Australian National University

Glossary – Information Security

Purpose

To define terms used in Information security policies and procedures.

Term	Definition
Applications	A software program or group of software programs designed for end users. Examples of an application include a word processor, a spreadsheet, an accounting application, a web browser, an email client, a media player, a file viewer, an aeronautical flight simulator, a console game, or a photo editor. The collective noun application software refers to all applications collectively.
Antivirus	Software that is designed to detect, stop, and remove viruses and other kinds of malicious software.
ANU DISP location	The Physics Building (Building #160, 60 Mills Road, Acton ACT 2601)
Authentication	The act of verifying the identity of a user, process or device as a prerequisite to allowing access to resources in an information system. Includes authentication measures such as passwords, passphrases and multifactor authentication.
Automated tool	A piece of software that enables people to define software testing tasks, that are afterwards run with as little human interaction as possible.
Authorised user	A person who has been permitted access to all or part of the information infrastructure of the University by a responsible officer, as defined in the Information Infrastructure and Services Rule.
Availability	The period for which information assets are available, which ensures their availability for their intended use.
Break Glass Account	Break glass accounts provide access in emergency or disaster recovery situations, where all other users are locked out or unavailable.
Classifying	The categorisation of systems and information according to the expected impact if they were to be compromised.

Code	Program instructions
Credential(s)	A set of attributes that uniquely identifies a system entity such as a person, an organization, a service, or a device.
Data	Includes raw data, micro data, unorganised facts or data sets in any format.
Defence Industry Security Program (DISP)	The Defence Industry Security Program (DISP), managed by the Defence Industry Security Office (DISO), supports Australian businesses to understand and meet their security obligations when engaging in Defence projects, contracts and tenders. It is essentially security vetting for Australian businesses. Further information is available at https://www.defence.gov.au/security/industry.
Digital record	Is a record produced, stored, or transmitted by digital means rather than physical means.
Digitisation	Is the conversion of analogue materials into a digital format. It can relate to the processing of materials to make items accessible for future use. It also relates to digital-to-digital file conversion.
Disaster Recovery	A set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity.
DISP Personnel	Staff and students who are working on projects that require DISP membership.
Distributor	An agent who supplies goods to retailers.
Encryption	A cryptographic function used to ensure the confidentiality of data. The University considers an appropriate level of encryption to be the standards specified in the Australian Government Information Security Manual. See section “ASD Approved Cryptographic Algorithms”.
Exploit	A piece of code that exploits bugs or vulnerabilities in software or hardware to gain access to a system or network.
External Service Provider	A separate legal entity from ANU that provides services such as consulting, software development etc.
File format obsolescence	Vendors and creators of file formats can update their file formats with new versions, introducing compatibility issues; or they may withdraw support for a file format completely.

Foreign control	When a supplier, manufacturer, distributor, or retailer is subject to foreign government laws.
Hardware obsolescence	Computer hardware and storage components become out of date and support for these products may be removed.
Information	Data that is processed, organised, structured or presented in a given context so as to make it useful in any format.
Information communications technology (ICT):	An extensible term for information technology that stresses the role of unified communications and the integration of telecommunications and computers, as well as related enterprise software, middleware, storage, and audio-visual systems, that enable users to access, store, transmit and manipulate information.
Information infrastructure	Includes buildings, permanent installations, information services, fixtures, cabling, and capital equipment that comprises the underlying system within or by which the University: • holds, transmits, manages, uses, analyses, or accesses data and information; and • transmits electronic communication.
Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Information security risk	Associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organisation.
Information Technology Services (ITS)	Provides services and infrastructure to support and enhance teaching, learning, research, and administration within ANU.
Information Technology Team	As not all ANU systems are managed by ITS this is a more generic term.
ICT Equipment	Any device that can process, store or communicate electronic information (e.g. computers, multifunction devices, mobile phones, digital cameras, electronic storage media and other radio devices).
Integrated Communication Network (ICN)	The University network infrastructure including the following network sites – Acton Campus, ANU UniLodge, Hume Library Store, Gowrie Hall, Mount Stromlo Observatory, Siding Spring Observatory, North Australia Research Unit, University House Melbourne, ANU Medical School remote sites and hospitals, and ANU Exchange sites.

Java	A general-purpose programming language that is a class-based and object-oriented, and designed to have as few implementation dependencies as possible.
Least Privilege Security Model	Only give a user or group the minimum level of permissions needed to perform a given task.
Macro	An instruction that causes the execution of a predefined sequence of instructions.
Malicious code	Any software that attempts to subvert the confidentiality, integrity, or availability of a system.
Malware	Malicious software used to gain unauthorised access to computers, steal information and disrupt or disable networks. Types of malwares include Trojans, viruses, and worms.
Manufacturer	A person or company that makes goods for sale.
Media	A generic term for hardware, often portable in nature, which is used to store information.
Metadata	Structured data describing the context, content and structure of records and their management over time
Mitigation	A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities.
Multifactor Authentication	A security measure that requires two or more proofs of identity to allow a user to authenticate. Multifactor authentication typically requires a combination of something the user knows (PIN, secret question), something they have (phone, card, token) or something they are (fingerprint or other biometric).
Multi-Function Device (MFD):	ICT equipment that combines printing, scanning, copying, faxing or voice messaging functionality in the one device.
Network devices	ICT equipment designed to facilitate the communication of information.
Passphrase	A sequence of words used for authentication (e.g. pineapple Imagine 99).
Password	A sequence of characters or words used for authentication (e.g. ^Mhall.ifwwa*99btls). The use of the term password(s) also includes passphrase(s).
Patch	A set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities, improve service stability,

	resolve operational issues; or to provide feature enhancements.
Personal Identification Number (PIN)	A sequence of numbers used for authentication.
Privileges	A special authorization that is granted to particular users to perform security relevant operations.
Privilege accounts	An account that provides elevated access to ANU systems.
Privileged account management	Refers to managing and auditing accounts and data access based in privileges of the user. Often a privileged user has been granted administrative access to system to perform a work function. For example, to create standard user accounts.
Service	An ICT deliverable, product or component of an overall system. This includes ICT infrastructure, end-user computing devices, operating systems, applications, drivers and firmware.
Software obsolescence	The application or software which is needed to render file formats may change; and there may be withdrawal of support for software.
Standard users	Users who do not have privileged or elevated access to University systems, as defined in the Information technology account management and access procedure.
Supplier	A supplier, also known as a vendor, is a business entity or person that provides goods or services for sale.
System Owner	The senior member of staff with delegated responsibility for information assets including defined responsibilities for the security of the data, information and application component of the asset, determining appropriate classification of information, defining access rights, and ensuring that information asset risk is identified and managed. System owners are a Service Division Director or an equivalent management position.
Trusted Insider	Anyone who has intimate and legitimate inside knowledge of an organisation and how it operates. Using this knowledge, a trusted insider can undertake malicious and disruptive acts, including disclosing classified information and facilitating unauthorised access into facilities.
University provided storage infrastructure	Data storage systems that are provided by the University and supported by Information Technology Services (ITS).

User	A person (wherever located) who accesses the information infrastructure. This includes services intended for public use.
VaHA	Visiting and Honorary Appointments; formerly referred to as Persons of Interest (POIs).
Vendor	A supplier, also known as a vendor, is a business entity or person that provides goods or services for sale.
Vulnerability	A weakness in system security requirements, design, implementation, or operation that could be exploited.