COLLEGE OF
Engineering, Architecture
&Technology

CEAT ITS User Access Policy and Procedure	Policies and Procedures CEAT-I-004 Effective Date: 12/10/15

Introduction

1.01 The College of Engineering, Architecture, and Technology (CEAT) adheres to Oklahoma State University Information Technology Division's "Appropriate Computer Use" policy, which is located at http://it.okstate.edu/policies/pol_app.php. The purpose of the CEAT-I-004 Policy and Procedure is to provide clarification and direction to CEAT faculty, staff and students on what is expected to successfully comply with the OSU IT Division's P&P.

Procedure

2.01 The OSU IT Division has the "Appropriate Computer Use" policy, which is used by CEAT as a guide. The control of use access is the single most important access control mechanism. The ability to identify and restrict use based on an individual user's credentials is vital to ensuring system integrity and security.

2.02 However, access to system and application is mainly a non-discretionary access (NDAC), which is when the set policies and procedures establish controls that can't be changed by users, but only through administrative action. The CEAT file servers require a role based access control.

2.03 Users are granted access to applications and systems in the CEAT based on the GPO set by the Domain Administrator and modified by the CEAT System Administrator. This is equally true for all others requiring access to the CEAT servers.

2.04 CEAT ITS has outlined procedures for all requiring access to CEAT servers as follows:

2.05 Application servers (such as the Linux based servers) require all users to have a secure connection (SSH or Putty with appropriate encryption level) on their devices (laptop, desktop, or other mobile device) in order to be allowed to access the server using an appropriate login name and password. Authentication for the access will be provided by the OSU Active Directory (AD) system. Password expiration, account lock out and other forms of security restriction are monitored and enforced by the OSU IT Division.

2.06 The same procedures apply to the CEAT file servers maintained by CEAT ITS. Authentication to the file share server is controlled by the OSU AD. However, the role of the user in CEAT determines the level of access to the data stored on these servers.

2.07 In regards to access control, the rules of user profiles will be as follows:

2.08 The user profile will start with the standard access role defined by the University Human Resources department (job description) of the user which may then be modified by the department/unit administrator of the CEAT to the meet the level of access determined by the department/unit.
A user can have multiple profiles, but level of access to resources is controlled by the organizational unit to which a server belongs and the modified definition of the role of the user by the department/unit administrator.

2.09 In regards to consistent management of access rights, the process is as follows:

2.10 The department/unit administrator shall designate a unit member or elect him/her self to manage the access rights of all department/unit members.

2.11 Implementation of access rights will be carried out by the designated CEAT ITS staff member.

2.12 The CEAT ITS designated implementer will be updated by the department/unit administrator promptly of all access modifications and changes.

2.13 In regards to administrative segmentation of access control roles, the process shall define:

- Level of access and role of user,
- Duration of access of user, and
- Number of departments/Units the user will need to access (inter-department access).

2.14 In regards to requirements for formal authorization of access requests, the following information will be required:

- Department/Unit Administrator
- Name of person making the request
- Requestor OSU Email
- Requestor Preferred Email
- Requestor Phone number
- Requestor Department
- Requestor Location

2.15 In regards to requirements for authorization and timely removal of access rights, the process is as follows:

2.16 A department/unit administrator will request change of access rights for a specific user in their department. Once this request is received, all compliance authorization will be obtained, processed and documented.

2.17 In regards to documentation and periodic review based on need, the process is as follows:

2.18 All operations concerning CEAT servers shall be fully documented.

2.19 These operations will include but are not limited to server setup and updates, application installation and updates, change management, access control, security updates, compliance updates, performance updates and backup.

2.20 Documentation will be reviewed periodically for updates.

2.21 In regards to contractors' and guests' service access, conditions for connection to the CEAT applications and systems on the OSU Network Infrastructure are as follows:

- Have received approval from an OSU authorized personnel to use the network, IT infrastructure and/or information and data.
- Read and understood the "Appropriate Computer Use Policy" and the "Application and System Access Policy."
- Will use the network, IT infrastructure and /or information and data in accordance with all university policies and associated laws applicable to the type of information stored, processed, displayed and/or transmitted thereof.
- Will immediately report any security related incident to the Information Security Office at (405) 744-4225. Such incidents may include a lost, stolen, or compromised computer device that contains OSU "Official Use" or "Confidential Data."
- Will not allow unauthorized individuals to access or obtain OSU owned "Official Use" or "Confidential Data."
- Will not access, or exceed authorized access, and/or obtain information from any system for which authorization is not granted.

- Will protect and will not distribute the authentication mechanism (i.e. passwords or token information) used to access OSU owned IT computing resources.

- Will install an approved personal firewall, and anti-virus software on the computing device or any other equipment used to access the network, IT infrastructure and/or information or data.

- Understand that using the university owned network, IT infrastructure and/or information is a privilege and can be withdrawn at any time due to misuse or non-compliance of this agreement.

2.22 As a condition for using CEAT IT applications, systems, and its associated information and data, the contractor and/or individual agrees to all of the aforementioned, which is documented on a form with the agreement indicators via initials/dates of the contractor and/or individual.

Date review completed by CEAT ITS Management: 11/10/15

Date approved by the CEAT Dean and CEAT Executive Council: 12/10/15