State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy Terminology Glossary

Contents

Authenticator

The means used to confirm the identity of a user, process, or device (e.g., user password or token).

Authorizing Official

Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.

Business Owner

The individual responsible for identifying business requirements, approving design and managing performance. Must be at an appropriately high level in the Organization and have authority to commit resources.

Client Agency

State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement.

Common Control Provider

An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).

Dark web

The Dark Web is a term that refers specifically to a collection of websites that exist on an encrypted network and cannot be found by using traditional search engines or visited by using traditional browsers.

Defense in depth

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

Employee

"Employee" means any person employed full-time, part-time, or pursuant to a contract and whose employment duties are subject to the direction and control of an employer with regard to the material details of how the work is to be performed.

Federal Information Processing Standard (FIPS)

A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

HIPAA Exchange

Any entity who is authorized to exchange electronic PHI at the federal, state or local level and is subject to the Minimal Acceptable Risk Standards for Exchange (MARS-E).

HIPAA privacy

The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

HIPAA security

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Honeynet

A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security.

Honeypot

Honeypots are fake computer systems, setup as a "decoy", that are used to collect data on intruders.

Incident Response Plan

A predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattack against State of Illinois Information Systems.

Information Owner

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security Architect (ISA)

Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.

Information Security Incident

A violation or imminent threat of a violation of information security policies, acceptable use policies or standard security practices. The definition of an Information Security Incident includes but is not limited to;

- attempts (either failed or successful) to gain unauthorized access to a system or its data;
- unwanted disruption or denial of service;
- discovery of network intrusions including bot-nets;
- malware events;
- the unauthorized use of a system for the processing or storage of data; changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent;
- unplanned, unauthorized or unexpected change to security baselines, including the unauthorized changes to security controls, technologies or processes;
- the inappropriate release of personal identifiable or other confidential information;
- theft or loss of information technology equipment which could contain information;
- violation of information security policies.

Information Security Incident Management

The capability to effectively manage information security incidents with the objective of minimizing impacts and maintaining or restoring normal operations within defined time limits.

Information System

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner (ISO)

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Security Officer (ISSO)

Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

Insider Threat

An insider threat is defined as a security threat that originates from within the organization being attacked or targeted, often an employee or officer of an organization or enterprise. An insider threat does not have to be a present employee or stakeholder, but can also be a former employee, board member, or anyone who at one time had access to proprietary or confidential information from within an organization or entity.

An insider threat is a threat that cannot be prevented by traditional security measures that focus on preventing access to unauthorized networks from outside the organization or defending against traditional hacking methods.

IT Resources

IT Resources are categorized as follows: Physical, Logical, and Communications. Physical resources include but are not limited to appliances, servers, desktop computers, portable computers, personal Information devices, and printers. Logical resources include computer software and data files digitally or optically stored as well as information itself. Communication resources include the capability to send messages either through the State internal network or via the Internet.

Least Privilege

Giving a user account only those privileges which are essential to perform job function.

Logical Access

The technical means (e.g. read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize information or information applications.

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 an information system.

Non-Organizational User

A user who is not an organizational user (including public users).

Organization

An entity of any size, complexity, or positioning within an organizational structure (e.g., an agency, board or commission or, as appropriate, any of its operational elements).

Organizational User

An organizational employee or an individual the organization deems to have equivalent status of an employee (e.g., contractor, guest researcher, individual detailed from another organization, individual from allied nation).

Personally Identifiable Information (PII)

Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

Physical Access

The physical ability, right or privilege to view, modify or make use of information by means of a physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Plan of Action and Milestone (POAM)

A document that “describes the measures that have been implemented or planned: (i) to correct any deficiencies noted during the assessment of the security controls; and (ii) to reduce or eliminate known vulnerabilities in the information system. The plan of actions and milestones document identifies: (i) the tasks needing to be accomplished; (ii) the resources required to accomplish the elements of the plan; (iii) any milestones in meeting the tasks; and (iv) scheduled completion dates for the milestones.

Privacy Impact Assessment (PIA)

An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Incident Response Plan

An incident response plan that only addresses incidents that relate to personally identifiable information (PII).

Risk Management Program

Risk Management allows an organization to allocate limited resources in a way that maximizes their return on investment and minimizes the susceptibility to breaches, disruption of services, and unauthorized disclosure of information.

Security Assurance

Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved.

Sensitive

Sensitive refers to information that would have an adverse impact on the State of Illinois if it were lost or compromised.

System Administrator

A person who manages the technical aspects of a system.

System Owner

Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

State Information

Any information used in conducting state business or in support of state services.

Technical User

Any authorized individual or entity assigned resource privileges by a Resource Custodian to administer, manage, develop or maintain an IT Resource for State operations.

User

Any person authorized to access State of Illinois IT Resources.