

S

Security and Privacy of Information Technology Management Systems



Javier Osorio and Julia Nieves
Universidad de Las Palmas de Gran Canaria,
Las Palmas de Gran Canaria, Spain

Synonyms

[Data protection](#)

Definition

Information security is usually defined as a feature of information systems management which involves three main aspects, named confidentiality, integrity, and availability (Lov om behandling [2000](#); ISO/IEC 27002:2005 [2005](#); ISO/IEC 27000:2009 [2009](#)). Usually, quality is included as a fourth aspect of information security, although it can be considered as overlapping with integrity. The following is a brief definition of these items: (a) Confidentiality is the guarantee that information is not made available or disclosed to unauthorized persons, entities, or processes; (b) integrity relates to the trustworthiness of the information, thus assuring that data has not been deliberately tampered with, nor accidentally changed; (c) availability means that information is accessible and can be utilized upon demand by an

authorized entity; and (d) quality refers to the information being correct and not misleading. Among the aforementioned aspects, confidentiality is particularly important because of the sensitivity of personal information. Associated with security, privacy emerges as an issue because of the right to privacy with respect to the processing of personal data. In this way, regarding the relationship between security and privacy, the latter could be defined as the right of the client and the former the duty of the service provider (Henriksen et al. [2013](#)).

Security

Introduction

The security of information technology (IT) is a matter of great importance for organizations. One important reason is the continued use of IT by different stakeholders and the large amount of information stored, sometimes critical to the organization or its customers. Education centers are not oblivious to this type of problem, with the main characteristic being that the clients, in this case, are the students who study at the center, and the sensitive information is of a mainly personal nature (Culhane et al. [2018](#)). Thus, the management of education centers is faced with a problem for which they are responsible as top management of the organization but for which they have often not received training. Many of the aspects related to the assurance of information security are

fundamentally based on technical issues, with which many school directors feel uncomfortable. However, this lack of knowledge or discomfort cannot be a pretext for neglecting this important aspect of the management of information systems (Weng and Tang 2014). The directors and top managers of education centers and institutions must be aware of the implications of guaranteeing the security and privacy of the information they are responsible for as leaders of their organizations.

Education centers, regardless of the level of education they provide (primary, secondary, or higher education), which utilize information technology (IT) infrastructure must guarantee its normal functioning, especially when a large part of their daily operations is based on the use of information systems and technologies. Errors and cyberattacks, both internal and external, can prevent its proper functioning. For this reason, it is crucial to have a security policy that includes actions to prevent errors or attacks from affecting the technological infrastructure. However, this policy should not be considered as optional since there are issues related to the safeguarding of privacy which are protected by law. Therefore, this issue becomes a mandatory element in the agenda of decisions and activities of those responsible for education centers and institutions (Brockmeier et al. 2005). In addition, the problems that education centers encounter in this area, although in many cases they are public, non-profit institutions, are the same as those faced by companies and organizations of all kinds that make use of information systems and technologies as part of their daily activities. The above is, however, an opportunity for schools because advantage can be taken of the great volume of knowledge generated in terms of the security and privacy of information systems and technologies in the business field.

The main aspects that should be considered in terms of the security of information systems within any organization, and therefore in educational organizations, are the following (CAP Gemini 2000): (i) errors due to a malfunction of hardware or software, (ii) errors due to IT users, (iii) natural catastrophes, (iv) unauthorized access

by external or internal personnel, (v) deliberate damage done by staff or by strangers, and (vi) deterioration due to aging or everyday use of infrastructure.

Policies and Procedures

Establishing policies and procedures related to the security of the IT infrastructure is a key issue that managers of any type of organization must face. The significance of this issue increases in environments where computers are connected through communication networks, whether internal or external. In this situation, to the physical threats are added the risks that arise through communications, either in the form of unauthorized deliberate access or by the introduction of harmful software (viruses) into the system.

Each organization should establish a security policy and communicate it to all staff. The policy should be the result of an analysis of the potential risks to which the organization may be exposed. The purpose is to protect the assets of the organization, in this case, data and information about the different stakeholders of the education centers; for this objective, the collaboration of those affected should be encouraged, i.e., teachers, administrators and technicians, as well as parents and students. The security measures must be coherent, and a key factor in obtaining the commitment to execute security procedures is to make them practicable. The people involved will most likely not accept procedures that make their work practically impossible and, if this were the case, in all likelihood they would end up using their time and ingenuity to bypass such controls. Therefore, impractical conditions raise the risks instead of decreasing them. The IT infrastructure cannot be protected by technical means alone; it is also necessary to have a security plan with the guarantee that people involved in IT are aware of and act to adhere to the general security policy (Culhane et al. 2018).

