

NOTICEBORED

Glossary

Identity theft terms

Click the hyperlinked (underlined) terms for further explanations.

Term	Meaning
Authentication, authenticate	Process by which an individual user, system <i>etc.</i> is positively identified by another, typically on the basis of something they know (e.g. a password) and sometimes something they have (e.g. a security token such as SecureID) or something they are (biometrics).
Biometric	Measurable physical characteristic of a person, such as a fingerprint, iris pattern, retinal patter, facial shape or voice pattern, that can be used to identify the person positively.
Digital certificate	File containing information about a user or system along with their public key plus a digital signature from the Certification Authority to authenticate the whole certificate.
Digital signature	Cryptographic hash of a message, constructed with the sender's private key, used to 'seal' the document thus revealing any subsequent changes and authenticating it.
Encryption	Application of cryptography to make information unintelligible to anyone without access to the correct key.
Information asset	Computer system, data, database, knowledge <i>etc.</i> <i>i.e.</i> valuable IT technology equipment and/or information content that requires protection against information security risks.
Information Asset Owner (IAO)	Manager held accountable for one or more information assets such as business application systems (hardware, software, data and processes). They define and/or approve appropriate information security controls for the assets , authorize access and monitor the effectiveness of the controls.
Integrity	Property of completeness and accuracy of data, IT systems <i>etc.</i> Protected through controls such as referential integrity, data entry validation , honesty, ethics and trust. One of the three core elements of information security, along with confidentiality and availability.
Logical access control	Automated information security control protecting electronic information assets (data/program files, directories, disks, tapes <i>etc.</i>) against access by unauthorized users, programs or systems.
Malware	Contraction of "malicious software" meaning programs written and circulated with malicious intent such as viruses , worms, Trojans , rootkits, logic bombs <i>etc.</i>

Term	Meaning
Passphrase	A secret phrase or saying that is either used directly as a password , or is used to recall one (e.g. using initial letters of the words).
Password	A secret string of characters that should only be known by one person and can therefore be used to authenticate them to a computer system.
Perimeter	The outermost physical and/or logical boundary around a collection of assets , such as the network perimeter dividing <ORGANIZATION>'s internal network from the Internet and other external networks.
PIN (Personal Identification Number)	Numeric password used on systems with numeric keypads instead of full alphanumeric keyboards.
Security Administration	<ORGANIZATION> information security function responsible for administering userIDs , passwords , access to applications <i>etc.</i>
Segregation of duties	Duties (activities at different stages of a process) are divided amongst several individuals.
Trojan	Contraction of "Trojan horse program" that may appear to the user to offer a useful function or to do nothing, but in fact contains hidden functions such as the ability for remote access by hackers; a form of malware .
UserID	User identifier or user identity, also known as a username, login name, computer account <i>etc.</i> ; this is a label used to identify a user and their activities on the system so that they may be controlled by logical access controls , logged in log files <i>etc.</i>
User Rôle	Logical access rights are standardized by defining and assigning minimal access rights necessary for users in certain job functions to perform their rôles within <ORGANIZATION>.
Valid	State of being true, accurate, complete <i>etc.</i>
Validation	Process to check whether something is valid .
Virus	Computer program that self-replicates and automatically spreads between systems; usually contains a "payload" that performs unauthorized functions such as deleting or modifying files <i>etc.</i> ; a form of malware .
*** End of glossary ***	

For more information

For advice on this issue, talk to your line manager first of all. IT Help Desk or Information Security can provide further information on request and you are always welcome to visit Information Security's intranet website.