OIT Information Security Definitions and Terminology

Table of Contents

1.0 Purpose

This document serves as a repository for definitions of words, phrases, concepts, and terminology used throughout the various information security standards, policies, and documentation developed by the university.

2.0 Scope

The following definitions are only authoritative with regard to standards, policies, and documentation published/developed by the UAF/SW MAU's, but are available for use/adoption by the UA community in general.

3.0 Definitions

Access Control System

Physical, procedural and/or electronic mechanism that ensures that only those who are authorized to view, update, and/or delete data can access that data.

Authorization

The process of giving someone permission to do or have something; a system administrator defines which users are allowed access to the system and what privileges are allowed for each user.

Confidentiality

Confidentiality is an attribute of information. Confidential information is sensitive, contractually protected, or information whose loss, corruption, or unauthorized disclosure could be harmful or prejudicial.

Data Custodians

As defined in the UA Information Systems Security Policy, individuals who have been officially designated as being accountable for protecting the confidentiality of specific data that is transmitted, used, or stored on a system or systems within a department, college, school, or administrative unit of the UA and certain affiliated organizations.

Encryption

The process of turning readable text into unreadable (cipher) text, which requires the use of a decipher key to render it readable.

Ownership

This term signifies decision-making authority and accountability for a given scope of control.

Personally Identifiable Information

Personally identifiable information is defined as data or other information that is tied to, or which otherwise identifies, an individual or provides information about an individual in a way that is reasonably likely to enable identification of a specific person and make personal information about them known.

Personal information includes, but is not limited to, information regarding a person's home or other personal address, social security number, driver's license, marital status, financial information, credit card numbers, bank account numbers, parental status, sexual orientation, race, religion, political affiliation, personal assets, medical conditions, medical records or test results, home or other personal phone numbers, non-university address, employee number, personnel or student records, and information related to the UA Affirmative Action Policy.

OIT Information Security Definitions and Terminology

Principle of Least Privilege

Access privileges for any user should be limited to only what they need to have to be able to complete their assigned duties or functions, and nothing beyond these privileges.

Principle of Separation of Duties

Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse or other harm.

Privacy

An individual right to be left alone; to withdraw from the influences of his or her environment; to be secluded, not annoyed, and not intruded upon; to be protected against the misuse or abuse of something legally owned by an individual or normally considered by society to be his or her property.

Record

Recorded information, regardless of medium or characteristics, made or received by the university that is evidence of its operations, and has value requiring its retention for a specific period of time.

[State of Alaska Records Definition - AS sect 40.21.150(6)] "Record means any document, paper, book, letter, drawing, map, plat, photo, photographic file, motion picture film, microfilm, microphotograph, exhibit, magnetic or paper tape, punched card, electronic record, or other document of any other material, regardless of physical form or characteristic, developed or received under law or in connection with the transaction of official business and preserved or appropriate for preservation by an agency or a political subdivision, as evidence of the organization, function, policies, decisions, procedures, operations, or other activities of the state or political subdivision or because of the informational value in them; the term does not include library and museum material developed or acquired and preserved solely for reference, historical, or exhibition purposes, extra copies of documents preserved solely for convenience of reference, or stocks of publications and processed documents."

Security

An attribute of information systems practices that includes specific policy-based, procedural, and technical mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services and the confidentiality of sensitive information.

Sensitive Information

A general term for any information that requires access controls and other control measures to meet legal, policy and/or ethical requirements.

System

A network, computer, software package, or other entity for which there can be security concerns.

System(s) Owners

As defined in the UA Information Systems Security Policy, individuals within the UA community who are accountable for the budget, management, and use of one or more electronic information systems or electronic applications that support UA business, client services, educational, or research activities that are associated or hosted by the UA.

Users

Any individual that has been granted access and privileges to UA computing and network services, applications, resources, and information.

4.0 Inquiries & Information

For more information, questions, clarification, details regarding these definitions and any related documents, please visit OIT's Security Administration website at the following link.

http://www.alaska.edu/itsecurity