The responsibility for security matters rests with the management of the center and, in the case of delegation, the person in charge of the IT department, assuming there is one. The responsibilities that are acquired include (i) the prohibition of the use of unauthorized software, (ii) the

implementation of the physical security process, (iii) the availability of procedures that prevent unauthorized access to the center's IT systems, and (iv) responsibility for the integrity of the data. One of the most important missions of the IT infrastructure security manager is to raise security awareness in all stakeholders. This is because success in this matter depends on procedures being followed, and this is only possible when there is full awareness. For this to be achieved, a culture of security must be created, which can be materialized through campaigns based on messages and information on this issue. The staff of the center in direct contact with IT must be the first recipients of this type of message, in which the need to protect the information and the IT infrastructure used in the center must be highlighted, as it is part of their work routine and, therefore, fundamental to the correct development of teaching tasks.

A very useful tool for checking the security of the IT infrastructure at the center consists of the regular practice of auditing the procedures and their level of effectiveness in terms of computer security. Essential aspects to evaluate as part of the audit include (CAP Gemini 2000) (i) access controls to the IT systems, (ii) physical access controls to the facilities in which the electronic devices are located, (iii) protection against physical threats, (iv) data integrity controls, (v) generation of backup copies, and (vi) security awareness procedures. The following is a set of factors recommended for consideration in defining security procedures. They cover a wide range of cases, and it must be the director or head of security of the center who establishes the degree of development of each one of them (for a greater development of the concepts, it is recommended to go to a computer security manual published by consultants or IT manufacturers).

Physical security. The protection of the IT infrastructure depends on the physical conditions in which computer systems and communication networks operate. There are also other risks, such as fire and flood, that are beyond the physical characteristics of the IT infrastructure, but that need to be considered. The storage of

documentation and magnetic supports deserve special mention due to the importance of ensuring their protection. Aspects to take into consideration related to physical security are electrical protection, fire risks, natural catastrophes, urban disorders, and buildings and facilities outside the center susceptible to generating hazards (gas stations, bus stations, high density traffic routes, railways, etc.).

Physical access. One way to ensure security is by restricting access to the room in which sensitive equipment is located, such as servers or communication racks. Access to this equipment allows control over the system, so protocols should be established to prevent unauthorized personnel from accessing the equipment. Access by authorized personnel should also be monitored. Aspects to take into consideration related to physical access are security controls in the areas of access to sensitive equipment, the use of booths or security boxes to store documentation and magnetic backup media, and security keys and protocols for control of access for both internal and external personnel (maintenance technicians).

Access to computer applications. Access by an unauthorized person to the information systems housed in an education center is a crime, and, as such, those who commit it can be reported and prosecuted. However, education center managers must articulate policies and procedures, directly or through specialized technical services, internal or external, to protect the IT infrastructure from unauthorized access. The nature of the information available in the center's databases and applications, and the possibility of accessing them through internal and external networks, makes this a critical point of IT security. The main requirement is to develop mechanisms that ensure that only authorized users can access computer systems with user identifiers and defined passwords. The first, identifiers, constitute a main component of computer security. It should apply to both people and terminals. Each user must have an identifier to control their access rights, privileges,

available resources, and access to sensitive information. For this reason, user identifiers must be assigned individually. The second key mechanism to ensure that no unauthorized person accesses the information systems of the center is the use of passwords. As far as this question is concerned, a password policy should be established, known to the users of the systems, which includes the characteristics of the password itself (length, type of characters) and the duration of its validity.

Installation of unauthorized software. The installation and use of unauthorized software pose many risks, both for potential infringement of intellectual property rights and for facilitating security breaches. Many unauthorized downloads come from internal personnel or from the organization's suppliers of IT equipment. It is often the case that the staff of education centers, whether due to dissatisfaction, boredom, or other reasons, add their own software to compulsory use programs for purposes unrelated to the requirements of their work. This software can lead to easy entry into sensitive parts of the information system, unauthorized operations (e.g., Trojan horses), or the installation of computer viruses into the center's systems. Installation of unlicensed software can damage the reputation of the organization if it is made public that this type of software is being used. The center can only be protected against such threats when users only make copies of the licensed software or obtain copies from external sources through control procedures. All users' computers should be audited and clear guidelines must be set to establish exactly which software applications can be approved for installation.

Network security. The systems are usually connected through communication networks, both internal and external through the Internet, which generate threats to security. The risk comes from, among other sources, unauthorized access from outside and the installation of malicious software that may negatively affect the proper functioning of the IT infrastructure. The use of encryption

systems, passwords, and advanced authentication systems through digital signature, firewalls, antivirus programs, etc. can decrease, although not avoid entirely, the potential risks derived from the use of communication networks. One of the least known forms of risk regarding the use of networks, especially the Internet, is the infringement of intellectual property. This could be the case regarding the information shown on the education center's official website. In this sense, part of the information present on the website may come from sources that are the intellectual property of third parties. On the other hand, there may be teachers or staff from the center who use material obtained on the Internet with registered copyrights. In this sense, it is important that all members of the organization become aware of the potential dangers of violating intellectual property laws, in addition to those mentioned above on safety.

