REPUBLIC OF POLAND
Ministry of Administration and Digitisation,
Internal Security Agency

CYBERSPACE PROTECTION POLICY OF THE REPUBLIC OF POLAND

REPUBLIC OF POLAND
Ministry of Administration and Digitisation,
Internal Security Agency

CYBERSPACE PROTECTION POLICY OF THE REPUBLIC OF POLAND

WARSAW
25 June 2013

TABLE OF CONTENTS:

This document has been drawn up in the Ministry of Administration and Digitization in cooperation with the Internal Security Agency, based on:

- the document discussed on 9 March 2009 by the Standing Committee of the Council of Ministers, "The Government Cyberspace Protection Programme of the Republic of Poland for 2009-2011 – Principles,"
- the periodic reports on the security status of the gov.pl area, published by the Governmental Computer Security Incident Response Team CERT.GOV.PL,
- the decision of the Chairman of the Committee of the Council of Ministers for Digitization No. 1/2012 of 24 January 2012 with regard to the creation of a Task force for the protection of governmental portals.

1. The main prerequisites and assumptions of the Cyberspace Protection *Policy* of the Republic of Poland

In the face of globalization, the cyberspace security has become one of the key strategic objectives in the area of security of each country. At a time of free movement of people, goods, information and capital – the security of a democratic country depends on the development of mechanisms which allow preventing and combating threats to the cyberspace security.

Due to the increase in threats to the ICT systems, from which the total separation is not possible, and the fact that the responsibility for ICT security is distributed, it is necessary to coordinate actions which will allow for a fast and effective response to attacks directed against ICT systems and services offered by them.

The ICT systems operated by the government administration, the legislative authorities, the judiciary, local government, as well as the strategic systems from the point of view of the security of the State as well as entrepreneurs and natural persons are covered by this "Cyberspace Protection Policy of the Republic of Poland," hereinafter referred to as the ***Policy***.

By this ***Policy***, the Government of the Republic of Poland accepts that by its representatives it takes an active role in ensuring the security of information assets of the State, its citizens, and it executes its constitutional duties.

A part of the ***Policy*** includes the support for social initiatives aimed at implementing the tasks coinciding with this document.

The Government of the Republic of Poland, in fulfilling the constitutional obligations implemented by cyberspace, consults organized groups of society, in particular the representatives of telecommunications entrepreneurs and purveyors providing services by electronic means, to agree on an acceptable level of security of execution of obligations in question.

Accepting the status of the ***Policy*** for this document, it should be noted that under the current system of governmental strategic documents a ***Policy*** is in the group of strategic documents detailing the courses of action identified in the strategies, development programmes and other programme documents, which do not specify new priorities and activities. They set the vision of development for a given sector and the way for its implementation, based on the provisions of the relevant documents.

The ***Policy*** does not cover with its task area the classified ICT systems. It should be emphasized that the area of protection of classified information has its own regulations and appropriate protective mechanisms. It has the organizational structures dedicated to the protection of classified information produced, processed and stored in separate ICT systems. The main legislative act is the Act of 5 August 2010 on the protection of classified information (OJ No. 182, item 1228).

1.1. DEFINITIONS

The meaning of terms and abbreviations used in this document:

Abuse – a common name of a security department of an internet service provider who manages the computer security incident response process and the examination of complaints of abuse,

cyberspace security – a set of organizational and legal, technical, physical and educational projects aimed at ensuring the uninterrupted functioning of cyberspace,

CERT (Computer Emergency Response Team), CSIRT (Computer Security Incident Response Team) – a team set up to respond to incidents violating security on the Internet,

cyber attack – an intentional disruption of the proper functioning of cyberspace,

cybercrime – an offence committed in cyberspace,

cyberspace – a space of processing and exchanging information created by the ICT systems, as defined in Article 3 point 3 of the Act of 17 February 2005 on the informatization of entities performing public tasks (OJ No. 64, item 565, as amended), together with links between them and the relations with users; in accordance with Article 2 paragraph 1b of the Act of 29 August 2002 on martial law and the powers of the Supreme Commander of the Armed Forces as well as the Commander's subordination to the constitutional authorities of the Republic of Poland (OJ No. 156, item 1301, as amended), Article 2 paragraph 1a of the Act of 21 June 2002 on the state of emergency (OJ No. 113, item 985, as amended) and Article 3 paragraph 1 point 4 of the Act of 18 April 2002 on the state of natural disaster (OJ No. 62, item 558, as amended),

cyberspace of the Republic of Poland (hereinafter referred to as CRP) –cyberspace within the territory of the Polish state and beyond, in places where the representatives of the RP are functioning (diplomatic agencies, military levies),

cyberterrorism – an offence of a terrorist nature committed in cyberspace,

computer security incident – a single event or a series of adverse events related to information security which pose a significant likelihood of disruption of business operations and jeopardize the security of information (according to the PN-ISO/IEC 27000 norm series),

organizational unit – an organizational unit within the meaning of the Act of 23 April 1964 – Civil Code (OJ No. 16, item 93, as amended),

