ZESZYT NAUKOWY
Wyższa Szkoła Zarządzania i Bankowości w Krakowie

Tomasz Szubert
Dr Tomasz Wojdyński
Faculty of Management, Finance and Computer Science
The School of Banking and Management in Krakow

LEGAL ASPECTS OF INFORMATION SECURITY MANAGEMENT IN PUBLIC ADMINISTRATION

Abstract

The security assurance of data and information is a key challenge for companies in the 20th and 21st centuries. Due to a widespread use of IT and the IT supported storage and processing of data, the issue concerns mainly the new technologies. Legal regulations, norms and good practices that are included in various management methodologies constitute signposts when analyzing and solving the complexity of the issue. The results of the analysis of these documents from the point of view of particular public administration entities or companies that protect their resources should be given in a document referred to as the Information Security Policy

Introduction

Nowadays, information security policy is a key factor that ensures efficient and safe operation of companies. The threat that the data, both in a paper or digital form, are endangered by theft, falsification or destruction is increasing with the growing volume of information to be processed in organizations and with the development of technologies.

Information is endangered both by external factors, such as hackers, computer viruses, thefts, and internal ones - the loss of data as a result of improper protection, the lack of backup copies or the loss of a flash drive that contains unprotected data. An improper protection of data may result in the loss of company's reputation, its customers' trust or in financial losses. This issue is of particular importance as regards the court system due to the volume of personal data that are processed and stored in courts and their unique character (sentences, orders, statements of reasons, convictions, personal details of victims or land registers). They all constitute information that must be protected against theft, loss or alterations. The loss of data could affect negatively the trial and the judicial independence by possible external pressure in cases where data was lost.

The aim of the article is to review and identify key legal factors that are crucial as regards information security in public administration.

1 Polish and international standards regarding information security

Information security is not only the standard and necessity but also the obligation of companies and organizations in Poland[1]. Organizations have always been exposed to offense or the possibility that their employees will make mistakes. However, because of the new technologies used by organizations, the scale of the danger has increased nowadays. The present-day information systems do not only play a supportive role but they also constitute an integral and crucial element of organizations[2]. In order to prevent against such negative phenomena, Security Policy should be introduced and implemented. The Policy is a general schedule or plan of action that aims at achieving adequately high security levels of company IT, ICT and data protection systems through appropriate administrative decisions. It defines a set of regulations and conditions that regard the ways of information management, protection and sharing[3].

The management of every organization is obliged to protect the information and the processed data, either in a paper or digital form. In the case of the court system the obligation is upon the presidents of courts, which is stipulated by the regulation of the Minister of Justice of 27 June 2012 on the implementation of Information Security Policy of the Ministry of Justice and common courts.

In the course of the development of the Security Policy, in order to avoid the omission of any important security aspects, Polish and international standards should be followed. The most essential standards are:

- PN ISO/IEC 27001:2007 Information technology – Security techniques – Information security management systems – Requirements.
- PN-ISO/IEC 17799:2007 Information technology – Security techniques – Information security risk management.
- PN-ISO/IEC 17799:2007 Information technology - Security techniques – Practical principles for information security management.

[1] http://www.iniejawna.pl/pomoce/ensi.html, (accessed: 10.05.2015).
[2] F. Wołowski, *Bezpieczeństwo systemów informatycznych*, edu-Libri, Kraków-Warszawa 2012, p. 15.
[3] J. Stokłosa, *Bezpieczeństwo danych w systemach informatycznych*, PWN, Warszawa 2001, p. 15.

- PN-I-13335 Information technology – Guidelines to information security management.
- PN ISO/IEC 20000-1:2007 Information technology – Service management part 1: Specification.
- PN ISO/IEC 20000-2:2007 Information technology – Service management part 2: Code of practice.