Privacy

Definition

Privacy in the field of IT is understood as limiting the use of information systems to guarantee the honor and personal and family privacy of citizens and the full exercising of their rights (Schwartz 2004). Under this definition, of a broad nature, some related aspects can be circumscribed, such as (i) personal data, referring to all information about an identified or identifiable person, that is, whose identity can be determined directly or indirectly; (ii) processing of personal data, which is any operation or set of operations carried out (or not) by automated procedures and applied to personal data, such as collection, registration, modification, consultation, communication, suppression, or destruction; and (iii) personal data file, i.e., a structured set of accessible personal data according to certain criteria, whether centralized or decentralized.

Introduction

The use of modern means of information processing and communication, with a huge capacity

to process information of all kinds, has given rise to a growing concern for the security of IT infrastructure, mainly because of the damage that can be caused to the functioning of the organization derived from fraudulent access or use. However, it should not be forgotten that much of the information that is stored in the information systems is personal, that is, it affects personal privacy and the freedom to make decisions regarding the automation and transmission of personal data. Therefore, the security of IT infrastructure and privacy are two closely related areas, and each must be considered as complementary to the other in the management of IT. For the specific case of educational centers, it is a function of educational management teams to ensure that not only are security policies and procedures established, but also that compliance with privacy requirements is ensured, given that there are numerous laws that establish compliance with minimum requirements which, if not met, is considered a crime.

Privacy or data protection is an issue that has acquired a high profile as a consequence of the continuous development of information processing systems, as well as the transmission of information through all types of networks. The right to personal privacy, which can easily be violated through these devices, has led to growing interest. This issue has been, for a long time, the remit of the courts, materializing in a series of national or supranational laws on the protection of the privacy of individuals' information. For educational managers, this question is of great importance because in schools there is a very sensitive group, namely, students. A large amount of personal or other information (academic, attitudinal, aptitude) is handled by these organizations, and irresponsible use of it is not only subject to sanctions but can also cause great moral damage. When dealing with information about minors in the case of schools, these considerations are all the more critical.

The set of terms and procedures related to privacy acquires special relevance in the figure of the controller, which is the person or public authority responsible for determining the purposes and means of processing personal data. Educational management teams have, therefore,

the maximum responsibility in this matter and are in charge of establishing the procedures and policies that have to be communicated to all the members of the organization for compliance with the privacy directives (Akbaba-Altun and Güler 2008).

Legal Basis

Electronic communication and the storage of personal information are subject to national legislation and, in some cases, such as with European legislation, to supranational legislation. Examples of this are the EU directive on the processing of personal data for the countries of the European Union (Directive 95/46/EC 1995) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States (Health Insurance Portability and Accountability Act 1996). Standardized procedures compiled as international ISO standards on best practices for the establishment of information security techniques and IT have also been developed (ISO/IEC 27002:2005 2005; ISO/IEC 27000:2009 2009).

Recommended Actions for Managing the Privacy of Information in Educational Environments

The work of the management consists, first of all, of establishing the necessary technical and organizational measures that must be implemented for personal data files, equipment, and information systems, as well as ensuring that the people who intervene in the processing of this data comply with the privacy requirements as established by law. The recommendations established in the ISO standards on information technology security techniques are also useful for this function. The person in charge of the treatment of information is the director of the educational center, who, in the case that they need support for these functions, can formally delegate the function of coordinating and controlling the required security and privacy measures (Wilk 2016). The following is a summary of recommended actions:

Security document. A first action in this matter is the development and implementation of

security regulations to ensure the privacy of information. This is done through a mandatory document for staff with access to automated personal data and information systems. Said document should contain the following aspects: (i) scope of application, with detailed specification of the protected resources (automated data files, equipment, systems, programs, people intervening at some stage of the process); (ii) standards and procedures to guarantee the required level of security; (iii) staff functions and obligations; (iv) structure of the files with personal data and description of the information systems that treat them; (v) procedure for notification, management, and response to incidents; and (vi) procedures for making backup copies and for data recovery. The document must be updated and revised whenever there are relevant changes to the information system or to the organization thereof. Its content must be adapted at all times to the current legal provisions regarding the security of personal data.

Functions and obligations of the staff. The functions and obligations of each person with access to personal data and information systems will be clearly defined and documented. The personnel must know the safety regulations that affect the performance of their functions, as well as the consequences that could be incurred in case of non-compliance.

