ORDINANCE ON THE GENERAL REQUIREMENTS FOR INTEROPERABILITY AND INFORMATION SECURITY

In force as of 25 November 2008
Adopted by CoM Decree Nr.279 of 17 November 2008
Promulgated State Gazette, Nr. 101 of 25 November 2008

Chapter One

GENERAL PROVISIONS

Article 1. (1) The Ordinance shall provide for:

1. the general requirements for interoperability and network and information security for the needs of the provision of internal electronic administrative services and the exchange of electronic documents between the administrations;

2. the keeping, storage and the access to the Register of the standards;

3. the manner of accreditation of the persons referred to in Article 57, (1) of the Law on E-Governance and the requirements for their activity;

4. the methods for assessing the conformity to the requirements for interoperability and network and information security;

5. the requirements for keeping, storage and access to the list of the accredited persons referred to in Article 57, (1) of the Law on E-Governance and to the list of the certified information systems.

(2) The Ordinance shall not provide for the network and information security of the information systems of the administrative bodies and the rules for information security in the use of classified information.

Article 2. (1) The obligations of the administrative bodies under the Ordinance shall be applicable also in respect of the persons executing public functions and of the organizations providing public services, in providing internal administrative services, except otherwise provided in a law.

(2) The application of the provisions of Chapter three and the use of information systems certified under the procedure of the Ordinance can be done by the persons executing public functions and by the organizations providing public services.

Article 3. The compliance with the requirements for interoperability and network and information security shall be guaranteed through:

1. certification of the information systems and products in accordance with Chapter six;

2. the functionality of the Unified environment for electronic documents exchange (ESOD), which allows only exchange of documents entered into the Register of information objects and with a content corresponding to the requirements entered into the Register;

3. certification and audit of the administrations in respect of an Information security management system according to the International standard ISO 27001:2005;

4. control on the part of the Chairman of the State Agency for Information Technology and Communications (SAITC) in implementation of Article 60 of the Law on E-

Governance, and in compliance with the Methods for current control of interoperability and network and information security, approved by him.

Chapter Two

INTEROPERABILITY

Section I
Connectivity requirements between the information systems of the administrative bodies

Article 4. (1) The administrations shall be obliged to send and to receive electronic documents among each other for the needs of provision of internal electronic administrative services through the ESOD.

(2) Exceptions under paragraph 1 shall be allowed:

1. when the administration does not have the technical capability for documents exchange through ESOD;

2. when the ESOD is not functioning as a result of technical failures, prophylaxis or other reasons.

Article 5. (1) In cases when the electronic documents are sent by exception through open networks, the communication interfaces and the protocols for exchange should correspond to the compulsory standards and the legal acts specified in the section "Communication and exchange procedures" in the Register of the standards.

(2) In the cases referred to in paragraph 1, when the documents are sent on-line under a standardized protocol through a publicly accessible web-based application, the communication interfaces and the exchange protocols should correspond to the compulsory standards entered into the Register of the standards.

Article 6. (1) Direct connection between information systems of various administrative bodies shall be admitted only in cases when the technical facilities working in the conditions of interoperability do not satisfy peculiar requirements for integrity, quick action and confidentiality.

(2) The development of direct connections referred to in paragraph 1 shall not repeal the obligation for provision of services to other administrations through the ESOD.

(3) The development of the direct connections referred to in paragraph 1 shall be done in compliance with the Ordinance for the internal flow of electronic documents and documents on a paper copy in the administrations, adopted by a Decree of the Council of Ministers of 2008 (State Gazette, Nr. 48 of 2008).

Article 7. (1) The presence of necessary prerequisites for the development of direct connections referred to in Article 6 is attested through certification of the task for development of direct connection under the procedure of Article 102, (1), p.2.

(2) The use of an already developed direct connection between the information systems of two administrative bodies by a third one shall be considered as an independent development of a direct connection, and for its development the rules referred to in paragraph 1 shall be complied with.

Section II
Interoperability requirements in respect of the data

Article 8. (1) The presentation of figures, letters, punctuation marks and other symbols in the information systems of the administrative bodies must be done through the standards entered in the section "Data integration" of the Register of the standards.

(2) The presentation of illustrations, photos and multimedia must be done through the standards entered in the section "Consumers interfaces" of the Register of the standards.

(3) For compressing of the transmitted data when an electronic administrative service is provided the following methods corresponding to the standards entered into the Register of the standards must be used:

1. for text files – methods of compression without loss;

2. for illustrations, photos, multimedia, etc. - methods for compression with a loss can also be used.

Article 9. In their activity the administrations shall use only unified descriptions of data, registered in the respective sections of the Register of the registers and the data according to Article 8 of the Ordinance on the internal flow of electronic documents and documents on a paper copy in the administrations.

Article 10. In cases of presence only of a non-unified description of data, the respective administration shall create unified description of these data and shall start to use them after registration in the Register of the registers and the data referred to in Article 3, paragraph 2 of the Ordinance on the internal flow of electronic documents and documents on a paper copy in the administrations.

Article 11. The control for the use of unified descriptions of data by the administrations shall be performed during the inspection of their internal rules developed in accordance with the Ordinance on the internal flow of electronic documents and documents on a paper copy in the administrations.

Article 12. The Minister of State Administration and Administrative Reform shall coordinate the projects of legal acts regarding the observance of the requirement for the use only of unified descriptions of data entered into the Register of the registers after the opinion of the Council for entries.

Article 13. (1) Formalized descriptions of data can be entered into the Register of the information objects only in cases when they are entered into the Register of the registers and the data is entered as unified data.

(2) The formalized descriptions referred to in paragraph 1 must have the same composition as the relevant descriptions of the data registered in the Register of the registers and the data.

(3) The creation of formalized descriptions shall be done in accordance with criteria and rules for their application for entries approved by the Minister of State Administration and Administrative Reform referred to in Article 32 of the Ordinance for the Registers of the information objects and the Register of the electronic services adopted by Decree Nr. 98 of the Council of Ministers of 2008 (State Gazette, Nr. 48 of 2008).

(4) The control for compliance with the requirements referred to in paragraph 1 – 3

shall be performed by the Minister of State Administration and Administrative Reform through the Council for entries.

Section III
Interoperability requirements in respect of the electronic documents

Article 14. (1) The formalized electronic documents exchanged between the administrations and issued by them towards other persons and organizations must have data organization corresponding to the information objects entered into the Register.

(2) The electronic documents referred to in paragraph 2 must contain valid data in accordance with the requirements entered in the Register for the information objects.

Section IV
Interoperability requirements in respect of visualization and/or editing applications of electronic documents

Article 15. (1) The visualization applications of electronic documents entered into the Register of the information objects and the editing applications of electronic documents entered into the Register of the electronic services must satisfy the requirements of this section.

(2) The applications referred to in paragraph 1 must be certified for conformity with the interoperability requirements and information security.

Article 16. (1) The applications for which a certification procedure has been successfully finalized shall be entered in the list of the certified information systems.

(2) If, applications certified as under paragraph 1 are also entered into the Register of information objects, they shall be provided for use free of charge through the provision of access for the loading of an installation set from the list of the certified information systems.

(3) The Chairman of SAITC shall ensure the conformity between the application subject to installation with the publicly accessible installation package and the certified application.

Article 17. The applications that ensure only visualization of electronic documents must visualize their content, while:

1. the content of all data shall be visualized according to the instructions entered during their registration in the Register of the information objects;

2. the name with which the data have been entered into the Register of the information objects shall be visualized for all data;

3. access to the text of data definition with which they have been entered into the Register of the information objects through a suitable interface shall be provided for all data;

4. indication for the name of an error in accordance with their registration into the Register of the information objects if the verification for their validity is unsuccessful shall be made for all data;

5. access shall be provided to the text of its definition with which it has been entered into the Register of the information objects through a suitable interface for every error found.