The PN ISO/IEC 27001:2007 standard defines the requirements regarding the development of information security management systems (ISMS) and it constitutes the basis for their assessment. The objective of the standard is to present the necessary and adequate measures that should protect personal, physical and information security in line with current legal regulations. It defines areas that should be regulated; however, the application of particular technical means depends directly on the organization itself. Normative appendix A includes 11 areas that are required to be fulfilled:

- information security organization,
- asset management,
- HR security,
- physical and environmental security,
- system and network management,
- access control,
- acquisition, development and maintenance of IT systems,
- continuity of operations management,
- compliance with legal requirements[4].

The standard in question is sufficiently general to be applied in all kinds of organizations where information is particularly protected and its loss would result in legal consequences. Among such organizations are banks, public administration institutions, health care institutions, non-profit organizations and courts.

The standard applied the Deming cycle, PDCA (i.e. plan – do – check – act), according to which the ISMS implementation process can be divided into four steps:

- plan – the establishment of ISMS, i.e. the development of policy, instructions, procedures and rules that are important in risk management and permanent improvement of information security;
- do – the implementation and execution of the policies, procedures and rules in everyday work. Staff training is a very important element of the implementation and it should

[4] *Biuletyn jakości (Quality Bulletin) No.1/2009, Systemy zarządzania bezpieczeństwem informacji ISO/IEC 27001*; TUV Rheinland Polska Sp. z o.o., 2009.

include issues concerning the implemented procedures and the awareness of the reasons why security policy should be executed;

- check – i.e. studying how ISMS is applied in the organization and monitoring whether the level of the process efficiency is adequate and the management is given the results of the checks. As a result, the security policy can be improved and there is a possibility to react to the emerging external threats as well as mistakes within the organization;
- act – i.e. checking whether ISMS policies, regulations, instructions and procedures are not out-dated due to the emergence of new systems or threats and, consequently, undertaking the necessary measures to update the ISMS[5].

The application of this standard is beneficial as it increases staff awareness as regards the significance of information security and of the losses resulting from its breach. Another advantage, which in the case of law courts is of particular significance, is the confidence of the customers of courts that information, including confidential, secret and top secret data that are processed by the court will not be lost. The implementation of an information security management system in a law court ensures the compliance with law requirements and the determination of methods that should ensure continuity of the court's operations in the case of an IT breakdown[6]. The PN ISO/IEC 27001:2007 standard is the equivalent of the ISO/IEC 27001:2005 which was developed by ISO and IEC in 2005.

The PN ISO/IEC 27005 standard includes guidelines for information systems risk management that aim at diminishing the risk to organizations. Risk management should be an ongoing process in organizations that involves risk identification and treatment as well as the reduction of its probability and effects. The analysis of risk management should first identify the risk, i.e. what may happen and what consequences it involves to the organization, and what should be done to reduce the risk to the level acceptable by the organization. Risk can be analyzed for the whole organization or for its particular departments, divisions or every ICT system that operates in the organization[7].

PN-I-13335 is the standard whose development was based on ISO/ICE TR 13335 (GMITS – Guidelines for the Management of IT security) technical report that was issued by ISO and IEC. It consists of five parts.

---

[5] *Biuletyn jakości (Quality Bulletin) No.1/2009, Systemy zarządzania bezpieczeństwem informacji ISO/IEC 27001*; TUV Rheinland Polska Sp. z o.o., 2009.
[6] Brochure of the Polish Standard Committee *SZBI PN-ISO/IEC 27001:2007 bezpieczeństwo informacji*, PKN, p. 2.
[7] F. Wołowski. *Bezpieczeństwo systemów informatycznych*, Wydawnictwo edu-Libri, Kraków-Warszawa 2012, p. 61.

Part one - PN-I-1335-1:1999 – includes guidelines for the management of the security of IT systems; the concepts, relations between the terms and basic models that can be applied to describe IT security systems.

Part two - PN-I-1335-2:2003 – includes a detailed description of IT security planning and managing.

Part three - PN-I-1335-3 – describes techniques for the management of IT security.

Part four - PN-I-1335-4 – deals with issues concerning the selection of adequate safeguards.