PCS – a plenipotentiary for cyberspace security in organizational units of public administration,

entrepreneur – an entrepreneur within the meaning of Article 4 of the Act of 2 July 2004 on freedom of economic activity (OJ of 2010, No. 220, item 1447, as amended) or any other organizational unit, regardless of the form of ownership,

risk assessment – means the total risk analysis, which consists of: risk identification

and determination of extent of risks, as well as the risk assessment process,

cyberspace user – each organizational unit, an office supporting a public administration authority, an entrepreneur and a natural person who uses the resources of cyberspace.

1.2. STRATEGIC OBJECTIVE

The strategic objective of the *Policy* is to achieve an acceptable level of cyberspace security of the State.

The achievement of the strategic objective is accomplished by creating a legal and organizational framework and a system for effective coordination and exchange of information between the users of CRP.

Actions undertaken to achieve the strategic objective are the result of risk assessments conducted by the qualified entities, with respect to threats occurring in cyberspace.

At the same time, the ***Policy*** is in line with the objectives of:

1) the Digital Agenda for Europe of the European Council [COM(2010)245];
2) the Strategy for Development of Information Society;
3) the National Security Strategy;
4) the Medium-Term National Development Strategy;
5) the "Europe 2020" Strategy;
6) the Efficient State Strategy.

1.3. SPECIFIC OBJECTIVES

1) Increasing the level of security of the State ICT infrastructure.
2) Improving the capacity to prevent and combat threats from cyberspace.
3) Reducing the impact of incidents threatening the ICT security.
4) Determining the competence of entities responsible for the security of cyberspace.
5) Creating and implementing a coherent system of cyberspace security management for all government administration entities and establishing guidelines in this area for non-state actors.
6) Creating a sustainable system of coordination and exchange of information between the entities responsible for the security of cyberspace and the cyberspace users.
7) Increasing awareness of the cyberspace users on the methods and safety measures in cyberspace.

The objectives of the ***Policy*** are implemented through:

a) the coordination system to prevent and respond to threats and attacks on cyberspace, including attacks of a terrorist nature;
b) the widespread adoption of mechanisms for the prevention and early detection of threats to the cyberspace security and the proper procedure for the identified incidents among the government administration units as well as non-state actors;
c) the general and specialized social education in the field of security of CRP.

1.4. ADDRESSEES AND EXTENT OF IMPACT

The ***Policy*** is addressed to all the cyberspace users within the State and beyond its territory, in places where the representatives of the RP are functioning (diplomatic agencies, military levies).

This ***Policy*** applies to the government administration:

1) offices supporting the state bodies of government administration: Prime Minister, the Council of Ministers, ministers and chairmen specified in statutes of committees;
2) offices supporting central bodies of government administration: other than the above-mentioned, i.e. bodies subordinate to the Prime Minister or individual ministers;
3) offices supporting local bodies of government administration: province governors, bodies of combined and non-combined administration;
4) Government Centre for Security.

At the same time the ***Policy*** is recommended for local government administration of communes, districts and provinces and other offices (units which do not belong to the state and local government administration), including:

a) Chancellery of the President of the Republic of Poland;
b) Chancellery of the Sejm of the Republic of Poland;
c) Chancellery of the Senate of the Republic of Poland;
d) Office of the National Broadcasting Council;
e) Office of the Human Rights Defender;
f) Office of the Children's Ombudsman;
g) Office of the National Council of the Judiciary of Poland;
h) offices of state control bodies and protection of the law;
i) National Bank of Poland;
j) office of the Polish Financial Supervision Authority;
k) state legal persons and state organizational units other than the above-mentioned.

The ***Policy*** is at the same time a guide to actions for all other users of cyberspace who are not mentioned above.

1.5. ESTABLISHING RESPONSIBILITY FOR THE SECURITY OF CRP

Due to the international nature of the ***Policy*** the entity coordinating the implementation of the ***Policy***, on behalf of the Council of Ministers, is the minister responsible for informatization who, with the help of the Team referred to in point 3.4.1, ensures coordination and consistency of actions undertaken to ensure the security of CRP.

In the implementation of tasks relating to the security of CRP the Governmental Computer Security Incident Response Team CERT.GOV.PL is acting as the primary CERT in the area of government administration and the civil area. The main task is to provide and develop the capacity of organizational units of public administration of the Republic of Poland to protect against cyber threats, with particular emphasis on attacks targeted at infrastructure including ICT systems and networks, destruction or disruption of which could pose a threat to human life, health, national heritage and the environment to a significant extent, or cause serious property damage and disrupt the functioning of the state.