Article 18. The applications ensuring editing of electronic documents besides the

functions for visualization of content of an electronic document under Article 17 must contain also functions for:

1. recording and reading of file content of an electronic document in and out of the file system environment, being directly under the control of the consumer of the editing application, including when situated on a portable physical carrier;

2. introduction, correction and deletion of value for all data in an electronic document.

Article 19. (1) The applications must ensure an opportunity for establishing inconformities in the content of a visualized or edited document with its registration into the Register of the information objects.

(2) The applications must give signals for the established inconformities through visualization of the respective error in accordance with the registration of the document into the Register of the information objects.

(3) The applications must permit the errors referred to in paragraph 2 to be taken into the content of a document of the type "Registered errors in a content of a document" generated by the application.

(4) The document referred to in paragraph 3 shall be declared for entry into the Register of the information objects by the Chairman of SAITC.

Section V
Interoperability in respect of information systems

Article 20. (1) The administrative information systems referred to in Article 4 and the subsequent of the Ordinance on the internal flow of electronic documents and documents on a paper copy in the administrations must correspond to the requirements of this section.

(2) The rules of this section refer also to the specialized information systems ensuring fully or partially the functions of an administrative information system as far as they create electronic documents regulated in the Ordinance on the internal flow of electronic documents and documents on a paper copy in the administrations.

Article 21. (1) In case of automatic creation of electronic documents by an information system, verification for the implementation of the requirements referred to in Article 14 shall be performed during the creation.

(2) In case of unsuccessful verification referred to in Article 1 the creation is terminated and this shall be communicated to the employee performing functions for processing in a non-automated regime or controlling the automatic execution of a stage of a service or procedure, whereat the creation of the document is being done.

(3) The verification referred to in Article 1 shall be performed by a certified application for verification for interoperability of electronic documents integrated into the information system.

(4) The availability of the application referred to in paragraph 3 is an obligatory prerequisite for certification of an information system.

Article 22. (1) The information systems must ensure portability of all data contained in them in cases of unforeseen circumstances while allowing for the transfer of the data from them into the content of an electronic document of the type "Data for transfer between information systems" and their introduction into another information system.

(2) The data subject to transfer under paragraph 1 shall be identified as composition and content in the Ordinance on the internal flow of electronic documents and documents on a paper copy in the administrations.

(3) The Chairman of SAITC shall apply for entry of a document of the type referred to in paragraph 1 in the Register of the information objects.

Article 23. The information systems must visualize the data they keep, while:

1. the content of the data shall be visualized according to the instructions entered during their registration in the Register of the information objects;

2. for the relevant data the name with which they are entered in the Register of the information objects shall be visualized;

3. access for the relevant data shall be provided through a suitable interface to the text of their definition with which they have been entered into the Register of the information objects.

Chapter Three

INFORMATION SECURITY

Section I
Policy for information security

Article 24. All information systems of the administrative bodies must correspond to the requirements and the policy for network and information security in view of their protection against illegal or occasional access, use, communication to third persons, change or destruction, as far as such events or actions can disturb the accessibility, authenticity, integrity and confidentiality of the stored or the transferred data, as well as of the provided electronic services related to these networks and systems.

Article 25. (1) In order to achieve network and information security the Heads of the administrations shall implement their own policy consistent with the specifics of the administrative processes in the given administration by undertaking respective administrative and technological measures.

(2) The policies of the individual administrative bodies and the measures undertaken must correspond to the general principles referred to in Annex 1.

Section II
Organization of the network and information security

Article 26. (1) The Heads of the administrations shall be directly responsible for the network and information security in the administrations.

(2) The Heads of the administrations shall develop and approve internal rules for the network and information security of their information systems and for the types of information exchange between them.

(3) The internal rules referred to in paragraph 2 shall be developed on the model of

“Systems for management of the information security” regulated with the requirements of the international standards ISO 27001:2005 and in compliance with the requirements of the Ordinance.

(4) The Heads of the administrations shall issue orders for allocation of the responsibilities of their employees to guarantee the network and information security of the used information systems.

Article 27. (1) The Heads of the administrations shall provide for certification of the internal rules as “Information security management system” in the meaning of ISO 27001:2005 by an organization authorized for the purpose.

(2) The Heads of the administrations shall organize complex verifications for assessment of the degree of the achieved network and information security in the information systems used by them in compliance with clause 7 of ISO 27001:2005.

(3) The results of the certification referred to in paragraph 1 and of the verification referred to in paragraph 2 shall be presented immediately to the Chairman of SAITC as well for the purposes of the current control in compliance with Article 60 of the Law on E-Governance.

(4) The provision of the information referred to in Article 3 shall be realized as an internal electronic administrative service which shall be developed and entered into the Register of the electronic services by the Chairman of SAITC.

Article 28. (1) Every Head of an administration shall designate an employee or an administrative unit responsible for the network and the information security.

(2) The employee or the unit referred to in paragraph 1 shall be directly subordinated to the Head of the administration.

(3) The functions of the employee or of the unit for information security are described in Annex 2.

(4) Where administration under an administrative body has territorial structures and allocated information systems, every territorial unit shall have an employee responsible for the information security.

Article 29. The Heads of the administrations shall ensure the required infrastructure in order to guarantee the information security of the information systems used by them in accordance with the internal rules referred to in Article 26, paragraph 2.

Article 30. (1) A Council for network and information security of the information systems of the administrative bodies shall be established under the Chairman of SAITC as a standing consultation body for coordination of the activity for obtaining network and information security of the used information systems.

(2) The Council for network and information security of the information systems of the administrative bodies shall function on the basis of Rules of Procedure approved by the Chairman of SAITC.

(3) Periodically, but not less than once a year, the Council for network and information security of the information systems of the administrative bodies shall prepare a report for the state of the information security.

Article 31. (1) The Heads of the administrations are obliged to include in the internal rules referred to in Article 26, paragraph 2 and approved by them a section providing for risk assessment and management for network and information security

(2) The recommendable actions for risk assessment and management should correspond to p. 4.2.1 of ISO 27001:2005 and to Annex 3.

(3) The potential risk factors for the network and the information security formulated and classified in the international standard ISO/IEC TR 13335:2000 are pointed out in Annex 4.

Section III
Access management and protection against illegal access

Article 32. (1) The internal rules for network and information security shall regulate the access to the information resources.

(2) The control on exercising a regulated access shall be executed under the rules and procedures pointed out in Annex 5.

Article 33. (1) The Heads of the administrations shall take measures to prevent illegal access of third parties to their information systems resources.

(2) The risk for illegal access referred to in paragraph 1 shall be analyzed in the annual reports of the Council for network and information security.

(3) In cases of an inadmissible level of the risk registered in accordance with paragraph 2, the administrative body shall plan and shall perform the necessary actions for its reduction.

Article 34. The Heads of the administrations shall determine in the internal rules referred to in Article 26, paragraph 2 approved by them the level of protection against illegal access to every information asset in accordance with the following classification:

1. level "0" or "D" – level of free access;
2. level "1" or "C" – level of random access management;
3. level "2" or "B" – level of forced access management;
4. level "3" or "A" – level of checked security.

Article 35. The Heads of the administrations shall be obliged to undertake the necessary actions for establishment and keeping of inventory lists of the available information assets according to Annex 6.

Section IV
Management of the exploitation processes

Article 36. (1) A National centre for action in case of incidents in respect of the information security shall be established under the Chairman of SAITC as an administrative unit in the specialized administration.

(2) The establishment of a National centre for action in case of incidents in respect of the information security shall be done in compliance with the methodological instructions (WP2006/5.1(CERT-D1/D2) of the European Network and Information Security Agency (ENISA).

Article 37. The Heads of the administrations shall ensure the security measures in the management of the exploitation processes in the information systems pointed out in Annex 7, including the security of the electronic messages in accordance with Annex Nr. 8.

