Oklahoma State University Policy and Procedures

INFORMATION & RESOURCES: ACCESS CONTROL POLICY	3-0604 ADMINISTRATION & FINANCE Information Technology October 2019

PURPOSE

1.01 With this policy, Oklahoma State University (OSU) sets in general terms the expectations and principles of access control, which apply at an institutional level in order to control risk of negative impact on institutional operations due to unauthorized or inappropriate access to University information systems.

SCOPE

2.01 This policy applies to all University owned or controlled information technology resources whether individually controlled or shared, stand alone or networked.

2.02 Exceptions may apply for computer systems research and/or teaching or class projects.

2.03 This policy applies to persons, whether students, staff, faculty, or authorized third-party users, within OSU units, colleges, departments and any other affiliated agencies, entities, groups or organizations which at any point, such as in business operations or administrative processes, control University-owned or University-leased information assets or technology resources.

2.04 This policy stipulates basic configurations of and applies equally to all information assets or systems used to access or protect access of those assets.

DEFINITIONS

3.01 Data – for the purposes of this document, electronic information (e.g. databases, spreadsheets, email, etc.) or non-electronic (e.g., paper files, publications, hardcopy research, etc.). Information or knowledge concerning a particular fact or circumstance, gained via business operations, academic study, communications, research, instruction, or otherwise, within the pursuit of the University's mission.

3.02 Data custodian – the authoritative head of the respective college or department, or a Principle Investigator or Project Director; those who manage and protect data and are responsible for operations relating to the information.

3.03 Data steward – an individual with the responsibility for coordinating the implementation of data classifications through the establishment of definitions of the data sets available for access and the development of policies and/or access procedures for those data sets.

3.04 Information assets – any University-owned, -leased, -protected, or otherwise authorized information or data.

3.05 Information systems – any resource or equipment used for accessing or for controlling access of information assets.

3.06 Information technology resources – technology and/or computer resources including, but not limited to, personal computers, workstations, mainframes, mobile devices (laptops, tablets, smart phones, etc.), printing equipment, and all associated peripherals and software, and electronic mail accounts, regardless of whether the resource is used for administration, research, teaching, or other purposes.

POLICY

4.01 Principle of Least Privilege

It is the expectation of OSU all organizational units will implement a principle of least privilege regarding access control within their college, department, unit, or otherwise university affiliated area. The principle of least privilege states users will receive **no more access than is absolutely required** for each specific user to complete the responsibilities of their position or role within the university.

4.02 Access Control Procedures

All organizational units will develop and maintain access procedures specific to the systems under their control.

All credentialing for information access (credentials) will be controlled by provisioning and deprovisioning procedures.

All access to information systems and all credentials will be role-based, limiting access to only *authorized* (via access procedures) users according to the user's role within the University.

4.03 Password Complexity

Password complexity rules will be applied to all credentialing used to access information systems.

Password complexity rules will follow industry standards.

Legacy systems which do not allow for industry standard complexity requirements must use the maximum character and complexity allowed by the system.

4.04 Systems Configuration Expectations

All systems will be configured with reasonable session timeout rules which logoff a user or lock a system, and require re-authorization in order to continue use of the system.

All systems will be configured with appropriate audit logging based on data classifications and any state or federal law which would apply to the system audit.

4.05 OSU Network Access Controls

Information Technology will secure, regulate, and control University communications via network services which restrict access to University information assets and systems.

Network-based access controls may include, but are not limited to:

- restricting remote access to University systems; and
- restricting network traffic to or from specific ports, via certain protocols, or when identified as creating excess network burden or otherwise malicious patterns of network usage or behavior.

4.06 Privileged Accounts Access Management

Privileged accounts on information systems determined to be high impact, or otherwise considered critical to the overall functionality of the University's business structure, will be limited, reviewed, and/or audited to ensure access control integrity.

4.07 Sensitive Data Access

Access to data which is considered confidential/regulated (e.g., protected specifically by federal, state, or OSU rules and regulations and includes information requiring protection under contractual agreements) or otherwise meets the highest level of classification according to any University policies, standards or guidelines regarding data classification must be protected by strong access approval controls, such as, but not limited to:

- multi-factor authentication (MFA);
- formalized/documented access approvals by appropriate data custodian or steward prior to access provisioning; and
- access restrictions as a result of, or tracking, reporting, monitoring, and/or incident response procedures regarding, failed login attempts on University systems.

4.08 Non-Compliance

Non-compliance with this policy can impact the University in a variety of ways, including, but not limited to, breach of sensitive information, government sanctions, loss of accreditation, or hindrance of University business.

Any individual within the scope of this policy is expected to report policy violations or other behaviors constituting non-compliance of this policy to their immediate supervisor or an appropriate authority associated with the related college, department, unit or other affiliated campus organization.

If held responsible for a non-compliance violation, individuals can be subject to immediate revocation of privileges to use the University's computing resources and/or University disciplinary action, up to and including, discharge, dismissal, expulsion, and/or legal action, which may include referral for criminal investigation and/or prosecution.

Approved:
Staff Advisory Council, December 2019
Faculty Council, January 2020
Council of Deans, February 2020
E-Team, April 2020
Board of Regents, April 2020