# 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 includes 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 custom environment | ANU owned devices that have a custom, non-SOE setup. |
| ANU owned IT asset | IT assets purchased with ANU funds, including research grants, including assets received as an ANU staff member or student. This includes devices operating an ANU SOE or ANU custom environment. All ANU owned IT assets must meet the ANU Minimum Security Standard or have an approved exemption. |
| ANU Standard Operating Environment (SOE) | ANU owned devices that use an SOE image (previously known as "ANU managed"). |
| Authentication | Verifying the identity of a user, process, or device as a prerequisite to allowing access to resources in a system. |
| 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 | Any appropriately cleared individual with a requirement to access an information system (IS) for performing or assisting in a lawful and authorized government function. |
| Availability | The assurance that systems and information are accessible and useable by authorised entities when required. |
| Break Glass Account | Break glass accounts provide access in emergency or disaster recovery situations, where all other users are locked out or unavailable. |
| Bring Your Own Device (BYOD) | The use of any personally owned electronic device not owned or leased by the University, to access the University’s IT services, data, or networks. This includes, but is not limited to, mobile phones, smartphones, tablets, laptops, notebooks, and portable storage devices. |
| Business Owner | The senior member of the staff with delegated responsibility of overall direction and management of the relevant business unit. This is usually at a D2 or D3 delegation level as per the [ANU Delegations Framework](https://services.anu.edu.au/planning-governance/governance/delegations).  Their defined responsibilities include strategic direction, managing financial aspects, overseeing operations, high level decision making and ensuring the business complies with laws and regulations. |
| 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 | The basic element that can be processed or produced by a computer to convey information. |
| Digital record | Is arecord 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. |
| Distributor | An agent who supplies goods to retailers. |
| Encryption | The conversion of electronic plaintext data into unreadable ciphertext using algorithms. Encryption protects the confidentially of data at rest and in transit. Both encryption and decryption are functions of cryptography. |
| 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 | Aseparate 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 | Is 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. |
| Highly sensitive data/ systems | As defined in the [Information and Data Classification Standard](https://policies.anu.edu.au/ppl/document/ANUP_6750451) – data and the systems that host that data that would cause a high impact (significant risks or liabilities) to the University, staff or students if disclosed (e.g. medical information, passport information, personal financial details), |
| Information | Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual. |
| 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 | 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 risk | The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. |
| 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, The University UniLodge, Hume Library Store, Gowrie Hall, Mount Stromlo Observatory, Siding Spring Observatory, North Australia Research Unit, Kioloa campus, The University Medical School remote sites and hospitals, and The University 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. |
| 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 | Descriptive information about the content and context used to identify information. |
| 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 method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). |
| 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). The use of the term password(s) in this policy does not include Personal Identification Numbers (PINs). |
| Patch | A piece of software designed to remedy security vulnerabilities or improve the usability or performance of software and ICT equipment. |
| 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. |
| Privileged account | An information system account with approved authorizations of a privileged user, such as elevated access to ANU systems. |
| Privileged account management | Refers to managing and auditing accounts and data access based on privileges of the user. |
| Privileged user | A user who is authorized (and, therefore, trusted) to perform security-relevant functions that standard users are not authorized to perform. Often a privileged user has been granted administrative access to a system to perform a work function. For example, to create standard user accounts. |
| Sensitive data/ systems | As defined in the [Information and Data Classification Standard](https://policies.anu.edu.au/ppl/document/ANUP_6750451) – data and the systems that host data that would cause medium impact to the University, staff or students if disclosed (e.g. identifiable staff or student data, financial data). |
| Service | A set of related IT components provided in support of one or more business processes. 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 Operating Environment (SOE) | A standard operating environment, or a specific computer operating system and collection of software that an IT department defines as a standard build. |
| Standard user | A user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass security measures. |
| Supplier | A person or organisation that provides a product or service. |
| System Owner | Person or organization having responsibility for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of an ICT system. |
| 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 | An individual that is authorised to access a system. |
| VaHA | Visiting and Honorary Appointments; formerly referred to as Persons of Interest (POIs). |
| Vendor | A commercial supplier of software or hardware. |
| Vulnerability | A weakness in system security requirements, design, implementation, or operation that could be exploited. |