Article 38. (1) The employee or the unit responsible for the information security shall watch for illegally installed software of the work stations or servers and shall undertake

measures for its removal.

(2) The Heads of the administrations shall ensure the necessary technical and organizational means for performing the control referred to in paragraph 1 including in cases of territorial remoteness.

Article 39. (1) The storage and the access to data in the information systems shall be realized through systems for management of data bases.

(2) The systems for management of data bases must be certified in compliance with the international standard ISO/IEC 15408:2005, defining the so called "Common Criteria for Information Technology Security Evaluation (CC)", or its national applications such as "IT-Grundschutz Methodology" of BSI (Germany), or with the American federal profile "US Government Protection Profile for Database Management System in Basic Robustness Environments".

(3) In cases of provision of multiconsumer access to the content of electronic documents the information systems have to ensure the functions for locking and unlocking of documents for ensuring joint work with documents.

(4) The minimum level of protection of the access to the resources of the information systems in the administration should be "1" or "C".

Section V
Protection against unwanted software

Article 40. The protection against unwanted software in the information systems of the administration shall be organized by the employees or the units responsible for the network and information security in the respective administration.

Article 41. The measures for protection against unwanted software are pointed out in Annex 9.

Article 42. The National centre for action in case of incidents in respect of the information security shall keep updated information for all attempts for penetration of unwanted software in the information systems of the administrative bodies as well as for the actions undertaken for protection against them.

Section VI
Monitoring

Article 43. (1) The Heads of the administrations shall organize monitoring of the events and the incidents that have occurred in the information systems used by them by creating instructions for its execution in the internal rules approved by them.

(2) The monitoring referred to in paragraph 1 shall be regulated in the internal rules for the network and information security in compliance with p. 4.2.3 of ISO 27001:2005 and Annex 10.

Article 44. The annual reports for the state of the information security of the information systems of the administrations to be adopted by the Council for network and information security of the information systems of the administrative bodies shall include as

obligatory information for the monitoring of the events and incidents and for its effectiveness.

Section VII
Physical security and environmental protection

Article 45. (1) The Heads of the administrations shall ensure measures for the physical protection of their information systems.

(2) The protection regime shall be regulated by the internal rules for the network and information security in compliance with Annex 11.

Article 46. (1) The Heads of the administrations shall undertake preventive actions for the protection of the information systems against natural calamities.

(2) The Heads of the administrations shall insure the risk from damages from natural calamities of the information system in the framework of the obligatory annual insurances.

Article 47. The Heads of the administrations shall provide conditions whereat the unauthorized persons cannot obtain physical access to the work stations and the servers used by the administration.

Section VIII
Management of incidents related to the information security

Article 48. The Heads of the administrations shall approve an action plan in cases of incidents related to the network and information security of the information systems used by them in order to ensure continuity of the activity of the respective administration. The plan has to correspond to the requirements of Annex 12.

Article 49. The employee or the unit responsible for the information security in the respective administration shall be obliged to inform immediately the National centre for action in cases of incidents in respect of the information security for every incident in the information systems of the administration.

Article 50. The Council for network and information security of the information systems of the administrative bodies shall discuss periodically and propose to the Chairman of SAITC for approval recommendable management measures for prevention of incidents in the information security.

Section IX
Security, related to the employees in the administration

Article 51. The Heads of the administrations shall include a section regulating the security measures related to the employees in the administration in the internal rules referred to in Article 26, (2) in compliance with Annex 13.

Article 52. The Heads of the administrations shall determine access profiles of various groups of employees to the resources of the information systems in the respective

administration.

Chapter Four

REGISTER OF THE STANDARDS

Section I
General provisions for the Register of the standards

Article 53. The Register of the standards is a data base managed by an information system containing technical standards and specifications which have to be applied by the administrative bodies for the provision of electronic services as well as for ensuring interoperability and information security.

Article 54. The Register of the standards shall be kept by the Chairman of SAITC through persons authorized by him.

Article 55. (1) Only the circumstances and their elements provided in the Ordinance shall be subject to an entry into the Register of the standards.

(2) The Register shall be updated in compliance with the dynamics of the international standardization processes and the possibilities for their application in the current moment.

(3) The new versions of the standards entered into the Register must not create obstacles for the functioning of the already realized solutions unless the standards used in these solutions could lead to violation of the requirements for information security.

Article 56. The Chairman of SAITC shall establish the organization for:

1. dissemination of knowledge about the application of the standards ensuring interoperability of the information systems and information security;

2. proposals to the Bulgarian Institute for Standardization for adoption of International or European standards as Bulgarian State Standards;

3. proposals to the Bulgarian Institute for Standardization for the drafting of new Bulgarian State Standards.

Section II
Circumstances subject to entry

Article 57. Standards in the meaning of the Ordinance shall be:

1. formal harmonized technical standards in the field of the information technologies, the electronic communications and the information security, approved by the intergovernmental standardization bodies such as ISO, ITU – at international level, or CEN, CENELEC, ETSI – at European level;

2. internationally adopted non-formal and hybrid technical standards and specifications in the field of the information technologies, the communications and the information security – a result of the standardization processes of the sector consortia such as OASIS, IETF, W3Consortium, UN/CEFACT, OMG.

Article 58. The following circumstances shall be subject to entry in the Register of the standards:

1. standard title – the full title of the standards established by the international organization that has drafted the standard and maintaining it shall be entered translated into Bulgarian language and in original in English language;

2. identifier of a standard – a code identifier of the standard established by the international organization that has drafted the standard and is maintaining it shall be entered;

3. clarification for the standard – a brief text clarification for the standard shall be entered;

4. version – the last internationally accepted version of the standard shall be entered;

5. date – the date of the adoption of the last internationally accepted version of the standard shall be entered;

6. organization – the data for the organization that has drafted the standard and is holding it shall be entered;

7. text – text of the standard shall be entered if the standard is published with free access by the organization that has drafted the standard and is maintaining it;

8. URL of a publication – the electronic address (URL) is entered on the Internet site from which access is realized to instructions for supply of the standard if it is not with free access;

9. degree of applicability – a characteristics which can have values: "compulsory", "recommendable", "under control", "white list", "grey list" and "black list" is entered;

10. thematic belonging – a characteristics which can have values: "communication and exchange procedures", "web-services", "data integration", management of the content and definition of meta-data"; "consumer interfaces"; "working stations"; "internal organization of the activity and working processes", "management of the electronic identity" and "information security" shall be entered;

11. scope of applicability – the possibility for application of the whole standard shall be entered or only the respective parts of it shall be enlisted;

12. URL batch – the automatically generated electronic address (URL) of the Internet site from which access is realized to the content of the batch of the standard in the Register shall be entered.

Section III
Keeping the Register

Article 59. (1) The proceedings for entry shall start with an application filed by an administrative body.

(2) The proceedings for entry can start also by the initiative of the Chairman of SAITC upon the proposal of the Council for standards for interoperability and information security according to Article 73.

(3) Persons beyond the ones referred to in paragraphs 1 and 2 can propose to the Chairman of SAITC to start proceedings for entry.

Article 60. The Chairman of SAITC shall provide the following electronic services related to the Register of the standards:

1. entry of a standard;
2. entry of changes of the circumstances for a standard;

3. information for the entries in the Register of the standards for an individual standard or for standards by specified criteria.

Article 61. (1) The Chairman of SAITC shall establish compulsory patterns in electronic form for:

1. application for initial entry for a standard;

2. application for entry of additional circumstances of a standard already entered;

3. application for information about the entries in the Register of the standards.

4. information for the entries in the Register of the standards for an individual standard or for standards by specified criteria.

(2) the patterns referred to in paragraph 1 shall be entered in Section "Documents" of the Register of the information objects and shall be published on the Internet site of the SAITC.

