Information Security Glossary

Information Security Branch, Ministry of Central Services

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

This document provides definitions for terms used throughout the documentation published to the IT Security Services Taskroom.

Access Control:	Means to ensure that access to any information system resource is authorized and restricted based on business and security requirements.
Access Control List (ACL):	A list of permissions associated with an object; the list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.
Advanced Encryption Standard (AES):	A U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information.
AES-256:	An implementation of the Advanced Encryption Standard (AES) that uses a cipher key of 256 bits.
Application:	A software program hosted by an Information System.
Asset:	Hardware, software, network infrastructure and all forms of electronic information that has value to the government.
Audit:	Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established standards, policies and operational procedures.
Audit Log:	A chronological record of system activities; includes records of system accesses and operations performed in a given period.
Authentication:	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization:	The granting of access to resources in an information system by security controls to authenticated identities.
Availability:	A property of being accessible and usable upon demand by an authorized entity.
Backup:	A copy of files and programs made to facilitate recovery, if necessary.
Biometric:	A measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual; facial images, fingerprints, and handwriting samples are all examples of biometrics.

Chain of Custody:	A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.
Commercial-off-the-Shelf (COTS):	A software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public.
Confidentiality:	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Control:	The management, operational, and technical controls prescribed for an information system to protect the Confidentiality, Integrity, and Availability of the Information System and its information.
Countermeasure:	See “Control”.
Cryptographic Key:	A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.
Cryptography:	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
Detailed Infrastructure Design (DID):	A formal technical document which provides details on information system infrastructure design.
Digital Signature:	An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature; digital signatures provide authenticity protection, integrity protection, and non-repudiation.
Disaster Recovery Plan (DRP):	The procedures and information necessary to recover critical IT functions from any event that may interrupt an operation or affect service or program delivery, within the timeframes determined in the Business Impact Assessment.
Egress Filtering:	The practice of monitoring and potentially restricting the flow of information outbound from one network to another, typically from a private network to the Internet.
Electronic Messaging Services:	Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yielding a business-quality electronic mail service suitable for the conduct of official government business.

Electronic Storage Media:	Includes computer hard drives, memory sticks, CD ROM's, floppy disks, digital video discs, microcomputer tapes, microfiche, microfilm, point-of-sale credit card terminals, portable digital assistants (PDAs) or any other permanent electronic storage media; other storage media included are cellular phones with internal storage, film, video and audio tapes, or any other recordable media or devices with memory; Refer to *Electronic Storage Media Disposal Policy*.
Electronic Security Perimeter:	The logical or physical demarcation point between networks of differing security protection requirements, ownership or governance.
Employee:	A person appointed pursuant to The Public Service Act, 1998 Refer to *The Public Service Act, 1998*.
Encryption:	The process of changing plaintext into ciphertext for the purpose of security or privacy.
Event:	An identified occurrence of a system or service state indicating a possible breach of information security policy or standards or failure of safeguards, or a previously unknown situation that may be security relevant.
Executive Government:	Means the executive government of Saskatchewan; Refer to *The Executive Government Administration Act*.
FIPS 140-2 Validated:	A product or cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in Federal Information Protection Standard (FIPS) 140-2 (as amended). Validated modules are approved for the protection of Sensitive Information in the US Government and Protected Information in the Government of Canada. Refer to the *US National Institute of Standards and Technology (NIST)* discussing CMVP.
Firewall:	A gateway that limits access between networks in accordance with local security policy or standards.
Government Records:	Include all recorded information that relates to the transaction of government business, regardless of format (e.g. documents, maps, e-mails, photographs, etc.); Refer to *Saskatchewan Records Management Policy*. See also "Record".
Identification:	The process used to verify identities.
Identity:	A set of attributes used by an information system to represent an external agent, such as an individual, organization, application, or device.

Identity Management:	Enables the right individuals to access the right resources at the right times and for the right reasons.
Incident:	an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security standards, policies, security procedures, or acceptable use standards and policies.
Information Owners:	A role, defined by the Asset Management Security Policy, which is responsible for the safeguarding and classification of a particular set of information.
Information Processing Facilities:	Any information processing system, service, or centralized infrastructure, or the physical location housing it.
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 Security Event:	See “Event”.
Information Security Incident:	See “Incident”.
Information System:	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Injury:	The damage to the national interests and non-national interest that business activities serve resulting from the compromise of IT assets.
Integrity:	A property of accuracy and completeness.
Intellectual Property:	Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights.
Intrusion:	An information security incident involving unauthorized access to, or activity on, a computer system or network.
Intrusion Detection:	The process of monitoring activity occurring in a computer system or network and analyzing them for signs of possible events.
Key Management:	The processes for the generation, exchange, storage, safeguarding, use, vetting and replacement of cryptographic keys.