Similarly, in the military this role is performed by "Departmental Centre for Security Management of ICT Networks and Services."

For the success of the ***Policy***, an active participation of users of CRP in the efforts aimed at improving the level of its security is essential.

It is also important to increase the participation of users of CRP in the implementation of the ***Policy*** by consulting its content and participation in the coordination of the implementation of the ***Policy*** and its reviews with the representatives of society and ICT community.

The general use of solutions aimed at improving the security by the users of CRP will be an expression of approval for the actions undertaken by the Government of the Republic of Poland in this area.

1.6. COMPLIANCE OF THE *POLICY* WITH LEGAL ACTS

The Policy is in compliance with the generally applicable laws of the Republic of Poland (the Constitution, acts, ratified international agreements and regulations) and without prejudice to any of them.

2. Conditions and problems of the cyberspace area

Functioning of the State and the implementation of its constitutional obligations is increasingly dependent on the development of modern technology, information society and uninterrupted functioning of cyberspace. Currently, the safe functioning of cyberspace largely depends on the security of ICT infrastructure, which allows the use of cyberspace, information resources and services gathered in it, operating thanks to it. The infrastructure functioning in CRP allows the State to fulfil its constitutional obligation to the citizen, ensures continuity and effectiveness of government administration as well as uninterrupted and efficient development of the economy of the Republic of Poland.

Polish government sees the need to introduce measures aimed at ensuring the security of the State ICT infrastructure, namely ensuring the correctness and continuity of functioning of ICT systems, facilities and installations used to implement the constitutional duties of the State to the citizens and its internal security. For this purpose it is necessary to determine the minimum security standard which will allow for the implementation of this objective and will reduce to the minimum potential damage which may be entailed by attack on individual elements of cyberspace of RP. The ***Policy*** is the basis for developing the concept of management of infrastructure security functioning within CRP and developing guidelines for the creation of the legal basis serving the implementation of tasks in this regard by the government administration. The principles of ensuring cyberspace security developed under the cooperation referred to in point 4.4, within the infrastructure of CRP are also recommended to entrepreneurs.

The actions concerning the security of ICT infrastructure will be complementary to the efforts aimed at protection of the critical infrastructure of the State. In this respect, the ***Policy*** does not affect the provisions contained in the National Critical Infrastructure Protection Programme.

The Policy indicates the need to develop the concept of ensuring security of infrastructure functioning within CRP and prepare legal basis for performance of tasks in this regard by the government administration.

The ICT infrastructure of CRP must be protected against attacks from cyberspace, destruction, damage or unauthorized access.

As a part of actions connected with the implementation of the ***Policy*** a risk assessment is carried out with regard to the identification of resources, sub-systems, functions and dependencies on other systems relevant to the functioning of CRP. At the same time, the implementation of the ***Policy*** will allow for the development of target guidelines for performance of risk estimates and model of reports containing general data on types of risks, threats and vulnerabilities identified in each of the sectors of the Polish economy in relation to the constitutional tasks carried out on the basis of CRP.

There is a need to develop, on the basis of the conducted risk analysis, the minimum safety standards according to which the identified resources and systems will be protected, thanks to which the constitutional obligations of the State are fulfilled.

3. The main lines of action

The ***Policy*** will be implemented through the following actions, in accordance with the priorities resulting from the order shown.

3.1. Risk assessment

The assessment of risk associated with the functioning of cyberspace is a key element of the process of cyberspace security, determining and justifying the actions undertaken to reduce it to an acceptable level.

In order to achieve an acceptable level of security, it is assumed that each government administration unit, referred to in point 1.4 (points 1-4), shall, no later than January 31 each year, submit to the minister responsible for informatization the report summarizing the results of the risk assessment (in accordance with the model developed by the minister responsible for informatization). The report should contain general information on types of risks, threats and vulnerabilities diagnosed in each of the sectors which an individual institution is operating in and is responsible for. The report should also present information on how to deal with risk.

Minister responsible for informatization in collaboration with the involved institutions will determine the uniform methodology for performing risk analyses. There is a necessity for the use of this methodology to be eventually mandatory for the institutions of government administration.

It is recommended that the Governmental Computer Security Incident Response Team CERT.GOV.PL presented to the minister responsible for informatization, in order to unify the approach, complied directories containing the specification of the risks and possible vulnerabilities affecting the security of cyberspace.

3.2. The security of government administration portals

The main place for exchanging information between the government administration units and a citizen, in e-society, are websites. They should comply with the fundamental safety requirements, that is, ensure adequate availability, integrity and confidentiality of data. Each organizational unit should independently assess the risk (referred to in point 3.1) for its portals. It is assumed that on this basis the appropriate (depending on the type of site and the results of the risk assessment) organizational and technical solutions will be implemented so as to ensure an adequate level of security. Due to the different types of parties and their different priorities, these solutions will differ from each other.

It is proposed that the government administration units running Internet portals, in addition to complying with the minimum requirements, implement also the relevant

recommendations and good practices in the field of security, which will be prepared by the Task force for the protection of government portals in cooperation with the Governmental Computer Security Incident Response Team CERT.GOV.PL.

3.3. PRINCIPLES OF LEGISLATIVE ACTIONS

The basic elements of the execution of the ***Policy***, planned for immediate implementation, are legislative actions. The Council of Ministers, understanding a high priority of these actions, notices the need for their initiation by the minister responsible for informatization in order to create regulations which give grounds for further actions in the implementation of the provisions of the ***Policy***. It is necessary to review the existing regulations with a view to the preparation of solutions aimed at increasing the sense of security, not only of government institutions, but of all the users of cyberspace.

3.4. PRINCIPLES OF PROCEDURAL AND ORGANIZATIONAL ACTIONS

An important step in the implementation of the ***Policy*** will be the procedural and organizational actions. Their aim is to optimize the functioning of CRP through the implementation of best practices and standards in this area. At this stage it is necessary to use both the legal tools developed in the first stage and the "soft"[1] mechanisms of regulations.

Performance of this stage will take place thanks to the creation of separate specific projects.

3.4.1. Management of the cyberspace security of the Republic of Poland

As a part of the management of the cyberspace security of the RP, as well as to improve the process of implementation of the ***Policy*** objectives and to ensure effectiveness of the State authorities in the field of security of CRP, it is necessary for the Prime Minister to appoint a team responsible for the preparation of recommendations concerning the implementation and coordination of any actions related to its security (hereinafter referred to as the Team).

The Team may be organized with the use of the existing potential of the Task force for the protection of government portals, appointed by the Chairman of the Committee of the Council of Ministers for the Digitization by the Decision No. 1/2012 of 24 January 2012.

It is recommended that the Team, within 30 days from the date of appointment, prepared and presented an action plan to ensure the security of cyberspace of the Republic of Poland.

The primary task of the Team shall be recommending actions aimed at coordination

[1] A soft regulation means, for example, codes of good practice, guidelines, recommendations, code of ethics, etiquette, best practices or standards, etc.

of activities of the institutions carrying out the tasks imposed by the ***Policy***, organization of regular meetings, recommending the proposed solutions for the security of CRP.

It is assumed that as for the implementation of tasks related to the security of CRP in the area of government administration and the civil area, the role of the main CERT is performed by the Governmental Computer Security Incident Response Team CERT. GOV.PL. Similarly, in the military this role is performed by "Departmental Centre for Security Management of ICT Networks and Services."

3.4.2. The safety management system in organizational unit

In each organizational unit of government administration, as a part of ensuring the cyberspace security, the head of the unit should establish an information security management system, in accordance with the applicable provisions and best practice.

It is assumed that the public body will develop and modify according to the needs, and implement a security policy for ICT systems used by it for the execution of public tasks. While developing the security policy a public body includes obligations arising from the Act of 17 February 2005 on the informatization of entities performing public tasks (OJ No. 64, item 565, as amended) concerning the minimum requirements for ICT systems in the field of information security.

In order to ensure consistency of information security policies of organizational units, it is assumed that the minister responsible for informatization in consultation with the Minister of National Defence and the Head of the Internal Security Agency may prepare guidelines for information security management systems.

3.4.3. The role of plenipotentiaries for cyberspace security

The organizational units of government administration should define the role of a plenipotentiary for cyberspace security (hereinafter referred to as PCS).

The tasks of a plenipotentiary within the scope of cyberspace security shall include in particular:

1) implementation of the obligations arising from the provisions of legal acts relevant to ensure cyberspace security;
2) development and implementation of procedures for responding to computer incidents which will apply in the organization;
3) identification and conducting periodic risk analyses;
4) preparation of emergency plans and testing them;
5) development of procedures to ensure information of appropriate CERTs about:
   a) the occurrence of computer incidents,
   b) the relocation of an organizational unit, contact information, etc.

The ***Policy*** does not indicate the location of a plenipotentiary for cyberspace security in the structure of an organizational unit, however, the role of a plenipotentiary should be assigned to the person responsible for carrying out the process of ICT security.

3.5. PRINCIPLES OF EDUCATION, TRAINING AND AWARENESS-RAISING IN THE FIELD OF SECURITY

As a part of execution of the ***Policy***, the Council of Ministers recognizes the need to begin work on the implementation of educational activities. It is assumed that the actions in this area will be conducted among the current and future users of CRP. They are designed to reinforce the impact of the two previous measures, strengthen them among the users, and create the possibility of passing to the next stage of implementation of the ***Policy***.

3.5.1. Training of plenipotentiaries for cyberspace security

In order to improve qualifications there is a need to develop a training system for plenipotentiaries for cyberspace security. The project of trainings should place emphasis on the issue of responding to incidents relating to the cyberspace security.

3.5.2. Introduction of ICT security topics as a permanent element of higher education

One of the fundamental aspects of ensuring security of CRP is highly qualified personnel working in the public and private sectors, responsible for maintenance of ICT systems with particular emphasis on resources crucial for the safety of the state. In order to ensure a continuous supply of well-trained professionals in the field of ICT security it is necessary to involve higher education institutions in achieving the objectives of the ***Policy***. The issues relating to the cyberspace security should become a permanent element of education. This applies in particular to technical higher education institutions teaching computer scientists. The situation where designers, computer programmers focus exclusively on functionality, forgetting the principles of creating a secure code, and system administrators give priority to the availability of resources of users forgetting the need to protect the processed information from intruders should be prevented from happening. For this purpose it is necessary to take into account the issues of ICT safety among the outcomes of education specified in the National Qualification Framework for Higher Education.[2]

3.5.3. Education of clerical staff in government administration

The Council of Ministers notices the need for education of government administration employees having access to and using CRP, in the scope of issues concerning the security of ICT systems – according to their positions and risks associated with them.

[2] Regulation of the Minister of Science and Higher Education of 2 November 2011 on the National Qualification Framework for Higher Education, OJ No. 253, item 1520.

3.5.4. Social campaign of educational and preventive nature

The widespread use of systems connected to the Internet by the citizens and the increasing importance of the availability of services offered by cyberspace forces the necessary to raise awareness of the safe methods of using the Internet and to sensitize the citizens to the emerging threats.

Awareness and knowledge on how to prevent and combat threats are key elements in the fight against these threats. Only responsible behaviour of appropriately educated user can effectively minimize the risks arising from the existing threats. It should be emphasized that in the modern world the assurance of ICT security is largely dependent on the knowledge and actions of each user of cyberspace.

Due to the fact that both individuals as well as public institutions, entrepreneurs, social organizations are at risk of crime in cyberspace, the campaign will be multi-dimensional and will take into account the necessary diversity of forms and content of communication, depending on the needs of its recipients. It is assumed that the public campaign will be long-term and widespread.

Due to the ICT security conditioning the implementation of public tasks, the addressees of information campaigns will be, in particular, government administration employees and entities whose resources are included in the ICT infrastructure of CRP.

It is assumed that the educational and preventive campaign will be directed to the public, and in particular:

1) **children and youth** – as the group most susceptible to influence. Education should begin already from an early age in order to develop habits which will protect young people from the dangers lurking on the Web (e.g. from a phenomenon called cyberbullying – violence on the Web, making dangerous acquaintances, obscene content, hacking, addiction to the Internet). Knowledge about the dangers of cyberspace should be received by a child, in the first place, at school at all levels of education (primary school, lower secondary school, upper-secondary school).
2) **parents** – as those responsible for the education of successive generations. Parents bear responsibility for the preparation of children to function in a society, including information society. With the aim to effectively oversee the activities of a child on the Internet, parents should get adequate knowledge about the dangers of cyberspace and the methods of their elimination.
3) **teachers** – since 2004, the education of teachers within the specializations has taken place in accordance with the Regulation of the Minister of National Education, defining the standards of teacher education.[3] As a part of the mandatory classes of higher education teachers gain basic knowledge in the field of information technology, including the safe and conscious use of ICT systems.

[3] Regulation of the Minister of National Education and Sport of 7 September 2004 on teacher education standards (OJ No. 207, item 2110).

Social campaign directed at children, youth and their parents should be largely implemented in educational institutions of all levels.

The campaign will be carried out also through the mass media. Mass media – as an important partner in promoting security issues, CRP and popularization of projects contained in the ***Policy*** – will improve the effectiveness of execution of the objectives. With its help during the implementation of the ***Policy*** it will be also possible to carry out informational and educational campaigns. For this purpose, the national, regional and local media will be involved. The assumption is that as a part of the social campaign information about the ICT security and educational and organizational and legal undertakings within the Policy will be presented on the websites of the Ministry of Administration and Digitization and on the website of the Governmental Computer Security Incident Response Team CERT.GOV.PL. At the same time, an effective communication of content, initiatives and results of the ***Policy*** to broad social and professional circles is assumed.

3.6. PRINCIPLES OF TECHNICAL ACTIONS

On the basis of procedural and organizational activities (e.g. plan for dealing with risk), the last stage of implementation of the ***Policy*** should be technical actions. Their goal will be to reduce the risk of threats from CRP. Performance of this stage will take place through launching specific projects.

3.6.1. Research programmes

Supporting research initiatives relating to the ICT security is essential for the effective implementation of the ***Policy***. The formula of support should encourage to conducting joint research by the actors in the sphere of ICT security from the sphere of public administrations, research centres and telecommunications companies and purveyors providing services by electronic means.

It is assumed that the entity coordinating the implementation of the ***Policy*** provisions in this regard will be the Ministry of Science and Higher Education (MNiSW), as the one responsible for the research and development work. The list of initiatives which take account of the dynamics of the state of knowledge will be defined at the level of specific projects, developed on the basis of the ***Policy*** and may be revised at the initiative of the competent bodies responsible for its implementation.

3.6.2. Expansion of ICT security incident response teams in government administration

In order to be able to effectively carry out activities related to ensuring the security of CRP, including response to ICT security incidents, it is necessary to provide adequate technical facilities which will not only enable the execution of current tasks, but will

also take into account the increasing demand for specialized ICT systems in the future.

All the teams, after the unification of responsibilities and response procedures, as well as determination of the constituency, would create a national computer security incident response system, which, in addition to cooperation, would also cover joint conferences, training and exercises.

3.6.3. Development of an early warning system and implementation and maintenance of preventive solutions

The ICT Security Department of the Internal Security Agency together with the CERT Poland, which is part of the Research and Academic Computer Network (NASK), has implemented an early warning system against threats from the Internet – ARAKIS-GOV. Development of the system will be implemented in accordance with the specific project.

At the same time, bearing in mind the progress taking place in ICT technologies and the related trend of emergence of increasingly sophisticated threats, taking initiatives to promote the creation of more and more modern solutions supporting the ICT security is assumed during the implementation of the ***Policy***.

The aim should be to use the widest possible range of different types of security systems to ensure the security of critical ICT resources.

3.6.4. Testing the level of security and the continuity of actions

As a part of testing the level of security and ensuring continues implementation of processes of CRP, the PCS should organize and coordinate periodic tests of both the level of technical, organizational protection and procedural solutions (e.g. procedures of continuity of actions or supra-departmental cooperation). The results of exercises will be used for evaluation of the current resistance of cyberspace to attacks, while the conclusions will form the basis for the preparation of recommendations for further preventive measures.

3.6.5. Development of security teams

The CERT-type teams are competency centres offering substantive help at the stage of creating appropriate structures and procedures. In addition, they are also used to solve problems during their operation in various organizational units of government administration or of entrepreneurs. Each institution, within own personal resources and technical means available, may establish its own local incident response team whose operation is coordinated in accordance with point 4.2.

Moreover, the tasks of Computer Security Incident Response Teams should include maintaining internal informational sites. The sites will be the main sources of information about the ICT security for people involved in ICT security in government administration institutions, as well as other persons interested in this subject.

In particular, the site will be a place for publication of the following information:

1) news related to ICT security;
2) information about potential risks and threats;
3) security bulletins;
4) different types of guides, best practices;
5) reports and information on the trends and statistics;
6) forum for the exchange of information and experience of those involved in activities related to ICT security.

The sites will function as points for reporting ICT security incidents. A site will be designed so that users without much computer knowledge can report the incident or find information where to report the incident.

4. Implementation and delivery mechanisms of the provisions of the document

It is assumed that the objectives and principles of the ***Policy*** will be executed taking into account risk assessment and implemented within the specific projects.

4.1. Supervision and coordination of the implementation

Due to the international nature of the ***Policy*** the body supervising its implementation is the Council of Ministers. The entity coordinating the implementation of the ***Policy***, on behalf of the Council of Ministers, is the minister responsible for informatization.

4.2. The national response system for computer security incidents in CRP

The government of the Republic of Poland establishes a three-level National Response System for Computer Security Incidents in CRP:

1) Level I – the level of coordination – the minister responsible for informatization;
2) Level II – computer incident response:
   a) the Governmental Computer Security Incident Response Team CERT.GOV.PL – at the same time performing the tasks of the main national team responsible for coordinating the process of handling computer incidents in CRP,
   b) Departmental Centre for Security Management of ICT Networks and Services performing tasks in the military sphere,
3) Level III – the level of implementation – administrators responsible for individual ICT systems operating in cyberspace.

The established response system ensures the exchange of information between teams of government administration and CERTs (CERT Poland, TP CERT, PIONIERCERT), CSIRT, ABUSE, telecommunications companies, within the meaning of the Act of 16 July 2004 – Telecommunications Law (OJ No. 171, item 1800, as amended), and purveyors providing services by electronic means, within the meaning of the Act of 18 July 2002 on providing services by electronic means (OJ No. 144, item 1204, as amended), in accordance with applicable laws, and in particular in accordance with the Act of 29 August 1997 on the protection of personal data (OJ of 2002, No. 101, item 926, as amended) and the Act of 5 August 2010 on the protection of classified information (OJ No. 182, item 1228).

4.3. INFORMATION EXCHANGE MECHANISM

An efficient system of coordination will ensure the exchange of information gained from the international cooperation between the governmental, military and civilian teams, in accordance with applicable law, and in particular in accordance with the Act of 29 August 1997 on the protection of personal data (OJ of 2002, No. 101, item 926, as amended) and the Act of 5 August 2010 on the protection of classified information (OJ No. 182, item 1228).

This system will, among other things, identify alternative channels for the exchange of information and introduce periodic tests of effectiveness of the information exchange processes.

4.4. METHODS AND FORMS OF COOPERATION

As a part of implementation of the ***Policy***, forms of cooperation between the authorities responsible for the security of cyberspace and responsible for combating computer crime of criminal nature should be developed. These forms of cooperation will have both a working form, in order to minimize delays of computer incident response, as well as a formalized form – serving the elimination of jurisdiction problems.

4.5. COOPERATION WITH ENTREPRENEURS

It is essential to activate entrepreneurs whose protection from the cyberspace threats is important from the point of view of the proper functioning of the State.

This group should include entrepreneurs active in particular in the following sectors:

1) supply in energy, energy resources and fuel,
2) communications,
3) ICT networks,
4) finances,
5) transport.

The ***Policy*** assumes taking up actions activating the cooperation between entrepreneurs managing their own ICT infrastructure, falling within the ICT infrastructure of CRP of a similar nature, and thus exposed to similar types of vulnerabilities and methods of attacks. One of the forms of cooperation will be the creation of bodies appointed for the internal exchange of information and experiences and the cooperation with the public administration in the field of security of ICT infrastructure of CRP.

4.5.1. Cooperation with manufacturers of ICT equipment and systems

Important partners for government institutions and other entities responsible for the ICT security and increasing the security in cyberspace are manufacturers of hardware and software. Development of cooperation with these partners, including the exchange of experiences and expectations, should be one of the most important factors which significantly influence the public and specialist education system, as well as the quality of the created systems. The cooperation of entities responsible for the ICT security with manufacturers of security systems should be of particular importance for the expansion of the spectrum of available tools.

The aim should be to provide the users with the largest range of solutions for the broadly understood ICT security and protection of information.

4.5.2. Cooperation with telecommunication entrepreneurs

Due to the global nature of threats, a close, coordinated cooperation in the field of cyberspace security between the Office of Electronic Communications (UKE), telecommunication companies and the users of CRP is required.

4.6. INTERNATIONAL COOPERATION

Due to the global nature of the problems related to cyberspace security, an important element is to maintain and develop international cooperation in this regard.

The government of the Republic of Poland recognizes the need for Poland, through its representatives, government agencies, public institutions and cooperation with non-governmental institutions, to initiate and conduct active steps to increase the security of CRP and the international security.

5. Financing

The ***Policy*** will not imply additional resources from the state budget to finance the assumed activities in the year of its entry into force, because the current organizational units of government administration have been already partially fulfilling the objectives set out in the ***Policy***. Therefore, it is assumed that after its approval each organizational unit will clearly indicate the tasks already performed and the expended financial resources.

This document assumes the continuation of the activities carried out and planned by the Team referred to in point 3.4.1.

It is assumed that since the entry into force of the ***Policy*** individual units are estimating the costs of the implemented tasks corresponding to the tasks imposed by this ***Policy***.

The presented estimates of costs will allow for their inclusion in the plan of the following fiscal year with a clear indication that they relate to cyberspace security.

Individual organizational units transmit data on the costs of implementation of tasks estimated by them to the minister responsible for informatization. The costs of the implementation of tasks will be determined by the results of the risk assessment and presented in specific projects with ascribing them to individual units and an indication of the sources of funding.

Necessary expenses related to the implementation of the ***Policy*** will be financed within the limit of budgetary expenditure provided for in the relevant part of the budget in the budget act for a given year.

6. Assessment of effectiveness of the Policy

Due to the innovative nature of this document, detailed indicators of implementation of the provisions of the ***Policy*** will be developed following the risk assessment.

It is essential, from the entry into force of the ***Policy***, for individual organizational units to analyse and suggest indicators of the implementation of tasks on whose basis information will be aggregated and global indicators of the objectives of this document will be developed. It is assumed that the presented proposals of global indicators will be used in updating the ***Policy*** and allow for assessment of the degree of implementation of the planned objectives and tasks related to the security of CRP.

The degree of implementation of projects related to the implementation of the strategic objective and specific objectives of the ***Policy*** will be evaluated within the specific projects by the following criteria:

1) the degree of saturation of all organizational units which have security systems and early warning systems in relation to the number of public administration employees;
2) the level of integration:
   a) the method and procedure for the exchange of information between teams, ensuring confidentiality, integrity and availability,
   b) the possibilities for and scope of achieving a common, dynamic imagery of cyberspace covered by this ***Policy***,
3) the degree of standardization – the degree of implementation of the standards, categories of incidents and procedures;
4) the degree of equipping the systems in a comprehensive anti-virus software, firewalls, anti-spam with relation to those requiring protection (identification of resources).

The following measures will be used to evaluate the effectiveness of specific projects, created on the basis of this ***Policy***:

1. Effectiveness measures – measure the degree of achieving the objectives and can be applied at all levels of task classification.

Sample effectiveness measure:

– the number of closed incidents in relation to the total number of categorized incidents.

2. Product measures – reflect performance of a given task in a short period and show specific goods and services produced by the public sector. Product measures – measure the degree of implementation of operational objectives.

Sample product measures:

– the number of responses to incidents reported by citizens,

– the number of handled incidents.

3. Result measures – measure the effects achieved through the actions included in a task or under a task, carried out by the appropriate expenditure, at the level of task/subtask/action. Measure the results of undertaken actions. Result measures – measure direct effects of undertaken actions in the short or medium term.

Sample result measures:

– shortening the time of handling an incident,
– the average response time to an incident.

4. Impact measures – measure the long-term consequences of implementation of a task. They can measure the direct effects of the implementation of a task which become apparent after a long period of time. Sometimes, the impact measures refer to the values which are only partially the result of the implementation of a task (the results are also affected by other external factors).

Sample impact measure:

– the increase of the sense of security on the Internet in Poland (research of CBOS – Public Opinion Research Centre). The degree of implementation will be assessed in percentage, while 100% means the implementation of all the tasks under specific projects developed on the basis of the ***Policy***.

Within one year from the entry into force of the ***Policy***, each involved entity, referred to in point 1.4. paragraph 1 of this document, shall estimate (in %) to what extent the principles of the Policy have been already achieved.

6.1. EXPECTED EFFECTS OF THE POLICY

The following long-term effects of actions resulting from the implementation of this ***Policy*** and specific projects developed on its basis are expected:

– a higher level of security of CRP and a higher level of resistance of the state to attacks in CRP,
– a policy concerning the cyberspace security consistent for all the involved agents,
– lower effectiveness of terrorist attacks in CRP and lower costs of removing the results of cyberterrorist attacks,
– effective system of coordination and exchange of information between public and private entities responsible for ensuring the security of cyberspace and those administering the resources constituting the critical ICT infrastructure of the state,
– greater competence of actors involved in the ICT infrastructure security of the State functioning in cyberspace,

– greater confidence of the citizens in the proper protection of the state services provided by electronic means,
– greater public awareness as to the methods of the safe use of systems available electronically and ICT networks.

6.2. EFFECTIVENESS OF ACTIONS

The measure of effectiveness of actions undertaken as a part of the ***Policy*** will be the assessment of the created regulations, institutions and relationships which will enable the actual existence of an effective cyberspace security system. One of the basic methods of influencing the effectiveness of the planned activities performed by many institutions is to establish the scope of tasks of each of the entities and to determine the responsibility for their implementation.

6.3. MONITORING THE EFFECTIVENESS OF ACTIONS AS A PART OF THE ADOPTED POLICY

Reports on the progress of implementation of the ***Policy*** will be sent by the bodies mentioned in point 1.4 to the minister responsible for informatization.

6.4. CONSEQUENCES OF VIOLATING THE PROVISIONS OF THE POLICY

Each government administration entity shall apply the provisions of this ***Policy***, regardless of liability specified in the provisions of generally applicable law.

Violation of the rules set out in this Policy may result in the exclusion of the entity from the information society and emergence of barriers in access to public information. Adequate protection, security of the processed data and reliability of the ICT systems are the highest values faced by the modern systems. Entities implementing the Policy in question should indicate ways for securing information systems, procedures for the ICT security breach in information systems in security policies of these systems. The implementation of the provisions of this document is to provide an adequate response, evaluation and documentation of cases of the system security breaches and ensure an appropriate way of responding to incidents in order to restore an acceptable level of security. An important obligation is to immediately inform an administrator or an appropriate CERT about detected incidents and take or refrain from actions aimed at handling them.

WARSAW, 25 June 2013