Article 62. (1) The procedure for initial entry of a standard or for changes for the entered circumstances shall include:

1. acceptance of the application for the entry;
2. verification for admissibility and reasoning of the entry;
3. verification whether the standard or the new circumstance has been already entered;
4. making the entry or issuing of a motivated refusal for making the entry;
5. information to the applicant for the refusal for the entry to be made.

(2) The verification referred to in p. 2 and p. 3 shall be made by the Council for the standards for interoperability and information security.

Article 63. (1) The Chairman of SAITC shall make an entry after receiving the opinion of the Council for the standards for interoperability and information security.

(2) Before stating a refusal the Chairman of SAITC shall notify the applicant for the entry to correct the irregularities.

(3) A refusal shall be pronounced in case of failure to correct the irregularities in a time period of 14 days from the notification referred to in paragraph 2.

Article 64. In case of initial entry of a standard, the introduction of the circumstances specified in Article 58 shall be compulsory.

Article 65. (1) In case of initial entry of a standard a batch shall be created for it.

(2) For every created batch a unique register identifier shall be generated consisting of:

1. unique register identifier of the Register of the standards –the unique register identifier created in the Register of the registers and the data during the registration of the Register of the standards in it shall be entered;

2. batch number –the number in turn of the batch in the Register of the standards shall be entered.

(3) For every batch a description shall be kept that shall include:

1. applicant of the entry – data for the administrative body that has applied for the entry shall be entered, and in the cases referred to in Article 59, (3) –SAITC;

2. unique register identifier of the application for entry - unique register identifier of the application with which the entry was applied for shall be entered;

3. time for making the entry – entry shall be made of automatically generated data for the time of the entry made into the Register;

4. employee who has made the entry – data identifying through the information

system supporting the Register the employee who has made the entry shall be automatically entered.

Article 66. To the content of every entered circumstance there shall be kept a description that shall include:

1. number of entry – entry is made of an automatically generated number in turn of the entry by circumstance in the composition of the batch;

2. unique register identifier of circumstance – a unique register identifier of the type of the circumstance/data shall be entered in the section "Types of circumstances" or section "Unified data" of the Register of the registers and the data;

3. content of the circumstance – the data that forms the content of the circumstance subject to entry shall be entered;

4. unique register identifier of an application for entry - the unique register identifier of an application with which the entry has been applied for shall be entered;

5. applicant for the entry – entry shall be made of the name, the unified identifier, e-mail address and the telephone of the administrative body that has applied for the entry, and in the cases referred to in Article 59, (3) – of SAITC.

6. time for making the entry – entry shall be made of automatically generated data for the time of the entry made in the Register;

7. employee who has made the entry –data, identifying the employee who has made the entry through the information system supporting the Register shall be automatically entered.

Article 67. (1) An entry of a change in the circumstances for a standard in the Register shall be made through the entry of a new circumstance.

(2) After the entry referred to in paragraph 1 the actual status of the batch of the standard shall reflect the last entry.

Section IV
Keeping and access to the Register

Article 68. The Register of the standards shall be kept unlimited.

Article 69. The Chairman of SAITC shall keep the Register of the standards in compliance with the requirements of the Ordinance as a system with a class of information security 3 or A.

Article 70. The Register of the standards shall be accessible through the Internet site of SAITC and in another manner depending on the technological readiness of the Agency.

Article 71. The Chairman of SAITC shall provide opportunity for review of the actual status of the batches of the standards towards the moment of the check-up as well as of their state towards a specific date back in time.

Article 72. (1) Anyone can request and can make a check-up for the entries in the Register through the Internet site of SAITC.

(2) Information can be obtained also through the service referred to in Article 60, p. 3.

(3) The checks in the Register shall be free of charge.

Section V
Council for the standards for interoperability and information security

Article 73. A Council for the standards for interoperability and information security shall be established under the Chairman of SAITC.

Article 74. The Council for standards for interoperability and information security shall be an assisting consultation body and shall include experts assigned with an order of the Chairman of SAITS.

Article 75. The Council for standards for interoperability and information security shall take decisions about the admissibility and the grounds for making entries in the Register of the standards.

Article. 76. (1) The Council for standards for interoperability and information security can hold meetings if more than the half of its members are present.

(2) The decisions of the Council shall be taken by simple majority.

(3) The rules for the functioning of the Council shall be approved by the Chairman of SAITS.

Article 77. The Chairman of SAITC shall approve methodises for assessment and preparation of standards to be entered by the Council for standards for interoperability and information security in compliance with the document "Common assessment method for standards and specifications" (CAMSS), developed within the framework of IDABC Programme of the European Commission.

Chapter Five

ACCREDITATION OF REVIEWERS

Section I
General provisions

Article 78. The conformity of the information systems implemented by the administrations with the requirements for interoperability and information security shall be certified by persons who are accredited by the Chairman of SAITS.

Article 79. The accreditation shall be done while observing the principles of rule of law, independence, impartiality, publicity and equality.

Article 80. The persons accredited along the procedure of the Ordinance shall be enlisted in a public list of the accredited persons kept by the Chairman of SAITS.

Article 81. (1) For the accreditation the applicants shall pay a state fee fixed with a tariff referred to in Article 57, (3) of the Law on E-Governance.

(2) In cases of accreditation of a state or municipal administration state fee shall not be payable by it.

Article 82. The Chairman of SAITC shall empower officials to perform the activity for accreditation of the persons who are certifying information systems.

Article 83. (1) The relations between the accredited person and the interested person who has filed a request for certification shall be arranged with a contract.

(2) The accredited person shall receive remuneration for the assessment made.

Section II
Accreditation procedure for accreditation of the persons certifying information systems

Article 84. (1) The persons who wish to perform certification of information systems for conformity with the interoperability requirements and information security shall submit an application to the Chairman of SAITC using a pattern of application form approved by him.

(2) The application shall contain:

1. unique identifier, the name, respectively the applicant's designation;

2. unique identifier, name, telephone and e-mail address of the representing persons.

(3) The application shall have the following enclosures.

1. a list of the technical means possessed by the applicant required for performing the respective activity including description of the technical means by type and factory number as well as a copy of the technical passports;

2. a list of the personnel of the accredited person performing the activities for certification containing names, unique identifier, education, specialty and occupied position, as well as documents certifying for the education and the qualification;

3. a copy of a contract for insurance for the damages that can occur as a result of the non-performance of his/her obligations with an amount of the insurance coverage no less than 100 000 BGN;

4. the applied procedures for certification of information systems;

5. a declaration for lack of circumstances referred to in paragraph 4, p. 1, 2 and 4.

(4) The candidates must satisfy the following conditions:

1. they should not be declared insolvent and there should be no open insolvency proceedings;

2. they should not be in liquidation;

3. they should not have public financial liabilities to the State established with an act of a competent body that has entered into force;

4. the sole traders, respectively the members of the management bodies of the legal entities should not be deprived of the right to exercise trading activity;

5. the accreditation for the performance of the same activity of the applicant should not have been withdrawn.

(5) For verification of the circumstances referred to in paragraph 4 the Chairman of SAITC shall collect information from the initial administrators of the respective data, when this is possible.

(6) The pattern of the application form shall be published on the Internet site of SAITC.

Article 85. (1) The Chairman of SAITC shall issue or shall refuse to provide accreditation in a 14-day time period from the date of submitting the application and the enclosed documents.

(2) The Chairman of SAITC shall refuse to provide accreditation in cases where from the presented documents and the verifications made it is found that the applicant:

1. does not have at his disposal the necessary technical means for performing the activity applied for;

2. does not have at his disposal qualified personnel for performing the activity applied for;

3. has not made the required insurance;

4. does not satisfy the requirements referred to in Article 84, (4).

(3) Before stating a refusal, the Chairman of SAITC shall indicate to the applicant for the entry to correct the irregularities.