Part five - PN-I-1335-5 – describes safeguards for the connections with external networks.[8]

2 Legal regulations on information security in public administration

The obligation to protect data results from legal provisions which define the requirements regarding the protection of information. Polish regulations include several acts and regulations that have to be known and applied when developing information security policy. The implementation of security policy in an organization involves business and legal aspects. The policy in an organization should be in line with the regulations that are in force in Poland. It cannot violate any provisions as it involves legal sanctions.

The following legal acts include definitions, information and requirements concerning information security:

- Act of 29 August 1997 on the protection of personal data, Journal of Laws 2002, No.101 item 926 as amended,
- Act of 27 July 2001 on the protection of databases, Journal of Laws 2001, No.128, item 1402 as amended,
- Act of 6 September 2001 on access to public information, Journal of Laws 2001, No.112, item 1198, 2002 No.153, item 1271, 2004 No.240, item 2407,
- Act of 18 September 2001 on electronic signature, Journal of Laws 2001, No.130, item 1450,
- Act of 18 July 2002 on providing services by electronic means, Journal of Laws 2002, No.144, item 1204,
- Telecommunications Act of 16 July 2004, Journal of Laws 2004, No.171, item 1800,

[8] http://www.governica.com/ISO-IEC_TR_13335; (accessed: 10.04.2015).

- Act of 5 August 2010 on the protection of classified data, Journal of Laws 2010, No.182, item 1228,
- Act of 22 August 1997 on the protection of personal data and property, Journal of Laws, 1997, No.114, item 740,
- Act of 4 February 1994 on copyright and related rights, Journal of Laws 1994, No.24, item 83,
- Act of 24 May 2000 on National Crime Register, Journal of Laws 2000, No.50, item 580,
- Act of 5 July 2002 on protection of certain services provided by electronic means and based on or consisting in conditional access, Journal of Laws 2002, No.126, item 1068,
- Act of 17 February 2005 on the computerizations of activities of entities performing public tasks, Journal of Laws 2005, No.64, item 565,
- Regulation of the President of the Council of Ministers of 20 July 2011 on basic requirements of ICT security, Journal of Laws 2011, No.159, item 948,
- Regulation of the Minister of Finance of 31 October 2003 on detailed principles of the creation, preservation, storage and protection of documents related to the conclusion and execution of insurance agreements, Journal of Laws 2003, No.193, item 1889,
- Regulation of the Minister of Justice of 28 April 2004 on technological methods of developing systems and networks to transfer information, store billing lists and other information transfers, and methods to protect IT data, Journal of Laws 2004, No.100, item 1023,
- Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 on documentation of personal data processing and technological and organizational conditions to be met by devices and IT systems applied for personal data processing, Journal of Laws 2004, No.100, item 1024,
- Regulation of the Council of Ministers of 20 July 2011 on determination of technological and organizational conditions for qualified entities offering certification services, certification policies for qualified certificates issues by these entities and technological conditions for secure devices for placing and verifying electronic signature, Journal of Laws 2002, No.128, item 1094,
- Regulation of the Council of Ministers of 29 May 2012 on the physical security measures used to protect classified information, Journal of Laws 2012, no.115, item 683,
- Regulation No.57 of the Minister of National Defense of 16 December 2011 on detailed organization and functioning of secret registry and other offices responsible for processing

classified information, the method and procedure for processing classified information and the selection of and application of physical security measures, Official Journal of the minister of National Defense, No.24, 30 December 2011.

The Act of 29 August 1997 on the protection of personal data defines procedures regarding personal data processing and the right of natural persons whose personal data are or may be processed in databases[9]. It appoints the GIODO (Inspector General for Personal Data Protection) and defines its competencies. It provides general principles of the protection of personal data bases, the rules regarding the registration and processing of personal data. It also defines the rights of individuals whose data are processed. It contains offence provisions for the breach of the act. The act is applicable to all, both state are self-government organizational entities and natural and legal persons that process personal data both in an electronic or paper way.