Incident registration. The notification and incident management procedure will necessarily contain a record stating the type of incident, the time it occurred, the person making the change, who is notified, and the effects that would have been derived.

Identification and authentication. The personal data security officer will ensure that there is an updated list of users who have authorized access to the information system and establish identification and authentication procedures for said process.

Access control. The users will have authorized access only to the data and resources that they need for the development of their functions. In this sense, within the scope of teaching activities, teachers should be prevented from

accessing sensitive personal data if it is not for a justified reason that affects the exercising of their teaching duties, in which case it will have to be done through a formal request. The information handled by teachers, in general terms, must be of an academic nature. Similarly, the administration staff, who habitually work with the personal data of students and their families, should have some kind of restriction on access to academic performance data. The officer responsible for the file will establish mechanisms to prevent a user from accessing data or resources with rights other than those authorized.

Management of data storage devices. The electronic devices that contain personal data must be able to identify the type of information they contain and be inventoried and stored in a place with access restricted to the personnel authorized as set in the security document. The movement of electronic devices that contain personal data outside the premises in which they are stored may only be authorized by the person responsible for the file.

Backup copies. A procedure for making backup copies and recovering data must be established. These procedures must guarantee their reconstruction in the state in which they were at the time of the loss or destruction. Backup copies should be scheduled periodically, at intervals that depend on the volume of updated data.

Summary

The right to information privacy and the security of the IT infrastructure is a matter of great importance that, however, has not traditionally received enough prominence in the agenda of educational managers. Among the set of functions assigned to educational managers are also included those involved in information management and IT. Education centers generate and store a large amount of personal information, which can have negative implications for people's lives if they are misused. The laws on data protection and the right to privacy oblige educational managers to establish

security protocols to safeguard people's right to privacy. For this reason, educational managers must assume this responsibility as part of their work. For this, they can rely on qualified personnel and on the wide range of recommendations and guides developed by national and international companies and organizations on information security and IT infrastructure. Each education center, according to its circumstances, must elaborate and comply with a security policy which is known to all the people who work at or have a relationship with the center and which includes coherent and practicable security measures.

Cross-References

- [Ethics](#)
- [Human, Social and Ethical Aspects of IT Management Systems](#)
- [Online Safety](#)

References

- Akbaba-Altun S, Güler MD (2008) School administrators' perceptions of their roles regarding information technology classrooms. *Eurasian J Educ Res* 33:35–54
- Brockmeier LL, Sermon JM, Hope WC (2005) Principals' relationship with computer technology. *NASSP Bull* 89 (643):45–63
- CAP Gemini (2000) Factbook of information technology. Aranzadi & Thomson, Navarra
- Culhane D, Fantuzzo J, Hill M, Burnett TC (2018) Maximizing the use of integrated data systems: understanding the challenges and advancing solutions. *Ann Am Acad Pol Soc Sci* 675(1):221–239
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The European Parliament and the Council of the European Union; 1995. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>. Accessed 15 Nov 2017
- Health Insurance Portability and Accountability Act of 1996 (HIPAA). US Department of Health & Human Services; 1996. <http://aspe.hhs.gov/admsimp/pl104191.htm>. Accessed 15 Nov 2017
- Henriksen E, Burkow TM, Johnsen E, Vognild LK (2013) Privacy and information security risks in a technology platform for home-based chronic disease rehabilitation and education. *BMC Med Inform Decis Mak* 13:85
- ISO/IEC 27002:2005 (2005) Information technology – security techniques – code of practice for information security controls. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), http://www.iso.org/iso/catalogue_detail?csnumber=50297. Accessed 14 Jan 2018
- ISO/IEC 27000:2009 (2009) Information technology – security techniques – information security management systems – overview and vocabulary. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), http://www.iso.org/iso/catalogue_detail?csnumber=41933. Accessed 14 Jan 2018
- Lov om behandling av personopplysninger [personopplysningsloven]. (Norwegian Act of 14 April 2000 no. 31 relating to the processing of personal data [Personal Data Act]). Det norske justis- og beredskapsdepartement (Norway's Ministry of Justice and Public Security) (2000). <http://www.lovdato.no/all/hl-20000414-031.html> (English version: <http://www.ub.uio.no/ujur/ulovdata/lov-20000414-031-eng.pdf>). Accessed 26 Feb 2018
- Schwartz PM (2004) Property, privacy, and personal data. *Harv Law Rev* 117(7):2055–2128
- Weng CH, Tang Y (2014) The relationship between technology leadership strategies and effectiveness of school administration: an empirical study. *Comput Educ* 76:91–107
- Wilk A (2016) Cyber security education and law. In: Proceedings – 2016 IEEE international conference on software science, technology and engineering, Article number 7515415, IEEE, Beer-Sheva, Israel, <https://doi.org/10.1109/SWSTE.2016.21>, pp 94–103