Policy Title and #	CIO-072: IT Access Control and User Access Management				
Effective Date:	06/01/2002	Revision Date:	09/01/2021	Review Date:	09/01/2021

POLICY STATEMENT:

This policy establishes controls designed to protect access to information technology (IT) systems, applications, network resources, and data. The policy provides guidance in decision-making and practices to mitigate risk, protect the privacy, security, confidentiality, and integrity of the Commonwealth of Kentucky resources and data, and prevent unauthorized access to such resources.

DEFINITIONS:

NIST: National Institute of Standards and Technology

Access Control: The process that limits and controls access to a system, application, or network resources.

Users: Employees, consultants, contractors, vendors, temporary staff, volunteers, and other workers within state government.

System or Application Accounts: User Identifiers (IDs) created on IT systems or applications that have specific access privileges for those systems or applications.

Access Privileges: System permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

POLICY:

The Commonwealth Office of Technology (COT) and agencies shall restrict access to resources based on the principles of need-to-know and least privilege to ensure only authorized users have access to Commonwealth of Kentucky resources and data. Enterprise agencies shall adhere to access control standards outlined in the NIST 800-53 Revision 4 Access Control (AC) family in accordance with CIO-091 - Enterprise Information Security Program.

Agencies shall define and design IT access control and user access management standards and procedures in accordance with policies, procedures, and standards established by COT. For details on COT-approved access controls, refer to the Office of the Chief Information Security Officer's (CISO) Enterprise Security Controls and Best Practices.

Agencies may request exceptions to this policy by submitting a Security Exemption Request Form COT-F085 and submit the form to the Commonwealth Service Desk via e-mail at CommonwealthServiceDesk@ky.gov. The CISO will consider requests on a case-by-case basis.

AUTHORITY:

KRS 42.726 authorizes COT to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government. KRS 42.724 gives the Office of the CISO the responsibility to ensure the efficiency and effectiveness of IT security functions and responsibilities.

APPLICABILITY:
All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services must adhere to this policy. This includes employees, contractors, consultants, vendors, temporary staff, volunteers, and other workers within state government.

RESPONSIBILITY FOR COMPLIANCE:
Each agency must ensure that staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy.

MAINTENANCE:
COT's Office of the Architecture & Governance (OAG) and Office of the CISO share responsibility for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

REVIEW CYCLE:
COT's OAG and Office of the CISO shall review this policy at least every two years.

REFERENCES:
Helpful references can be found on the Enterprise IT Policies webpage.