I. **POLICY**

   a. Computing Services maintains the security and reliability of campus Information Technology (IT) infrastructure. Every IT user of these resources also maintains a responsibility to protect the security and integrity of IT resources and information.

II. **PURPOSE**

   a. This policy establishes the basic Information Technology (IT) security safeguards that must be taken by every person using an Adams State University (ASU) IT resource or otherwise accessing non-public University information. More detailed IT policies are referenced in section V of this document. Additional safeguards may be appropriate, depending on the situation and its inherent risk to ASU information and IT resources.

   b. This policy does not impose restrictions that are contrary to ASU’s established culture of sharing, openness, and trust. However, the University is committed to implementing the safeguards necessary to ensure the privacy of personal information, the availability of University information and IT resources, and the integrity of ASU’s operations.

III. **DEFINITIONS**

   a. Information Technology (IT) Resource: Computing and networking resources owned and maintained by the University, including but not limited to email, accounts, workstations, mobile devices, and phones.

   b. Information Technology (IT) User: Any individual that has been granted access to any IT resource.

IV. **PROCEDURES**

   a. It is the responsibility of every IT resource user to know the University’s IT security requirements and to conduct her/his activities accordingly. IT resource users shall comply with the following requirements:

      i. **Protect the Privacy of Others.** Users shall respect the privacy of others when handling personal information and shall take appropriate precautions to protect that information from unauthorized disclosure or use.
Computing Services | IT User Responsibility and Training | 500-006 | Reviewed 10/2015

ii. **Do Not Store Sensitive Information on Workstations and Mobile Devices, Except When Specifically Needed for Business Purposes.** Ordinarily, sensitive information shall not be stored on workstations and mobile computing devices (laptops, flash drives, backup disks, etc.) unless specifically justified for business purposes and appropriately secured. If sensitive information is stored on a workstation or mobile computing device or transmitted to an external network or organization, IT resource users shall encrypt or adequately protect that information from disclosure. In addition to encryption, other protections may include the use of passwords, automatic logoffs, physical security and secure Internet transmissions. The protection of sensitive information shall be in accordance with campus IT security requirements and other guidance as available from ASU’s Computing Services Department. Computing Services will provide detailed training on any of these methods as requested.

iii. **Keep a Clear Desk and Clear Computer Screen.** IT resource users shall keep all sensitive information out of plain sight unless in use and shall not leave such information displayed when it is not needed.

iv. **Protect Workstations and Other Computing Devices.** IT resource users are responsible for helping to maintain the security of workstations and other computing devices by striving to protect them from unauthorized access and malicious software infections (e.g., viruses, worms, and spyware). Users shall consult ASU’s Computing Services Department for guidance on protecting their computing devices.

v. **Protect Passwords.** Passwords are used to authenticate the identity of individuals and gain access to University resources. Each person is responsible for protecting the passwords assigned to her or him and shall not share them with others.

vi. **Report Security Violations, Malfunctions, and Weaknesses.** IT resource users shall report security related events; known or suspected violations of IT security policy; and inappropriate, unethical, and illegal activities involving University IT resources to ASU’s Computing Services Department.

vii. **Utilize University Information and IT Resources for Authorized Purposes Only.** IT resource users shall access or otherwise utilize University information and IT resources only for those activities they are specifically authorized and in a manner consistent with ASU’s policies, federal and state laws, and other applicable requirements.

b. **Required Information Technology Security Training for IT Users**

   i. All IT users that have access to information technology resources will be required to take an Information Technology Security training prior to receiving access, and annually thereafter.

c. **Compliance**

   i. Violations of this policy are dealt with seriously. Users suspected of violating these policies may be temporarily denied access to ASU’s information technology resources during investigation of the alleged abuse. Illegal acts involving ASU information technology resources may also be subject to prosecution by state and federal authorities.

   ii. IT users that have not completed IT security training are subject to revocation of access to IT resources, such as account suspension.

   iii. Campus notification schedule. Computing Services will implement the following schedule annually for notifying campus of the required training:
1. Annually in October, an email to all employees will be sent that contains the policy and information about the required training. The training system will also email all employees with the instructions to log into the training and get started.
2. Annually in January, a reminder email will be sent via the ABM system and the training system.
3. Annually in April, a second reminder will be sent through the training system ONLY to employees who have not completed the training. A follow-up ABM will be sent if a high percentage of employees have not yet completed the training.
4. Annually in early May, a final reminder will be sent through the training system ONLY to employees who have not yet completed the training.
5. Annually in May, and after grades have been turned in, Computing Services will start the process of locking accounts for employees who have not completed the training, and helping them to get through the training and their accounts reactivated.

V. RELATED POLICIES

a. The following policies provide detailed information relating to the roles and responsibilities of the ASU computing community. Users of campus IT resources are responsible for reading and complying with these policies. These policies may be found on the ASU Computing Services Web Site, computing.adams.edu. Questions regarding these policies should be directed to ASU’s Chief Information Officer.

   i. Policy 500-001, ASU Bandwidth Policy
   ii. Policy 500-002, ASU Voicemail Policy
   iii. Policy 500-003, Acceptable Use Policy
   iv. Policy 500-004, Mobile Computing Policy
   v. Policy 500-005, Data Handling & Storage Policy

VI. RESPONSIBILITY

a. Computing Services is the primary organization responsible for ensuring this policy is properly disseminated and implemented.

VII. AUTHORITY

a. This policy has been prepared under the authority of the President, Adams State University, as delegated by the ASU Board of Trustees.

VIII. HISTORY

a. This document is based on the previous IT User Responsibility Policy approved by Cabinet on 1 May, 2008.

IX. ATTACHMENTS

a.