(4) A refusal shall be announced if in a time period of 14 days after the notification referred to in paragraph 2 the irregularities are not corrected.

(5) A refusal to provide accreditation shall be appealed according to the procedure under the Administrative Procedure Code.

Article 86. The period of validity of the accreditation shall be 3 years.

Article 87. The accredited persons shall be obliged to notify the Chairman of SAITC about every change in the circumstances contained in the application for accreditation and in the documents enclosed to it, in a 7-day time period from the occurrence of the change.

Article 88. (1) The reaccreditation shall be subsequent confirmation of the competence of the accredited person for the same activity.

(2) The reaccreditation shall be made using the procedure for the initial accreditation.

(3) The application for reaccreditation should be submitted in a time period of up to one month before expiry of the term of validity of the accreditation.

(4) The Chairman of SAITC shall make the reaccreditation in the term referred to in paragraph 3.

(5) During the reaccreditation any change in the circumstances referred to in Article 137 shall be entered.

Section III
Control

Article 89. (1) The activity of the accredited persons shall be subject to control during the period of validity of the accreditation.

(2) The control shall include actions performed by the Chairman of SAITC aimed to

ensure constant conformity of the accredited persons with the requirements of the Ordinance and preserving the trust in quality of the services offered by the accredited persons.

(3) The control shall be performed every year for the term of validity of the accreditation.

Article 90. (1) The Chairman of SAITC shall perform the following verifications:

1. periodical verifications that are performed on the basis of programmes approved by him;

2. verification upon a signal for violations on the part of the accredited persons and published or announced critical materials in the media.

(2) The control shall be performed using a questionnaire-declaration which is made available to the accredited person for filling it.

(3) If necessary the Chairman of SAITC can request for additional information to be presented.

(4) The accredited person shall be obliged to return the filled questionnaire-declaration or to present information in a 14-day term from the date of receipt.

Article 91. In case of found substantial or systematic failure to satisfy the requirements of the Law on E-Governance and the Ordinance on the part of the accredited persons, the Chairman of SAITC can withdraw the accreditation.

Article 92. A file shall be kept for every accredited person in whom the information and the documents provided by the accredited persons shall be kept.

Section IV
Suspension and withdrawal of an accreditation

Article 93. Suspension of the accreditation for a time period of 6 months shall be done on the basis of an application when the accredited person temporarily is not in a position to perform the activities for which he/she has been accredited.

Article 94. (1) The accreditation shall be renewed on the basis of an application of the accredited person and a declaration for lack of change in the circumstances referred to in Article 84, (4).

(2) The application for renewal should be submitted in one-month time period before the expiry of the term referred to in Article 93.

Article 95. In case of suspension of the accreditation and in case of its renewal these circumstances shall be marked in the Public register of the accredited persons.

Article 96. The accreditation shall be withdrawn when the accredited person:

1. is in a permanent incapacity to perform the activities he/she has been accredited for;

2. when the person does not satisfy or ceases to satisfy any of the requirements for granting accreditation;

3. in case of substantial or systematic violation of the provisions of the Ordinance and other acts regulating the activity for which accreditation has been granted;

4. in case of failure to observe in due term the obligation for notification referred to in Chapter six, section IX of the Ordinance;

5. when in the term referred to in Article 94, (2) no actions have been undertaken for the renewal of the accreditation after it has been suspended.

Article 97. (1) In case of withdrawal of the accreditation the date of the withdrawal shall be officially marked in the content of the circumstance "term of validity of the accreditation" and the grounds for the withdrawal.

(2) The suspension of the accreditation can be entered upon the written application of the accredited person while marking the date of applying for the suspension for the circumstance in the content of "Term of validity of the accreditation".

Chapter Six

INTEROPERABILITY AND INFORMATION SECURITY CERTIFICATION METHODICS FOR CERTIFICATION

Section I
General provisions

Article 98. The administrations shall be obliged to use only information systems and programme applications which are certified for conformity with the interoperability and information security requirements established by the Law on E-Governance and the implementing regulations.

Article 99. No certification shall be made using the procedure of the Ordinance for:

1. information systems intended for processing and storage of classified information;

2. information systems with special purpose (national security, defence, etc.);

Article 100. The certification shall be made while observing the principles of lawfulness, independence, impartiality, publicity and equality.

Article 101. The information systems and the programme applications certified using the procedure of the Ordinance shall be entered into a public list of the certified information systems kept by the Chairman of SAITS.

Section II
Objects of interoperability and information security certification

Article 102. (1) Subject to certification for conformity with the interoperability and information security requirements shall be specifications for:

1. development or acquisition of an administrative information system;

2. building of direct connectivity between the information systems in accordance with Article 7;

3. development or acquisition of specialized information systems referred to in Article 20, (2).

(2) The certification referred to in paragraph 1 shall be made upon the request of an interested administrative body.

Article 103. (1) Subject to certification for conformity with the interoperability and information security requirements for shall be an information system which:

1. has a functionality according to the requirements of Article 20;

2. is a new version of an information system which has been already certified in accordance with p. 1;

(2) The certification referred to in paragraph 1 shall be made upon the request of an interested person who is supplying or developing the information system.

Article 104. (1) Subject to certification for conformity with the requirements for interoperability and information security shall be programme applications that:

1. perform functions for visualization and/or editing of electronic documents in accordance with Article 15;

2. in the composition of other applications or systems they perform functions for the verification of electronic documents for conformity with their registration in the Register of the information objects.

(2) The certification referred to in paragraph 1 shall be made upon a request of an interested person supplying or developing the programme application.

Article 105. The certification does not include verifications for the presence of copy rights, related or other rights of intellectual or industrial property on the verified information systems and programme applications.

Section III
Certification of specifications for interoperability and information security

Article 106. (1) The specification for the development of information systems should contain explicit and clear indication whether it falls into the scope of Article 20.

(2) In cases of lack of indication referred to in paragraph 1 or in cases of lack of conformity between the indication and the requirements for the information system the accredited person shall refuse the certification.

Article 107. The certified specifications shall be entered into the list of the certified information systems.

Section IV
Compiling of documents containing test data for performing procedures for certification for interoperability

Article 108. (1) For every type of electronic document registered in the Register of the information objects the interested person shall present a set of documents of the same type containing test data for performing tests for conformity with the registration in the Register of

the information objects.

(2) In the set of documents referred to in paragraph 1 only one document should not contain deviations from the registration of the respective type of document.

(3) The tests shall be created in a way that permits the wrong values specified in them and the irregularities in the organization of the data to present all possible deviations from the registration of the respective type of document in the Register of the information objects.

(4) For every document containing the test data referred to in paragraph 1 the interested person shall present a document of the type "Registered errors in a content of a document" which contains a description of the errors in the test document in accordance with the nomenclature of the errors for the information objects contained in the documents that has been entered into the Register of the information objects.

(5) The responsibility for the completeness of the set of documents containing test data referred to in paragraph 1 shall be of the accredited person performing the certification.

Article 109. (1) In line with the notification for the certification made, the accredited person shall send to the Chairman of SAITC the full set of documents referred to in Article 108, (1) and (4).

(2) The Chairman of SAITC shall enter the set of documents referred to in paragraph 1 in the list of the certified information systems.

(3) The verifications in respect of a document registered in the Register of the information objects for which there are entered sets of documents referred to in Article 108, (1) and (4) shall be made using these sets.

Article 110. (1) For every document registered in the Register of the information objects there shall be a list of the data contained in the document.

(2) The list referred to in paragraph 1 for the tested document shall be prepared as a check-up referred to in Article 15, p. 7 of the Ordinance for the Registers of the information objects and of the electronic services.

Article 111. (1) Changes in the entered sets of documents referred to in Article 108, (1) and (4) shall be made upon notification from an accredited person in cases of:

1. found errors in the documents with the tests;
2. found functional incompleteness in the tests in a set of documents.