The Act of 27 July 2001 on the protection of databases is the result of the implementation of the Directive 96/9/EC of the European Parliament and the Council of Europe of 11 March 1996 on the legal protection of databases. The act defines databases and their significance: database is a collection of data or any other materials or elements arranged systematically or methodically that can be accessed individually by various ways, including electronic means and that requires a substantial, regarding quality or amount, investment to develop, verify or present its contents[10].

By the Act of 6 September 2001 on access to public information, Journal of Laws 2001, No.112, item 1198, the term *public information* refers to any information on public matters and is subject to sharing in accordance with the principles and procedures provided by the Act[11]. Pursuant to the Act, with the provision of Art.5, everybody has the right of access to public information. The following bodies are obliged to share public information:

- bodies of public authority,
- bodies of economic and professional local authorities,
- entities representing the State Treasury in accordance with the separate provisions,
- entities representing the state legal persons,

[9] Act of 29 August 1997 on the protection of personal data, Journal of Laws 2002, No.101 item 926
[10] Act of 27 July 2001 on the protection of databases, Journal of Laws 2001, No.128, item 1402
[11] Act of 6 September 2001 on Access to public information, Journal of Laws 2001, No.112, item 1198, chpt. 1, section 1.1

- bodies which perform public functions and dispose of public or the State Treasury property,
- legal persons in which the State Treasury or units of local authority or economic or professional local authority hold dominant position[12].

Making public information available takes place by means of

- announcing it in the Public Information Bulletin,
- attending the meetings of the bodies of public authority and making available the material documenting these meetings,
- making it available to person that is interested in particular information.

The legislator determined restrictions regarding the access to public information, which is included in the provisions on the protection of classified information and the protection of other information protected by the act and due to the protection of the privacy of natural persons. This concerns such issues as appropriate anonymity of the shared documents, i.e. the conversion of first names, surnames, geographical names, commercial names and the names of appliances and vehicles, etc. into initials.

The act of 18 September 2001 on electronic signature defines the conditions for the application of electronic signature, legal consequences of its applications, the principles of certification services and of the supervision over entities that render such services[13]. Thanks to this act, electronic documents can be signed as it is the case with paper documents. However, several conditions provided by the act have to be met for the electronic signature to be recognized as secure. The act also includes penal provisions for service providers, i.e. the entities that issue the certificates, if they do not meet the requirements of the act, and for natural persons that use signatures belonging to other persons.

The Act of 18 July 2002 on providing services by electronic means defines:

- the obligations of service providers resulting from the provision of services by electronic means,
- rules of releasing service providers from legal liability by virtue of the provision of services by electronic means,

[12] Ibid, Chapter 1, Art. 4.1.
[13] Act of 18 September 2001 on electronic signature, Journal of Laws 2001, No.130, item 1450,

- rules for the protection of personal data of natural persons using the services provided by electronic means[14].

The Telecommunications Act of 16 July 2004, Journal of Laws 2004[15], implements the EC directives on electronic communication. It is the basic legal regulation that provides legal framework for telecommunication activities and specifies the activity range of the regulatory office. The act, determines – among other things – the following:

- the principles of performing telecommunication services, providing telecommunication networks and their supervision,
- the rights and obligations of telecommunication business operators,
- the conditions for data processing and confidentiality protection in the telecommunication sector,
- the requirements regarding broadcasting and telecommunication appliances,
- the requirements regarding telecommunication confidentiality and data protection of end-users.

The legislator's aim of the Act is to ensure a widespread access to telecommunication services in the country and the development of modern telecommunication networks, to support healthy competition on the telecommunication market, and to ensure the safety and defense capability of Poland as well as public order and safety.

