, and other applicable laws; University rules and policies; and all applicable contracts and licenses. Users are responsible for ascertaining, understanding and complying with these laws, rules, policies, contracts, and licenses.
2. Abide by copyright laws when using University computing resources. The unauthorized publishing or use of copyrighted material on a University resource is prohibited and users are personally liable for the consequences of such unauthorized use.
3. Use only authorized computing resources, and use them only in the manner and to the extent authorized, understanding that incidental use of computing resources may be permitted if not in violation of other policies.
4. Keep all account credentials private, and under no circumstances share those credentials with another person.
5. Use due diligence in protecting the data and information to which access has been granted. Refrain from making unnecessary copies of sensitive information. It is the user’s responsibility to ensure any copied or printed data is appropriately protected and securely disposed of after use.
6. Understand that the Internet must be considered insecure. The University does not guarantee the accuracy, availability, or privacy of any information on or communication sent through the Internet.
7. Follow guidance provided by Information Technology Security Services (ITSS) regarding transmission of potentially sensitive or confidential information.
8. Understand that this and other Information Technology APPMs are applicable when using University-provided remote access Virtual Private Networks (VPNs), as these services attach the connecting device directly to University networks.
9. Do no harm.

All users of these resources **shall not**:

1. Engage in the use of University computing resources to create and/or transmit any material which a reasonable person could deem offensive, harassing, or threatening.
2. Obtain unauthorized access of another person's files, programs, accounts, and data.
3. Attempt to circumvent security measures for servers, workstations, network infrastructure equipment, or any other technology equipment.
4. Knowingly compromise, or attempt to compromise, the security of any servers, workstations, network infrastructure equipment, or any other technology equipment.
5. Engage in any activity that is not business-related and which could potentially expose a security risk, disrupt services, or damage institutional resources. This includes, but is not limited to, port scanning, reconnaissance and information gathering, and vulnerability scanning.
6. Store sensitive or critical data solely on local workstations. Any such data should be stored on appropriate network shares to ensure access to said data is properly controlled, and to ensure that data is backed-up on a regular basis.
7. Use University computing resources for commercial purposes or personal gain.

Additionally, faculty and staff, including temporary or contract workers, must complete ongoing, mandatory information security training as prescribed by ITSS and Human Resources.

Any questions regarding appropriate use of any technology resources should be directed to ITSS (**infosec@erau.edu**).

Enforcement

Users who violate this policy may be denied access to University computing resources and may be subject to disciplinary actions and/or criminal and civil penalties. Violations will normally be handled through the University disciplinary procedures applicable to the user and may include referring suspected violations of applicable law to appropriate law enforcement agencies. However, the University may immediately suspend or block access to an account, prior to the initiation or completion of such procedures, when it appears necessary to do so in order to protect the confidentiality, integrity, availability or functionality of University or other computing resources.

Responsible Authority: Chief Information Officer