Least Privilege:	The security objective of granting users only those accesses they need to perform their official duties.
Local Admin:	In a Windows environment means unrestricted access to a specific computer.
Malicious Code:	Malicious code is designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, disclosing unauthorized information, corrupting information, denying service, or stealing resources. Types of malicious code include viruses, worms, Trojans, spyware and denial of service attacks.
Malware:	See "Malicious Code".
Media:	Devices onto which information is recorded, stored, or printed within an information system.
Media Sanitization:	The actions taken to render data written on Media unrecoverable by both ordinary and extraordinary means.
Ministry:	Means a ministry, department, secretariat, office or other similar agency of the executive government; Refer to *The Executive Government Administration Act*.
Mobile Device:	A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable data storage; and is powered-on for extended periods of time with a self-contained power source. *Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a Portable Storage Device, not a mobile device. See "Portable Storage Device".*
Monitoring:	Regular/ongoing check on aspects of operations to identify and correct deviations from policies and standards.
Multifactor Authentication (MFA):	Authentication using two or more factors to achieve authentication; factors include: something you know (e.g. password/personal identification number (PIN)), something you have (e.g., cryptographic identification device, token), or something you are (e.g., biometric).
Need-to-Know:	A requirement for a person to have access to particular information to perform his or her duties.

Network:	Information System(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Network Security Zone:	A logical entity containing one or more types of services and entities of similar security requirements and/or risk levels.
Network Segregation:	A logical entity containing one or more types of services and entities of similar security requirements and/or risk levels.
Network Service Agreement:	The contract or agreement between a service provider and a service consumer which defines the services to be delivered and the terms and conditions of delivery.
Non-repudiation:	Protection against an individual falsely denying having performed a particular action; provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
Personal Health Information:	personal health information as defined in *The Health Information Protection Act.* Refer to *The Health Information Protection Act*.
Personal Information:	personal information as defined in *The Freedom of Information and Protection of Privacy Act.* Refer to *The Freedom of Information and Protection of Privacy Act*.
Portable Storage Device:	Portable device that can be connected to an information system (IS), computer, or network to provide data storage. These devices interface with the IS through processing chips and may load driver software, presenting a greater security risk to the IS than non-device media, such as optical discs or flash memory cards. *Note: Examples include, but are not limited to: USB flash drives, external hard drives, and external solid state disk (SSD) drives. Portable Storage Devices also include memory cards that have additional functions aside from standard data storage and encrypted data storage, such as built-in Wi-Fi connectivity and global positioning system (GPS) reception.*
Privacy Impact Assessment (PIA):	a diagnostic tool designed to help organizations assess their compliance with the privacy requirements of Saskatchewan legislation; Refer to the *Office of the Saskatchewan Information and Privacy Commissioner*.
Privilege:	A right granted to an individual, a program, or a process.
Privileged User(s):	User(s) with permissions to alter access rights and structures of information systems; this includes (but is not limited to) system administrators, network administrators, database administrators, security administrators, web site administrators, system operators and network operators.

Record:	Means a record of information in any form and includes information that is written, photographed, recorded, or stored in any manner, but does not include a computer program or other mechanism that produces records; Refer to *The Archives and Public Records Management Act*. See also "Government Records".
Remote Access:	Access to an organizational Information System by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
Removable Media:	See "Portable Storage Device".
Risk:	Combination of the probability of an event and its consequence.
Risk Analysis:	The process of identifying the Risks to Information System security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.
Risk Assessment:	See "Risk Analysis".
Security Control:	See "Control".
Security Incident:	See "Incident".
Security Posture:	The security status of the government's or a service provider's networks, information, and systems based on resources (e.g., people, hardware, software, standards, policies) and capabilities in place to manage the defense of the government's information technology and information and to react as the situation changes.
Security Weakness:	A fault or deficiency in an application, procedure, process or associated technology that may result in a Security Incident.
Service Owners:	A role, defined by the Asset Management Security Policy, which is responsible for the safeguarding of a particular service.
Spyware:	Code with malicious intent that is secretly or surreptitiously installed into an Information System to gather information on individuals or organizations without their knowledge.
Statement of Sensitivity (SOS):	A formal document stating the classification of a particular set of information.
Telework:	Telework is the regular performance of work by an employee from a Teleworkplace. Refer to the *Human Resource Manual PS 1104*.
Threat:	Potential cause of an unwanted Incident which may result in harm to a system or organization.

Threat and Risk Assessment (TRA):	The evaluation of the nature, likelihood and consequence of acts or events that could place sensitive information and other assets at risk.
Trusted Path:	A network path that has been protected from eavesdropping, intrusion, and data tampering.
Uninterruptible Power Supply (UPS):	A backup power source for computers and computer networks to ensure on-going operation in the event of a power failure.
User ID:	Unique symbol or character string used by an information system to identify a specific user.
Virtual Private Network (VPN):	A logical network layer, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks.
Virus:	A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk.
Vulnerability:	Weakness of an asset or control that can be exploited by one or more threats.
Vulnerability Assessment:	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.