| ACCESS CONTROL POLICY | 6-015<br>TECHNOLOGY SERVICES<br>December 2020 |
|---|---|

PURPOSE

1.01 With this policy, OSU Institute of Technology (OSUIT) sets in general terms the expectations and principles of access control, which apply at an institutional level, in order to control the 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 This policy applies to persons, whether students, staff, faculty, or authorized third-party users, within OSUIT 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.

2.03 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 such as contained in databases, spreadsheets, email, etc. or non-electronic, such as contained in paper files, publications, hardcopy research, etc. Data also include 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 school 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, servers, 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 OSUIT that all organizational units will implement a principle of least privilege regarding access control within their school, 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 Separation of Duties
Separation of duties acts as an audit and control standard that mitigates the risk of malicious or accidental compromise of system security. Individuals or support tier groups must not be able to control all parts of a transaction or business process. Employees must be tasked and permissioned such that multiple individuals or groups have oversight over IT processes in order to mitigate the risk of loss of integrity, confidentiality, and availability of the university's information assets.

4.03 Login Banner
Prior to being authenticated for access to any OSUIT system, each user must be presented a login banner informing them that by logging into this system the user is required to comply with all university policies and all laws concerning appropriate computer use. Users must be informed that they have no expectation of privacy and that access and activity on university systems and networks are monitored. This login banner must be accepted to be granted access to any system.

4.04 Access Control Procedures
All authentication to OSUIT computers and networks requires the use of O-Key username and password according to OSUIT User Password Creation Policy. All credentialing for information access (credentials) will be managed by provisioning and deprovisioning procedures. All shared access to information systems and all credentials will be role-based, limiting access to only authorized users according to the user's role within the university. Requests for access to confidential data are required to be approved by the supervisor at or above the director level (data custodian), who own the specific data. The access change requests made by these data custodians are stored in the OSUIT Service Desk portal and authenticated through Active Directory using login username and password. After approval by the Associate Vice President of Technology Services, these access requests are granted, implemented by Active Directory Group Policy, and documented in the change management system. Alerts must be in place to notify the Service Desk in the event of an unusual number of concurrent sessions using a single

user's credentials. Physical access provided by digital ID card access control follows the same provisioning process as the above logical access requests.

Upon separation or termination of employees, the Director of Human Resources will send an email to the OSUIT Service Desk requesting that an employee's active status and rights be removed by Technology Services. Technology Services, upon receipt of the email, will issue a block employee services request within O-Key. In the event of a change of position within the university, the Human Resources department creates and distributes a Transition List. When the Transition List is received, the Service Desk modifies roles and permissions as indicated. As an employee transitions into another role at the university, their global security group changes based on the employee's new department code. This change automatically changes the associated role-based access.

4.05 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. All authentication to OSUIT computers and networks requires the use of O-Key username and password according to OSUIT User Password Creation Policy. Direct access to network servers requires multi-factor authentication.

4.06 Systems Configuration Expectations
All systems will be configured with reasonable session timeout rules, not greater than 10 minutes of an idle session, which log off 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. All systems must notify the user, upon successful login, of the date and time of the last login attempt. Network device software versions must be updated to the latest versions per software vendor. The university firewall rules must start with a deny all by default posture, denying all inbound and outbound traffic. Firewall exceptions must be explicitly requested through the Service Desk management system and approved through OSU System change approval process prior to being configured and implemented on the OSUIT firewall. All patches to systems must be tracked, risks managed, exceptions recorded, and be approved first by the Infrastructure Administrator and then by the Associate Vice President of Technology Services.

4.07 OSUIT Network Access Controls
Technology Services 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.

Remote access, from outside the OSU and OSUIT network, must be accomplished using an encrypted VPN tunnel, authenticated by university credentials and use multifactor authentication. System level administrative rights to any OSUIT Technology Services servers are limited to

OSU System domain administrators and OSUIT Infrastructure Administrator, OSUIT Infrastructure Support Specialist, and OSU AVP of Technology Services.

4.08 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.

4.09 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;
• access restrictions as a result of, or tracking, reporting, monitoring, and/or incident response procedures regarding failed login attempts on university systems.

4.10 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 school, 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.

4.11 Policy Review
Due to the constantly changing state of information technology resources and the controls needed to mitigate emerging risks to information assets, this policy should be reviewed and updated annually, or earlier as emerging risks develop.

Approved: December 2020