The Act of 22 August 1997 on the protection of persons and property determines – among other things – areas, premises and facilities that are subject to mandatory protection. It defines the rules of the creation and functioning of internal security services, the rules of conducting commercial security services aimed at protecting persons and property and the qualifications and rights of security staff.[16]

The Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 on documentation of personal data processing and technological and organizational conditions to be met by devices and IT systems applied for personal data processing, provides a list of items that should be covered by the security policy:

- a list of buildings, premises or their parts comprising the area where personal data are processed;

[14] Act of 18 July 2002 on providing services by electronic means, Journal of Laws 2002, No.144, item 1204, Chpt. 1, Art. 1.
[15] Telecommunications Act of 16 July 2004, Journal of Laws 2004, No. 171, item 1800, Chpt. 1, Art. 1.1.
[16] Act of 22 August 1997 on the protection of persons and property, Journal of Laws, 1997, No.114, item 740

- a list of data filing systems with an indication of software used for data processing;
- a description of the structure of data filing systems and indication of the contents of particular information fields and connections between them;
- a method of transferring data between particular systems;
- definition of technical and organizational measures necessary to ensure confidentiality, integrity and accountability of the data being processed[17].

It also determines the contents of a management manual for IT systems used in personal data processing. They should include:

- authorization procedures for data processing and the registration of the rights for data processing in IT systems as well as pointing at individuals responsible for such activities,
- authorization methods and measures to be applied and procedures regarding their management and application,
- procedures for commencing, suspending and completing the operations for the system users,
- procedures for making back-up copies of databases and the software and tools applied to process the data,
- the method, place and time period for storing electronic information carriers with personal data and back-up copies,
- the method for securing the IT system.

The Regulation also introduces three levels of data processing security in IT systems and defines security measures that should be applied on each level.

The Regulation of the Minister of Justice of 28 April 2004 on technological methods of developing systems and networks to transfer information, store billing lists and other information transfers and methods to protect IT data determines:

- technological development of systems and networks for information transfer, storage of billing lists and other information transfers,
- IT data security measures applied in facilities storing such data and in information carriers, including data transferred by electronic mail[18].

[17] Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 on documentation of personal data processing and technological and organizational conditions to be met by devices and IT systems applied for personal data processing, Journal of Laws 2004, No.100, item 1024,

The entity in question is obliged to store data related to information transfers and to ensure the possibility to file the information flow 24 hours per day. The entity should protect the data with the application of technology that enables its reproduction[19].

When securing the data on an information carrier, the person responsible should put down:

- the reference number,
- his/her name, surname and position,
- data regarding the security reasons,
- completion time of the security operation.

and – additionally – the person in charge should make an official note including the above listed information as well as the data identifying the location of the data filed, the name and the surname of the system- or network- user that is subject to data protection

3 Classification of data subject to protection

Information that is processed by organizations can be divided into public and protected information. Public information is not protected. It is developed within an organization and shared without any damage to the organization.

Protected information includes information for official and internal uses. The information for official use is processed within the organization and may be transferred to other organizations in the course of its work. Internal information is the information that cannot be released from the internal structures of the organization or its particular departments or divisions. An example of public information in the court system is the information placed on the Internet. Information for official use is, for example, the information stored on the court's intranet, personal data of claimants, internal communication, etc.

The information for internal use includes, for example, confidential post or e-mails, personal data of the staff, data concerning security measures, back-up copies, passwords, access codes or encryption keys.

[18] Regulation of the Minister of Justice of 28 April 2004 on technological methods of developing systems and networks to transfer information, store lists of telephone calls and other information transfers, and methods to secure IT data, Journal of Laws 2004, No. 100, item 1023, section 1.1

[19] Tamże § 3, 4.1, 4.2 i 4.3.

Additionally, the legislator issues regulations and acts on information classification and the protection of information, computer hardware and information and communication infrastructure applied when processing classified information.

The Act of 5 August 2010 on the protection of classified data determines the protection principles of information whose unauthorized disclosure would cause damage to the Republic of Poland or would be harmful to its interests [20]. The rules concern:

- classification of classified information,
- organization of classified data protection,
- processing of classified information,
- verifying procedures as regards individuals who have access to classified information,
- organization of the control over classified information protection,
- organization of classified information protection in ICT systems,
- implementation of physical security measures with respect to classified data[21].

