PURPOSE

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

"Access Control" - means the process that limits and controls access to a system, application, or network resources.

"Access Privileges" - means system permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

"NIST" - means National Institute of Standards and Technology

"System or Application Accounts" - means user Identifiers (IDs) created on IT systems or applications that have specific access privileges for those systems or applications.

"Users" - means employees, consultants, contractors, vendors, temporary staff, volunteers, and other workers within state government.

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 5 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 completing a Security Exemption Request through Service Now. The CISO will consider requests on a case-by-case basis.

CORRECTIVE OR DISCIPLINARY ACTION

Each agency must ensure that all relevant 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.

APPLICABILITY

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government. Organizations may modify this policy to fulfill their responsibilities but must obtain approval through an exception request. Staff should refer to their internal policy that may have additional information or clarification.

REFERENCES

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