FRSECURE®

Cybersecurity Glossary for Schools

A Guide to Information Security Terminology

General Information

Users/titles in K-12

Students, teachers, staff, instructors, administration, school board, superintendent, principal, vice principal.

CIO, CTO, IT Leader, IT Director, assistant/associate superintendents.

FERPA

The federal education records law is a primary compliance focus.

The Family Educational Rights and Privacy Act (FERPA) is a federal law enacted in 1974 that protects the privacy of student education records. FERPA applies to any public or private elementary, secondary, or post-secondary school and any state or local education agency that receives funds under an applicable program of the US Department of Education.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

COPPA

COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

State-Level Privacy Acts

Although a there is not yet a comprehensive federal law that governs data privacy in the United States, several states have passed their own privacy laws and regulations to address growing security concerns. Some notable instances of this are the California Consumer Privacy Act (CCPA) and the Stop Hacks and Improve Electronic Data Security Act (NY SHIELD Act). These privacy laws vary based on region, and while they can be confusing to navigate, they are important to understand.

Osano.com keeps an up to date list of state-level privacy acts that is adjusted when new laws are passed, or existing laws are changed.

Language Variations

Training = Professional development

Fiscal year = School year (in US Education, that’s July 1-June 30)

Parts = Semester, quarter, etc.

Business/organization = District, or other agency (COE, BOCES, ESAs, DOEs, etc.)

Breach = Digital intrusion

Distributed/remote workforce = Hybrid/remote learning

Customers/clients, stakeholders = Parents/students

Common Term Definitions

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Availability

Ensuring timely and reliable access to and use of information.

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration settings

The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and /or functionality of the system.

External system

A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

CONFIDENTIAL INFORMATION: This document may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this document or the information herein is prohibited without prior permission of FRSecure.

External system service

A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External system service provider

A provider of external system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements (; licensing agreements; and/or supply chain exchanges.

External network

A network not controlled by the organization

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, transmits or stores or that constitutes a violation or imminent threat of violation of security polices, security procedures or acceptable use policies.

Information security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information technology

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

For the purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishings of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Integrity

Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Internal network

A network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (with regard to confidently and integrity). An internal network is typically organization-owned yet may be organization-controlled while not being organization-owned.

Least privilege

The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform it's function.

media Physical devices or writing surfaces including but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.

Multifactor authentication

Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN number, password); something you have (e.g., device, token, cryptographic identification device); or something you are (e.g., biometric).

Network

A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Privileged account

A system account with authorizations of a privileged user

Privileged user

A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Remote access

Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet)

CONFIDENTIAL INFORMATION: This document may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this document or the information herein is prohibited without prior permission of FRSecure.

Risk

A measure of the extent to which an entity is threatened by a potential circumstances or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. System-related security risks are those risk that arise from the loss of confidentiality, integrity or availability of information systems. Such risks reflect the potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the nation.

Risk assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management, risk assessment incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Sanitization

Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

Security control

A safeguard or countermeasures prescribed for a system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Security control assessment

The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for a system or organization.

System component

A discrete, identifiable information technology asset (hardware, software, firmware) that represents a building block of a system. System components include commercial information technology products.

User

Individual, or (system) process acting on behalf of an individual, authorized to access a system.