The above regulations are applied to public authority bodies, particularly to:

- the Sejm (the lower house of the Parliament) and the Senate,
- the President of the Republic of Poland,
- the state administration bodies,
- local administration bodies,
- courts of justice and tribunals,
- bodies of state control and protection of law.

The above regulations also apply to the entities that report to the Minister of National Defense, the Central Bank (NBP), organizational entities that report to public authority bodies and to entrepreneurs completing or wishing to complete agreements associated with the access to classified information.

The Act divides classified information into the following categories:

- top secret,
- secret,
- confidential,
- restricted.

[20] Act of 5 August 2010 on the protection of classified data, Journal of Laws 2010, No.182, item 1228, Chpt. 1, Art. 1
[21] Ibid, Chapter 1, Art. 1.1.

Regulation No.57/MON of the Minister of National Defense of 16 December 2011 on specific organization and functioning of secret registries and other offices responsible for processing classified information, the method and procedure for processing classified information and the selection of and application of physical security measures[22] determines – among other things - the following:

- the organization and functioning of secret registries and other offices responsible for processing classified information,
- the selection and implementation of physical security measures,
- the rules of registration, completion and destruction of classified information, work organization of secret registries and their protection, document flow during maneuvers and war,
- the rules of processing classified information in ICT systems,
- samples of registration instruments.

The Regulation includes guidelines regarding the functioning of secret offices in which classified information can be processed. It provides adequate standards that the secret offices have to conform to as regards filing cabinets and classified data destruction tools. It also enumerates all standards concerning physical security measures such as safes, doors, bars, windows, monitoring, alarm and fire systems as well as air hole grates that make it impossible to eavesdrop electronically the talks held in the secret office. The accreditation of secret offices in district courts is conducted by an employee of the District Court, the Plenipotentiary for Protection of Classified Information.

The Regulation of the Council of Ministers of 29 May 2012 on physical security measures used to protect classified information defines:

- basic criteria and methods to determine the threat level,
- the selection of physical security measures that are adequate to a particular threat level,
- types of threats that should be taken into consideration when determining the threat level,
- basic elements that should be considered by the classified information protection plan,
- the range of physical security measures that should be applied,

[22] Regulation No.57/MON of the Minister of National Defense of 16 December 2011 on specific organization and functioning of secret registries and other offices responsible for processing classified information, the method and procedure for processing classified information and the selection of and application of physical security measures. Chapter 1, Art. 1.

- the criteria for the development of protection zones. [23]

Pursuant to the Regulation, there are three threat levels (high, medium and low) as regards the possibility of the loss of confidentiality, integrity and availability of information. The Regulation defines how to conduct the analysis to determine the threat level. It states the obligation to consider both natural threats, resulting from natural forces or breakdowns of facilities, and threats that are related to human purposeful or non-purposeful activities. It defines three protection areas with a precise determination of requirements related to each of the areas. It enumerates the physical security measures that should be applied with regard to the threat level and the type of protection area and it points to the standards that have to be met by the measures in question.

The above provisions aim at the proper protection of classified information, i.e. correct processing, differentiation of access in line with the authorization, detection and prevention from unauthorized operations or the theft of classified information.

The Regulation of the President of the Council of Ministers of 20 July 2011 on basic requirements of IT security determines:

- basic IT security requirements for ICT systems,
- necessary data that should be included in the ICT systems security documentation as well as the methods of its development[24].

The Regulation introduces basic ICT security requirements that aim at the assurance of confidentiality, integrity and availability of classified information. It obliges to implement a multilevel ICT system protection and limited trust to other networks, ICT systems and their users.

