21 APR AUTOMATION
Security Governance

Resource	Description	Location
21APR Rules of Behavior	The Rules of Behavior provide the rules that govern the appropriate use of 21APR for all authorized users.	https://21apr.ed.gov/support
21APR Data Dictionary	This Data Dictionary is a technical dictionary providing the basic technical requirements for any variable built into the US Department of Education's 21st Century Community Learning Center's data collection system, 21APR	https://21apr.ed.gov/support
FISMA (Federal Information Security Management Act)	This framework requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.	https://www.dhs.gov/fisma
ED's Handbook for Information Assurance Security Policy	The purpose of this Handbook is to document and set forth the Department Information Assurance Security Policy, which establishes policies required to comply with Federal laws and regulations, thus ensuring adequate protection on the Department Information Technology resources.	https://www2.ed.gov/fund/contract/about/acs/acshbocio01.doc
Privacy Act of 1974	The Privacy Act of 1974 establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.	https://www.justice.gov/opcl/privacy-act-1974

Resource	Description	Location
Unauthorized Access Act	This Act protects the privacy of stored electronic communications, either before such a communication is transmitted to the recipient, or, if a copy of the message is kept, after it is delivered.	https://www.justice.gov/usam/criminal-resource-manual-1061-unlawful-access-stored-communications-18-usc-2701
OMB Circular A-130	This Circular establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices.	https://obamawhitehouse.archives.gov/omb/circulars_a130_a130trans4/
OMB Appendix III	This Appendix establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.	https://georgewbush-whitehouse.archives.gov/omb/circulars/a130/a130appendix_iii.html
NIST SP 800-47	The Security Guide for Interconnecting Information Technology Systems provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations.	https://csrc.nist.gov/publications/detail/sp/800-47/final

Resource	Description	Location
NIST SP 800-53 Revision 4	The Security and Privacy Controls for Federal Information Systems and Organizations provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional).	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
FIPS 200	The Minimum Security Requirements for Federal Information and Information Systems specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf