

CR National Strategy for Information Security
CR NSIS

Contents

Contents	2
Introduction.....	3
Legal Basis.....	3
Relationship to other CR and EU Strategic Documents	3
The Importance of Information Security	5
Priorities, Tasks and Strategic Goals	6
Objective I: Improving Information Security Management and Risk Management.....	7
Objective II: Developing Knowledge of Information Security.....	8
Objective III: Support for National and International Cooperation in Information Security.....	9
Objective IV: Support of the Use of Best Practices for Information Security.....	10
Objective V: Support for Human Rights and Freedoms	11
Objective VI: Support for the Competitiveness of the Czech Economy	12
Strategy and Measures for Development and Implementation	13
Economic and Social Impact.....	14
Definitions and Fields of Information Security	15

Introduction

Information and communication systems enable a large number of areas of society to function properly, and indeed the existence of these areas depends on these systems.

The rapid expansion of information and communication systems, which are part of every aspect of people's lives, and their wide availability has increased the risk of these systems becoming attacked, either intentionally, by accident, or by human error or through ignorance of the medium. Increasing attention must therefore be paid to securing these systems against attacks or abuse.

Properly functioning information and communication systems are the foundations of our national economy. The secure functioning of these systems is based on rules for information security which have been set out correctly and which have been duly complied with and checked. This requires the coordinated efforts of our overall society, the Government, the public authorities, commercial and non-commercial entities and our citizens.

Given the current speed and anonymity of attacks on information and communication systems, it is difficult to identify the difference between terrorist, criminal or random acts.

The vision of the CR National Strategy for Information Security (CR NSIS) is as follows: to increase the confidence of citizens and commercial and non-commercial entities in the information society; to improve the overall management of information security; to increase the understanding of information security; to increase international cooperation; to collate and recommend best practises for information security management; ensure that basic human rights are protected when using information and communication systems, and to support the competitiveness of the Czech economy.

This Strategy is an articulation of the CR Government's efforts to achieve its strategic goals for information security.

This Strategy creates a joint platform for securing information for the public administration authorities, commercial and non-commercial entities and individual citizens alike.

Legal Basis

The CR NSIS has been compiled within the framework of the protection of information legislation (which not only applies to the information and communications technology environment), at the level of the rights and legal interests of individual entities, information security requirements laid down by EU directives and OECD recommendations and in relation to key standards.

The legal framework for information protection in the CR is made up by the Acts set out in Annex No. 2.

Relationship to other CR and EU Strategic Documents

The drafting of this document was initiated by the "State Information and Communications Policy: e-Czech 2006" White Paper (*approved by CR Government Decree No. 265 of 24 March 2004*) and is directly connected to the "CR Security Strategy" (*approved by CR Government Decree No. 1254 of 10 December 2003*), elaborating its information security section.

The CR NSIS introduces to the Czech Republic the principles set out in the "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" and supports the harmonisation of Czech legislation and technical and technological standards with their EU equivalents.

The EU legislation takes the form of regulations and directives which are applicable to all member states. The most important of these for information security are set out in Annex No. 2.

The Importance of Information Security

A solid level and quality of information security is important for protecting the rights and interests of citizens, commercial and non-commercial entities and for protecting the interests of the State and ensuring the proper functioning of public administration bodies as well as their public image. Insufficient information security could threaten the security and economic interests of the State, the private sector and citizens and could weaken the trustworthiness of individual entities. Any losses incurred and information lost could cause extra work and costs which would not have been incurred if there had been sufficient preventative protection of this information.

While the information society is being built, the importance of direct electronic access to information and services provided by public administration authorities and commercial and non-commercial entities increases. The expansion of direct access to information in information systems increases the security risk level of the services provided and therefore proportionately increases protection requirements for information and communication systems and for processing information.

From an information protection point of view it is just as important to have secure and failure-free operations of information and communication systems, as well as to ensure that the information they contain is correct, reliable, accessible, untampered with, trustworthy and up-to-date.

A sufficient level of information security is a pre-requisite for using electronic services.

Knowledge on information security requirements can be provided through training, cooperation and continuous raising of public awareness.

The backbone of the information infrastructure is the Internet, which connects computer networks and enables the functioning of a wide range of services and infrastructure. The Internet plays a considerable role in business and commerce, the provision of public administration services to citizens, and commercial and non-commercial entities and of course provides a means of communication for people.

The problem for the Internet and information and communication systems is the threat from organised and non-organised individual and group attacks which could affect the assets of these systems and eventually the economy and the functioning of the State's infrastructure. A large number of attacks are currently characterised by having low technological requirements but high technical knowledge on the part of the attacker. The danger comes from the availability of the resources used in attacks and the methods and level of sophistication of such attacks.

The development of the competitiveness of the information society depends to a certain extent on the ability to protect the national wealth. Knowledge and information are a part of this wealth and it doesn't matter if they are owned by the State, commercial or non-commercial entities or individuals.

Priorities, Tasks and Strategic Goals

The National Strategy for Information Security of the Czech Republic creates a platform for building a credible and democratic information society based on a legal foundation, which takes care to secure information in all areas of peoples' activities and enables information to be used and shared freely and securely.

The purpose of the NSIS CR is to influence the implementation of best practises and cooperation of all sectors of society in administrating and building trustworthy information and communication systems. At the same time it sets out the role and responsibilities of central bodies of the public administration for supporting information protection.

The basic priority is to protect information and communication assets from threats which are aimed at information and communication systems, and to reduce potential damage to these systems by minimising risk.

This Strategy will be considered as being the basic document used when creating policies, guidelines, methodology instructions, rules, principles, handbooks, operational regimes, plans and recommendations, etc.

The implementation of credible information and communication systems and their operation and administration must be part of the interests and responsibility of all levels of the public administration, the private sector and the general public.

The priority areas for this strategy are:

1. Information security management and risk management,
2. Information security knowledge,
3. National and international cooperation for information security,
4. Using best practises in information security,
5. Human rights and freedoms protection,
6. The competitiveness of the Czech economy.

Each priority area contains a strategic goal. Measures are set out for each individual strategic goal, which, when implemented, will fulfil that goal. Each individual measure consists of activities which are compiled at project or task level.

Objective I: Improving Information Security Management and Risk Management

The goal is to develop and improve the quality of information management systems and implement these as a part of the overall management of organisations, which means obtaining a higher quality of management. These systems must ensure the security of all forms of information, both in the computer and the “classic administration” environment.

The secure use of information and communication systems is currently a necessity and has an increasing importance for all users.

Improving all activities within information security management systems means covering all the aspects of information security equally, and duly documenting, implementing, checking and continually assessing these aspects.

Risk management must become an integral part of information security management.

In view of the new threats and the associated risks it is necessary to perform systematic monitoring together with assessments of the actual situation and to implement effective counter-measures. The affects of threats can be effectively minimised by implementing timely (pre-emptive) counter-measures.

Measures for Objective I:

1. Implementing best practises as part of information security management

a) *Support best practises in security management and support the implementation of information security management systems.*

2. Systematic threat monitoring

a) *Perform systematic and regular threat monitoring and analyses of the actual situation.*

3. Implementation of early warning and response systems

a) *Using the Public Administration Portal, create a system for early warning, response and information exchange for reducing the risk of threats to the assets in information and communication systems.*

b) *Establish a national centre for managing, monitoring and analysing the secure environment of information and communication systems in the Czech Republic.*

4. Monitoring the effectiveness of proposed counter-measures

a) *Implement the monitoring of the effectiveness of security risk and proposed counter-measure management processes as a part of security risk management systems.*

5. Improving the information security of public administration bodies

a) *Provide information security in the computer and the “classic administrative” environments of the public administration.*

b) *Provide supervision of the public administrations communication infrastructure.*

c) *Increase the efforts of the State’s security services related to protection against information crime and cyber-terrorism.*

d) *Implement a uniform classification system for information.*

6. Protection of the State’s critical information infrastructure

a) *Support the implementation of information security instruments for protecting the information and communication systems of the State’s critical infrastructure.*

b) *Create the necessary procedures for a rapid transfer from a normal to a critical status for the information and communication systems of the State’s critical infrastructure.*

c) *Announce principles and draft methodological procedures for setting the required minimum resistance for the State’s critical infrastructure information and communication systems.*

d) *Increase the efforts of the State’s security services related to defending against attacks on the State’s critical infrastructure information and communication systems.*

Objective II: Developing Knowledge of Information Security

Many crashes and breakdowns of information and communication systems occur as a result of insufficient levels of understanding of the computer environment by the general public, regular management and even by professionals in the field.

These faults due to insufficient knowledge represent a serious risk not only in the operation of these systems but particularly for the protection of the information contained in them.

The causes are generally the low level of awareness of the need for information security when working with information, the lack of professionally trained experts and the non-existence of Czech certification programmes for professionals working in information security or directly handling information in information systems.

The ability to use information security instruments and information literacy is becoming a new civil skill.

Competency in information protection has become a new professional qualification.

All users of information and communication systems must be aware of the risks related to their working with information as well as the possibilities of mitigating these risks. Each user and owner of information and communication systems should know what the consequences of unauthorised use of these systems as an instrument of attack against other infrastructure could be. At the same time they should make maximum efforts to secure these systems.

Measures for Objective II:

1. Increase awareness in citizens, commercial and non-commercial entities and public administration bodies of information security, security risks and defence possibilities.
 - a) *Support awareness of information security between companies, the public administration and other organisations.*
 - b) *Increase awareness of information security by way of disseminating relevant information.*
 - c) *Disseminate knowledge of best practises in information security.*
 - d) *Raise awareness in individuals by education on the subject of information security.*

2. Introduce training and educational programmes
 - a) *Define a target level of knowledge for the individual roles in information security.*
 - b) *Support the private sector in implementing training programmes.*
 - c) *Include information security in the training programmes of civil servants.*

3. Support an overall national awareness programme for information security
 - a) *Introduce information security into the curriculum of all levels of training.*
 - b) *Spread awareness and improve cooperation with the media when providing information for publication related to information security.*

4. Increase the effectiveness of training programmes
 - a) *Spread the best methods of raising awareness into all education institutions.*
 - b) *Include the information security issue in training programmes for information literacy.*
 - c) *Support the improvement of the general standard of trainers.*

5. Increase awareness in users of the importance of using information and communications technology products and services with security certification
 - a) *Spread awareness of the importance of security certification for information and communication technology products and services.*

Objective III: Support for National and International Cooperation in Information Security

The Internet as a global information and communication network linking the CR with the rest of the world brings positive effects as well as global threats in the form of attacks which may be carried out from any place in the world and may jeopardise geographically very distant systems at a very high speed which multiplies the threat.

The Czech Republic must be capable of securing and protecting its systems and computer networks. For this to be possible, cooperation is needed both at the national level and at the international level. This national and international cooperation will assist in creating, developing and spreading best practises, threat identification, the implementation of joint defensive and remedial measures, and in identifying attackers.

The Czech Republic participates in many cooperation programmes within the European Union and the Organisation for Economic Cooperation and Development (the OECD). It is in the interests of the Czech Republic to further develop this cooperation and a commitment with this aim in the CR NSIS is an important step in strengthening international trust and cooperation.

Information security must be understood as being an issue for the entire information industry in cooperation with users and the public administration, and not just an issue for a limited circle of companies.

Measures for Objective III:

1. Implementation of effective cooperation and coordination at the national level

- a) *Support the Public Administration Portal as a uniform information resource for providing efficient communication on information security.*
- b) *Pay sufficient attention to considering information security requirements when creating national legislation standards and guidelines.*
- c) *Establish a CR Committee for Information Security with the participation of public administration stakeholders.*
- d) *Establish a CR Information Security Forum with the participation of the experts in the field and support cooperation between business and other organisations active in information security.*

2. Implementation of active international cooperation

- a) *Actively participate in preparing legislation and standards and other cooperation relating to information security within the European Union and outside it (as part of OECD, ISO, CERT, ENISA, ASEM, NATO and other international organisations).*
- b) *Join in creating national and international monitoring and warning networks which will be capable of uncovering and protecting against electronic attacks at the moment these occur.*
- c) *Support cooperation between international public and private sectors via the CR Information Security Forum.*

3. Improve cooperation for national defence against information threats

- a) *Improve cooperation as part of coordination between the offices responsible for the State's critical infrastructure information and communication systems and the other relevant security services.*
- b) *Improve the capabilities for identification, coordination and remedial measures in the case of potential attacks.*

Objective IV: Support of the Use of Best Practices for Information Security

In order to exchange best practices an efficient way of carrying out this exchange must be provided. Even though standards are not binding under Czech law, yet they could become binding via a reference from a binding regulation, it is generally advantageous for them to be upheld at both a national and an international level.

A list of the most important standards relating to information security is set out in Annex No. 2.

Measures for Objective IV:

1. Exchange of experience
 - a) *Lay out best practice using the Public Administration Portal.*
 - b) *Use the Public Administration Portal as a platform for exchanging experience in the field of information security.*

2. Use best practise in building information security
 - a) *Support systemic solutions for information security based on procedures.*
 - b) *Support the implementation and efficient administration of management systems for information security supported by the Plan – Do – Check – Act model.*

3. Utilisation of Standardisation
 - a) *Support cooperation between the public administration and the national standardisation body when issuing standards for information security.*
 - b) *Support standardisation aimed at broader usage of open standards and programmes using open source code.*

4. Increase the user friendliness of systems
 - a) *Support the introduction of user friendly systems which will allow for the “Human Factor” in the field of information security.*

Objective V: Support for Human Rights and Freedoms

The basic human rights, which must be maintained, include the right to protection of privacy, freedom of speech and the right to information. Businesses need to protect their trade secrets, information on their customers and all their new knowledge base (know-how, intellectual property).

All Czech citizens must have easy access to the information they are authorised to obtain, including handicapped citizens who are provided with these services via special instruments of the information systems.

At the same time each citizen must be able to choose a user friendly solution for information protection.

A basic condition for creating an information society is citizens' confidence in its development.

The confidence of citizens and companies in the information society can be increased by improving the information society itself by protecting privacy, human rights and freedom.

There must be universal confidence that information is correct, that messages are sent reliably, and that complete confidentiality is respected when information is processed and filed and that this information cannot be abused.

Measures for Objective V:

1. Provide a legal basis for the protection of the basic human rights and freedoms
 - a) *Ensure that constitutionally guaranteed rights to freedom of speech, access to information for all groups of people, privacy protection and information confidentiality are upheld and that these rights are taken into consideration in statutes and statutory instruments.*
 - b) *Create conditions in which businesses can and do protect their trade secrets, information on their customers, their new knowledge base and other aspects of their business activities.*

2. Create an operational environment which provides for information security and privacy protection
 - a) *Provide a sufficient level of information security for all public administration electronic transactions.*
 - b) *Perform active checks on the confidentiality of transactions performed using personal data.*
 - c) *Support the use of reliable (security-certified resources and services) and user-friendly tools for providing information security and the possibility of choosing information security products and services.*

Objective VI: Support for the Competitiveness of the Czech Economy

Information is a very valuable form of capital on the global market. The development of an information society and the accessibility and usability of information has an influence on international competitiveness.

Open access to information must be provided, whilst ensuring a secure and stable environment. This will contribute to establishing new business opportunities for businesses.

Access to national and international information is an opportunity which improves the competitiveness of Czech business and creates resources which can be used to further develop our society, and which then results in a positive social impact.

International legislation and best practises help to promote information security and support the competitiveness of the CR in the international environment.

Measures for Objective VI:

1. Support for the accessibility and usability of information

- a) *Support for the accessibility and usability of information security knowledge and technology for the public administration, commercial and non-commercial entities and Czech citizens in a way which does not discriminate against any of these groups.*
- b) *Support for cooperation in information and best practise exchange projects for information security between the public administration and the private sector at a national and international level.*

2. Monitoring and Assessment of legislation and best practices

- a) *Regular assessment of international legislation, agreements, trends and recommendations related to information security, electronic commerce and electronic transactions, publishing conclusions and recommendations along with these assessments and implementing these in the Czech environment.*
- b) *Draft recommendations for information security best practices so that these may be used to the broadest possible degree.*
- c) *Support the convergence of information security best practice procedures between the public administration and the private sector.*
- d) *Introduce information security requirements to contractual relations between different entities.*

3. Remove barriers

- a) *Create conditions in order to avoid restrictions on the trading potential of the private sector through open solutions, transparency, non-discrimination and a choice of products and services for information security based on open standards.*
- b) *Provide stability to the computer and the “classic administrative” environment for obtaining information.*
- c) *Support the use of services and transactions by improving confidence in the computer and “classic administrative” environment.*

Strategy and Measures for Development and Implementation

The implementation of this strategy is the key to building a credible information society. In order to implement this strategy, the cooperation of all users of information and communication systems is necessary.

The Strategy lays the foundation for good cooperation in the protection of information and creates room for coordinated planning in order to achieve strategic objectives in an efficient manner.

The Czech Ministry of Informatics is responsible for the development, implementation, up-dating and evaluation of the achieving of NSIS. The Czech Ministry of Informatics sets up the “Committee for information security of the CR” as the coordination body with the participation of all public administration bodies involved in the field of information security.

This Committee is the platform for the cooperation of all parties involved in order achieve common objectives in the field of information security.

Representatives of the key public administration bodies for information security and the implementation of the NSIS CR are in this Committee.

In order to achieve strategic objectives in information security efficiently, the Committee shall lay down a schedule for the implementation of activities.

The Committee shall through the Minister of Informatics provide annual reports to the Government on the progress of the Strategy implementation and the need of up-dating it.

Under the present legislation, a number of public administration bodies are responsible for the implementation of the protection of information and for the development of information security. The responsibilities for information security in public administration are listed in Annex No. 1 of this Strategy.

In the field of public administration, the responsibility, implementation, development and control of information security is provided separately by different public administration bodies.

Economic and Social Impact

The role of public administration in resolving information security issues is acceptable only if the benefits of an intervention offset the related costs. This principle is important mainly in cases where there is a private sector solution aimed at potential threats. For each individual case, the principle applies that everything should be done in view of the cost and impact of the state intervention concerned in comparison to alternative actions or no action at all.

The activities of the public administration for securing the computer and “classic administrative” environment are meant for the following objectives: the protection of computer networks and systems important for national safety, indication of, warning and protection against organised attacks capable of damaging the economy. Activities of the public administration should also foster technological development which would allow the private sector to better secure privately owned parts of the national infrastructure.

In economic terms, the objective of this Strategy is to protect investment and more efficient use of public resources by introducing effective measures in the field of information security.

Strategic objectives may be achieved on the basis of plans and strategic decisions which must be made in line with the annual national budget.

The Strategy shall contribute to more secure communication environment in trade which will increase the competitiveness of the Czech economy.

It will also raise the awareness of information security on the part of all information systems users.

This Strategy is conceived as a support document for all entities in the CR; however, it does not prejudice their responsibility for the choice and implementation of information security.

The Strategy does not affect the present sharing of responsibility for information security and the existing organisational structures.

Definitions and Fields of Information Security

The terms set out in this chapter serve the needs of this Strategy.

Information security is a comprehensive and dynamic part of all the activities performed in our society. Information security must cover all its aspects.

It is a part of information security to provide the following:

- 1) **Accessibility** – ensuring that information and the related activities is accessible to authorised users (entities) according to their requirements and at the required time;
- 2) **Confidentiality** – ensuring that information is accessible only to persons (entities, processes) authorised to have access to that information;
- 3) **Integrity** – protection of accuracy (from modification – unauthorised changes) and ensuring the information is complete;
- 4) **Responsibility** – is ensured by individual responsibility;
- 5) **Reliability** – ensures consistent behaviour and results.

Information system – is a functioning unit or its part providing for the systematic gathering, processing, storing and access to information. It includes data and information sources, carriers, technical, programme and work instruments, technology and procedures, related standards and workforce.

Information security – is a system of inter-linked measures for the organisation, administrative, personnel and physical security as well as measures of information and communication technology to ensure accessibility, confidentiality and integrity of information.

Information and communication technology – is understood as being any equipment which is used for processing and transferring information, i.e. in particular computer and communications equipment and its programmes.

Communications infrastructure – is a communication system environment where targeted transfer of information is carried out.

Assets – are parts of an information and communication system which have a certain value that can be reduced by an impact of a threat and should therefore be protected using the measures of information security (i.e. technical equipment, communications equipment, software equipment, information, knowledge).

Vulnerability – is a weakness in an information or communication system which can be abused to cause damage and loss of assets.

Threat – refers to the possibility of abusing a vulnerability in an information or communication system to carry out an attack and cause damage to assets.

Attack – is an intended or unintended use of a vulnerability of an information or communication system resulting in damage to assets.

Risk – refers to the probability that a particular threat uses a vulnerability in an information or communication system.

Best Practices – repeated (transferable) best practices, procedures, habits, etc. tried and tested in practice.

Information Society – is a society based on the use of information and communication technologies. It is based on a continuous exchange of knowledge and information and its use which requires the ability to understand it. Such a society considers the creation, the spread and handling of information to be the most important economic and cultural activity.

Critical Information Infrastructure of the State – serves to provide proper information security ensuring the functioning of the critical infrastructure of the State and refers to complex information and communication systems and services. It includes e.g. telecommunications, computer systems and software equipment, transmission networks, services provided, etc.