(2) The changes referred to in paragraph 1 shall be made by the Chairman of SAITS.

Section V
Certification for interoperability and information security of applications for visualization or editing of electronic documents

Article 112. (1) The interested person can request from an accredited person certification for interoperability and information security of an application for visualization or editing of electronic documents.

(2) The interested person shall present to the accredited person an installation package of the application together with a detailed guide for installation and use.

Article 113. The accredited person shall make the following verifications for establishing the technical functionality of the application for:

1. reading and visualization of a content of an electronic document from file recorded in the information system being under control of the consumer or recorded on an external carrier;

2. compiling of an electronic document of the type "Registered errors in content of a document" containing the results from verification of the stored electronic document for conformity with its registration in the Register of the information objects;

3. availability of functionality for true and correct visualization of all errors – a result from tests with the set of documents containing test data referred to in Article 108, (1) in performing the verification referred to in p. 2;

4. availability of functionality for true and correct visualization of the messages containing the names and the descriptions of all errors caused during the tests with the set of documents;

5. availability of functionality for true and correct visualization of the content, the name and the description of all data in accordance with the registration of the visualized electronic document in the Register of the information objects.

Article 114. In case of certification for interoperability and information security of an application for editing of electronic documents besides the verifications referred to in Article 113 verifications shall also be made for the establishment of the availability of functionality for:

1. recording of an electronic document as a file in the information system being under control of the consumer including on an external carrier;

2. creation, deletion and correction of all data in accordance with the registration of the electronic document in the Register of the information objects.

Article 115. (1) The results from the verifications performed shall be reflected in a document of the type "Results from tests for interoperability by document".

(2) The accredited person who has made the verification shall sign with electronic signature the document referred to in paragraph 1.

Article 116. The tests for application for visualization or editing which is operating with several documents shall be made for every one of them.

Article 117. (1) In case of successful verifications, the accredited person shall issue to the interested person a certificate for interoperability and information security.

(2) The certificate for interoperability and information security of applications shall contain the following data:

1. data identifying the certified application such as model, version, configuration, etc;

2. data identifying the interested person;

3. data for the accredited person who has issued the certificate;

4. scope of the certification including the types of electronic documents supported by the application;

Article 118. In case of enlarging the scope of the electronic documents which may be visualized or edited with the certified application, verifications for certification shall be made

only for the new documents.

Section VI
Certification of applications for verification of electronic documents for conformity with their registration in the Register of the information objects

Article 119. (1) An interested person can request certification for interoperability and information security of an application for verification of electronic documents for conformity with their registration in the Register of the information objects from an accredited person.

(2) The interested person shall present to the accredited person an installation package of the application along with a detailed manual for installation and use.

Article 120. The accredited person shall make the following verifications in order to establish the technical functionality of the application for:

1. reading the content of an electronic document from a file recorded in the information system being under control of the consumer or recorded on an external carrier;

2. creation of an electronic document of the type "Registered errors in a content of a document" containing the results from the verification of the stored electronic document for conformity with its registration in the Register of the information objects.

Article 121. The rules referred to in Article 114 – 118 respectively shall be applied for the certification of electronic documents for conformity with their registration in the Register of the information objects.

Section VII
Certification for interoperability and information safety of information systems

Article 122. (1) An interested person can request certification for interoperability and information security of information systems from an accredited person.

(2) The interested person shall present to the accredited person an installation package along with a detailed manual for installation and use.

(3) The interested person shall be obliged to specify:

1. the data related to the certification of an application integrated in the information system when making verification for interoperability of electronic documents;

2. the technical requirements regarding the environment in which the information system will be installed and tested.

Article 123. The Chairman of SAITC shall create, maintain and present a special environment-polygon for making verifications for conformity of the information systems with the interoperability and information security.

Article 124. (1) The interested person shall install alone the information system in the environment-polygon referred to in Article 123.

(2) The interested person shall ensure a technical assistant who shall enter the data and shall activate the respective functions in the information system under the guidance of the

accredited person.

Article 125. For every document created by the administrative information system referred to in Annex 1 to the Ordinance for the internal flow of electronic documents and documents on a paper copy in the administrations, verification shall be made for:

1. the possibility for entering of the values of the data in the composition of a verified document in manual or automatic regime;

2. the possibility for generation in manual or automatic regime of a valid document of the verified type containing the data entered as per p. 1.

Article 126. The verifications for the implementation of the requirements referred to in Article 22 shall be made in the following sequence:

1. the electronic documents created during the tests referred to in Article 125 shall be entered into the information systems;

2. a document "Data for transfer between information systems", shall be created

3. the availability in the document referred to in p. 2 of the documents referred to in p. 1 and the data accompanying their entry shall be verified;

4. they shall be entered into the information system according to three values for every type of data supported by it and their availability in the document referred to in p. 2 shall be verified.

Article 127. (1) The set of data for the verification referred to in p. 4 shall cover all data described in the Ordinance for the internal flow of electronic documents and documents on a paper copy in the administrations, which the Chairman of SAITC shall publish on the Internet site of the Agency on a Certification data list maintained by the administrative information systems.

(2) For all data referred to in paragraph 1, verification shall be made for:

1. true and correct visualization of the name of the data;

2. true and correct visualization of the definition of the data.

Article 128. The accredited person shall make the verification for the implementation of the requirements for information security referred to in Article 39.

Section VIII
Changes in an issued certificate

Article 129. The interested person can request a change in an issued certificate for interoperability and information security from the accredited person in case of changes in the circumstances recorded into the certificate.

Article 130. The change of an issued certificate shall be made through the reissue of the certificate provided that the changed circumstances do not concern the requirements for information security and interoperability.

Section IX
Obligation for notification. Collection of information

Article 131. Interested persons who have received certificate for conformity of the information system shall be obliged to notify immediately the accredited person who has

issued the respective certificate for any change in the circumstances about the certified programme application, specification or information system.

Article 132. (1) The accredited persons shall be obliged to keep all documents and protocols from the verifications made for a time period of 10 years.

(2) The accredited persons shall present the documents referred to in paragraph 1 to the Chairman of SAITC when making verifications.

Article 133. (1) The accredited persons shall inform the Chairman of SAITC for every issued certificate immediately after its issue for its entry into the list of the certified information systems.

(2) The Chairman of SAITC shall enter the certificate in the List of the certified information systems in a time period of 3 days from the date of receipt of the notification referred to in paragraph 1, after verification whether the certificate contains all required requisites.

Chapter Seven

LIST OF THE ACCREDITED PERSONS AND LIST OF THE CERTIFIED SYSTEMS AND PRODUCTS

Article 134. (1) In the lists of the accredited persons and of the certified systems and products, circumstances about the persons accredited for certification of information systems, respectively about the certified information systems and products shall be entered.

(2) The lists referred to in paragraph 1 shall be kept by the Chairman of SAITC by persons authorized by him.

Article 135. (1) The lists are data bases managed by an information system containing the descriptions of the composition and the organization of the data referred to in Article 134, paragraph 1.

(2) History of the entries shall be kept in the lists.

Article 136. The list of the persons accredited for the certification of information systems shall consist of one section – "Accredited persons" in which the circumstances about these persons shall be entered.

Article 137. The following circumstances shall be entered into the list of the persons accredited for certification of the information systems:

1. unique identifier, name, respectively designation, of the applicant;
2. unique identifier, name, telephone and address of the e-mail of the representing persons;
3. term of validity of the accreditation;
4. date of initial accreditation;
5. grounds for suspension or withdrawal of the accreditation.

Article 138. (1) The following types of objects shall be entered into the list of the certified information systems:

1. objects of the type "certified system";
2. objects of the type "certified application";
3. objects of the type "certified specification";

4. objects of the type “test set of documents”.

(2) The list referred to in paragraph 1 shall consist of the following sections, divided into types of objects in which the circumstances of these objects are entered:

1. section “Certified systems”;
2. section “Certified applications”;
3. section “Certified specifications”;
4. section “Test sets of documents”.