Conclusion

Information and knowledge are the basis for the functioning of any temporary organization. They are frequently more important than its material assets. Without these two factors organizations are not able to function effectively and efficiently and, what is more, they cannot survive on the market as all competitors do their best to implement increasingly

[23] Regulation of the Council of Ministers of 29 May 2012 on physical security measures used to protect classified information, Journal of Laws 2012, item 683, section 1.1

- Regulation of the President of the Council of Ministers of 20 July 2011 on basic requirements of IT security, Journal of Laws 2011, No.159, item 948,

better and more effective solutions. Organization devote increasingly more time and means to protect information and knowledge against loss, theft or destruction, both purposeful and coincidental in nature. Nowadays, knowledge and information does not exist only in a verbal or paper form but also in a digital form, which is dominating. Due to the development of IT and ICT technologies, the emphasis should be put on the protection of data with regard to modern technologies. However, it is not enough to purchase modern solutions that would protect and secure data against loss or destruction. One should also remember about the development, observance and continuous improvement of Information Security Policy. The Policy should be developed individually for every organization and continually adjusted and improved together with the emergence of both new threats and new protection systems.

Bibliografia

Bibliography

Biuletyn jakości nr 1/2009, *Systemy zarządzania bezpieczeństwem informacji ISO/IEC 27001*; TUV Rheinland Polska Sp. z o.o., 2009

Stokłosa J., *Bezpieczeństwo danych w systemach informatycznych*, PWN, Warszawa 2001.

Wołowski F., *Bezpieczeństwo systemów informatycznych*, Wydawnictwo edu-Libri, Kraków-Warszawa 2012.

Wykaz aktów prawnych:

Legal acts:

Act of 22 August 1997 on the protection of persons and property, Journal of Laws, 1997, No.114, item 740
Act of 29 August 1997 on the protection of personal data, Journal of Laws 2002, No.101 item 926
Act of 24 May 2000 on National Crime Register, Journal of Laws 2000, No.50, item 580
Act of 27 July 2001 on Law on common courts organization, Journal of Laws 2001, No.98, item 1070,

Act of 27 July 2001 on the protection of databases, Journal of Laws 2001, No.128, item 1402,
Act of 6 September 2001 on access to public information, Journal of Laws 2001, No.112, item 1198,
Act of 18 September 2001 on electronic signature, Journal of Laws 2001, No.130, item 1450,
Act of 18 July 2002 on providing services by electronic means, Journal of Laws 2002, No.144, item 1204,
Regulation of the Minister of Justice of 28 April 2004 on technological methods of developing systems and networks to transfer information, store billing lists and other information transfers, and methods to protect IT data Journal of Laws 2004, No. 100, item 1023,
Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 on documentation of personal data processing and technological and organizational conditions to be met by devices and IT systems applied for personal data processing, Journal of Laws 2004, No.193, item 1889,
Telecommunications Act of 16 July 2004, Journal of Laws 2004, No.171, item 1800,
Act of 17 February 2005 on the computerizations of activities of entities performing public tasks, Journal of Laws 2005, No.64, item 565,
Act of 5 August 2010 on the protection of classified data, Journal of Laws 2010, No.182, item 1228,
Regulation of the President of the Council of Ministers of 20 July 2011 on basic requirements of ICT security, Journal of Laws 2011, No.159, item 948,
Regulation No.57/MON of the Minister of National Defense of 16 December 2011 on specific organization and functioning of secret registries and other offices responsible for processing classified information, the method and procedure for processing classified information and the selection of and application of physical security measures,
Regulation of the Council of Ministers of 29 May 2012 on physical security measures used to protect classified information, Journal of Laws 2012, item 683, section 1.1
Regulation of the Minister of Justice of 27 June 2012, section 93, Warszawa 28 June 2012 on the implementation of Information Security Policy of the Ministry of Justice and common courts.

Normy:

- PN ISO/IEC 27001:2007 Information technology – Security techniques – Information security management systems – Requirements.
- PN-ISO/IEC 17799:2007 Information technology – Security techniques – Information security risk management.
- PN-ISO/IEC 17799:2007 Information technology - Security techniques – Practical principles for information security management.

- PN-I-13335 Information technology – Guidelines to information security management.
- PN ISO/IEC 20000-1:2007 Information technology – Service management part 1: Specification.
- PN ISO/IEC 20000-2:2007 Information technology – Service management part 2: Code of practice.

The Internet:

http://www.governica.com/ISO-IEC_TR_13335
http://www.iniejawna.pl/pomoce/ensi.html