Article 139. The following circumstances for objects of the type “certified systems” shall be entered into the section “Certified systems” from the list of the certified systems:

1. data identifying the certified system such as model, version, configuration, etc;
2. data identifying the interested person;
3. data for the accredited person who has made the certification;
4. scope of certification including the types of electronic documents which are maintained by the system;
5. number and date of the issued certificate.

Article 140. The following circumstances for objects of the type “certified application” shall be entered into the section “Certified applications” from the list of the certified systems:

1. data identifying the certified application such as model, version, configuration, etc;
2. type of certified application - application for visualization and/or editing or application for verification of electronic documents for conformity with their registration;
3. data identifying the interested person;
4. data for the accredited person who has made the certification;
5. scope of certification including the types of electronic documents maintained by the application;
6. number and date of the issued certificate;
7. hyperconnection for access to the installation package of the application when the certified application has been entered as circumstance in the Register of the information objects or in the Register of the electronic services.

Article 141. The following circumstances for objects of the type “certified specification” shall be entered into the section “Certified specifications” from the list of the certified systems:

1. data identifying the certified specification;
2. data identifying the interested person;
3. data for the accredited person who has made the certification;
4. number and date of the issued certificate.

Article 142. The following circumstances for objects of the type “test set of documents” shall be entered into the section “Test sets of documents” from the list of the certified systems:

1. type of the documents in the test set;
2. list with test documents, their content and their corresponding documents “registered errors in a content of a document”;
3. data for the accredited person who has sent the set to be entered.

Article 143. (1) The Chairman of SAITC shall provide the following electronic services related to the lists of the accredited persons and of the certified systems and products:

1. recording of changes in the circumstances for the accredited person;

2. recording of the suspension of the accreditation;

3. information for the entries in the list of the accredited persons;

4. recording of the certified specification, system or product;

5. recording of changes in the circumstances for a certified specification, system or product;

6. information for the entries in the list of the certified systems or products.

(2) The initial entry of the accredited person shall be made officially by the Chairman of SAITC in the process of the accreditation.

Article 144. The Chairman of SAITC shall approve compulsory samples in electronic form for the applications referred to in Article 143 for delivery of services.

(2) The samples referred to in paragraph 1 shall be entered into the section "Documents" from the Register of the information objects and shall be published on the Internet site of the SAITC.

Article 145. (1) The procedure for entry of accredited persons shall include:

1. receipt of the application for entry;
2. verification for admissibility and availability of grounds for the entry;
3. check-up whether the circumstance have been already entered;
4. realization of the entry.

(2) In case of inconformities the Chairman of SAITC shall give instructions for their correction.

Article 146. (1) The procedure for initial entry of certified specifications, systems and products or of changes of the entered circumstances shall include:

1. receipt of the application for entry;

2. verification for admissibility and availability of grounds for the entry;

3. check-up whether the object or the new circumstance has been already entered;

4. realization of the entry or issuing of motivated refusal for entry;

5. notification of the applicant for the announced refusal.

(2) Before stating a refusal, the Chairman of SAITC shall instruct the applicant of the entry to correct the irregularities.

(3) A refusal shall be stated if in a time period of 14 days from the notification referred to in paragraph 2 the irregularities are not corrected.

Article 147. The entry in the lists shall be made through introduction of data for the entered circumstances in the data base of the lists.

Article 148. (1) A batch shall be created in case of initial entry for every object.

(2) For every created batch a unique register identifier shall be generated and it shall consist of:

1. unique register identifier of a section of the lists – entry is made of the unique register identifier created in the Register of the registers and the data during the registration of the lists of the certified systems and the list of the persons accredited for certification of the information systems in it;

2. batch number – the number in turn of the batch shall be entered.

(3) A description shall be kept for every batch containing:

1. time of entry – entry is made of automatically generated data for the time of entry into the list;

2. employee who has made the entry – data shall be automatically entered identifying the employee who has made the entry in the respective list through the information system supporting the lists.

Article 149. To the content of every entered circumstance a description shall be kept which shall include:

1. number of entry – entry shall be made of automatically generated number in turn of entry of a circumstance in the composition of the batch;

2. unique register identifier of a circumstance – entry shall be made of a unique register identifier of the type of the circumstance/the data in the section "Types of circumstances" or section "Unified data" from the Register of the registers and the data;

3. content of the circumstance –the data forming the content of the circumstance subject to entry shall be entered;

4. time of entry - automatically generated data for the time of entry into the list shall be entered;

5. unique register identifier of an application for entry –the unique register identifier of an application with which the entry has been applied for shall be entered;

6. applicant of the entry –the name, BULSTAT code, e-mail address and telephone of the headquarters of the administrative body that has applied for the entry shall be entered;

7. employee who has made the entry - data shall be automatically entered to identify the employee who has made the entry through the information system supporting the lists.

Article 150. (1) A change in the circumstances shall be made through entry of the new circumstance.

(2) After the entry referred to in paragraph 1 the current condition of the batch of the respective object shall reflect the last entry.

Article 151. The lists of the persons accredited for certification of information systems and of certified systems shall be kept termless.

Article 152. The Chairman of SAITC shall keep the lists in compliance with the requirements of the Ordinance as a system with a class of information security 3 or A.

Article 153. The lists of the persons accredited for certification of the information systems and of certified systems shall be accessible through the Internet site of the SAITC and in another way depending on the technological readiness of the Agency.

Article 154. The Chairman of SAITC shall ensure possibility for review of the current condition of the files of the lists towards the moment of the review as well as of their condition towards a specified date back in time.

Article 155. (1) Anyone can request and can make a check for the entries in the lists through the Internet site of SAITC.

(2) Checks can also be made through a formalized application.

(3) The checks in the lists shall be free of charge.

Supplementary provisions

§ 1. In the meaning of the Ordinance:

1. "Administrative information system" shall be an information system in the meaning of Article 4 and the next articles from the Ordinance for the internal flow of electronic documents and documents on a paper copy in the administrations.

2. "Electronic services" shall be the general term for electronic administrative services and internal electronic administrative services.

3. "Network and information security" shall be the capacity of the networks and the information systems to resist to a definite level of impact or to random events which can disturb the accessibility, the integrity and the confidentiality of the stored or the transmitted data and of the services related to these networks and systems.

4. "Information assets" shall be the tangible and intangible assets and information objects related to the information system which have a useful value for a given administration.

5. "Information security incident" shall be a single event or a series of events related to the information security which damage or there is serious probability to damage operations or to endanger the information security.

6. "Unwanted software" shall be a computer programme which is disseminated automatically and against the will or without the knowledge of the persons using the information systems and is being intended for provoking unwanted conditions by the people using the information systems or computer networks or in realization of unwanted results as well as a computer programme which is designed for disturbance of the activity of the information system or computer network or for getting to know, deletion, erasing, change or copying of data without permission when such permission is required.

7. "Policy for information security" shall be a totality of documented decisions made by a Head of an administration directed towards the protection of the information and the resources associated with it.

8. "Web service" shall be an autonomous, completed and realizable functionality of an information system with a unified and automated inlet and outlet that has the following properties:

a) independence from the accompanying applications which create it and from those it is creating;

b) slightly related functionality based on system technical, platform and software independence between the information system of the supplier of the service and of its user;

c) functional and operational specifications for the quality in service delivery such as maximum time for provision of the service, procedures for processing of errors, etc;

d) functionality based on a definite set of internationally accepted standards;

e) easy to be detected and used without peculiar actions on the part of its supplier.

9. "Open network" shall be a network free from limitations for the type of the equipment which can be added, as well as for the ways of communication which do not limit the content, the sites or the platforms.

10. "Profile of access" shall be a description of the information assets of the system which can be used by a group of consumers with analogous rights to access.

§ 2. The levels of protection of the information system from unregulated access regulated in Article 34 of the Ordinance shall be characterized with the following basic measures:

1. Level “0” or “D” shall cover open and commonly accessible information (for example publishing on the Internet sites of the administrations). It shall offer anonymous use of the information and lack of means for confidentiality.

2. Level “1” or “C” shall require:

a) the access to exactly specified objects to be allowed to exactly specified users;

b) the users to be identified before performing any kind of actions controlled by the system for access. For the establishment of the identity, a protection mechanism has to be used of the type identifier/password. There are no requirements for a proof for the identity in case of registration;

c) the identifying information has to be protected against unregulated access;

d) the confidential calculation system, i.e. the functionality of the information system which manages the access to its resources has to maintain an area for its own realization protected against external influences and against attempts for following the process of work;

e) the information system has to possess technical and/or programme means enabling to periodically check the correctness of the components of the confidential calculation system;

f) the protection mechanisms have to have passed a test which shall confirm that an unauthorized user does not have an obvious possibility to obtain access to the confidential calculation system.

3. Level “2” or “B”, in addition to the requirements of the previous level, shall require:

a) as a mechanism for verification of the identity, a certificate for the electronic signature has to be used irrespective whether it has been issued for intradepartmental needs within the framework of an internal infrastructure of the public key or it has been issued by an external supplier of certification services;

b) in issuing the certificate the issuing body shall check the essential data for the personality of the user without his/her personal presence;

c) the confidential calculation system has to ensure realization of forced management of the access to all objects;

d) the confidential calculation system has to ensure mutual isolation of the processes through the separation of their address areas.

4. Level “3” or “A” in addition to the requirements of the previous level, shall require:

a) a certificate for universal electronic signature shall only be used as a mechanism for identification;

b) in issuing the certificate the physical identity of the person has to be guaranteed;

c) the confidential calculation system has to be with checked resistance to attempts for penetration;

d) the communication between the user and the system has to be realized solely through protocol Transport Layer Security (TLS) or Secure Sockets Layer (SSL), and the minimum length of the symmetric key has to be 128 bytes;

e) the confidential calculation system has to have a mechanism for registration of attempts for violation of the security policy.

Transitional and final provisions

§ 3. The Chairman of SAITC shall ensure the initial entry of data in the Register of

standards in a 3 month period from the promulgation of the Ordinance in the State Gazette.

§ 4. (1) In a 12-month period from the entry into force of the Ordinance the Heads of the administrations shall organize the development of internal rules in accordance with Article 26 and shall make their certification as a System for management of the information security in accordance with ISO 27001:2005.

(2) In 24-month period from the entry into force of the Ordinance the Heads of the individual administrations shall organize an audit to be performed by an authorized independent organization for recognition of conformity between the developed intradepartmental rules "Systems for management of the information security" and the international standard ISO 27001:2005.

§ 5. In a 6-month period from the entry into force of the Ordinance the Chairman of SAITC shall approve a Methodics for planned and current control of the interoperability and the network and information security in the information systems of the administrative bodies.

§ 6. In a 12-month period from the entry into force of the Ordinance the Chairman of SAITC shall establish a Council for network and information security of the information systems of the administrative bodies as a consultative body supporting his activity.

§ 7. In a 12-month period from the entry into force of the Ordinance the Chairman of SAITC shall make consultations with representatives of the Association of Bulgarian Insurers about the possibility for provision of an insurance product "Insurance of the risk in relation to the network and the information security".

§ 8. The Chairman of SAITC shall establish a National centre for actions in case of incidents with respect to the information security no later than 6 months from the entry into force of the Ordinance.

§ 9. The Ordinance shall be adopted on the basis of Article 43, (2) of the Law on E-Governance.

§ 10. The Ordinance shall enter into force from the day of its promulgation in the State Gazette except for Article 7 which shall enter into force after the commissioning into exploitation of the Unified environment for exchange of electronic documents (ESOD).

Annex 1 to Article 25, (2)

General strategies for information security

1. The information security policy shall be a set of normative documents, rules and norms for behaviour which determine how the organization is protecting the processing, storage and dissemination of the information.

2. The information security policy of information systems of the administrative bodies has to be in conformity with the series of international standards ISO 270XX, unifying the majority of existing standards for management of the information security – mainly with the standard ISO 27001:2005, providing a model of a system for management of the information security for adequate and proportional control of the security for protection of the information assets and creation of confidence on the part of the interested parties.

3. The decisions about the policies for network and information security have to be developed for provision of several levels of security in respect of:

a) network;

b) system;

c) applications;

d) information.

4. For every of the levels referred to in p. 3 the respective control has to be ensured in order to ensure the security of the general programme application for protection. The practice called "deep defence" shall be applied for ensuring the adequate level of security which shall ensure multi-layer protection for limiting the propagation of any attacks and provision of impossibility for discrediting of the general programme application for protection.

5. The following principles shall be used when formulating the security policy:

a) "Minimum privilege" – concept where the access shall be restricted only to resources required for the performance of the approved functions. A definite user or process has to have only such rights which are necessary for the performance of the specific task.

b) "Deep defence" – concept where the protection of more than one component or mechanism is being entrusted, ensuring the security in such a way that the impossibility for one component or mechanism to restrict the attack shall not lead to discrediting of the general protection.

c) "Plugging point" – concept where persons making interventions are forced to use a narrow channel for access which permits that the actions be monitored and controlled. It is usually applied at the inlet and outlet of the so called "Demilitarized zones" ("DMZ").

d) "Weakest unit" – concept where the units with the weakest resistance to interventions or with presence of possibility for penetration is observed and eliminated.

e) "Position of safe stopping" – concept where the systems have to stop work safely and to prevent the possibility for access to be provided for the persons making interventions to the system in case of unexpected stopping of the work of a system.

f) "Universal participation" – concept where all units of the system observe for the security at the presence of distribution of the functions for what restricts the possibility for the persons making interventions to benefit from the lack of protective activity by a specific unit.

g) "Diversity of the protection" – concept where one does not rely only on one system or application for security irrespective of how reliable or comprehensive are they.

h) "Simplicity" – concept where the maintenance of a simplified general environment is ensured for which protection against intervention is more easily ensured.

i) "Fragmentation" – concept where the possible harmful consequences on one information system are reduced to minimum through the fragmentation of a maximum number of individual units; in this way the possibility is restricted for access to the whole system in case of penetration into an isolated unit.

j) "Protection against internal and external threats" – concept where rules are introduced for the users so that no actions shall be tolerated of the employees which could ensure possibility for interventions; such rules can be rules for management of the content, additional levels for identification, registration for access to critical information assets, etc.

Annex Nr. 2 to Article 28, (3)

Functions of the employee (unit) responsible for information security

1. Manages the activities related to achievement of network and information security of the administration in which he/she is working in compliance with the normative framework and the policies and the objectives for the network and information security of the organization in interaction with the units for information provision and for internal audit.

2. Observes for the application of the standards, the policies and the rules for information security and risk management in the administration.

3. Consults the management team of the administration in relation with the information security.

4. Manages the periodical assessment of the risks for the information security and the observance of the adopted policies and procedures.

5. Prepares periodically (no less than twice a year) reports for the condition of the information security in the administrative unit and shall present them to the Head.

6. Coordinates the training of the managers and the employees in the administrative unit in relation with the information security.

7. Participates in the organization, the training and the analysis of the results from the trainings for actions in cases of incidents.

8. In charge of the protection of the intellectual property and the tangible assets of the administrative units in the field of the information and communication technologies.

9. Participates in the formulation of the policies, the objectives, the procedures and the metrics for assessment of the information security.

10. Keeps relations with other administrations, organizations and experts working in the field of the information security.

11. Investigates and analyzes the incidents in the field of the network and information security in the administrative unit, the reactions in cases of incidents and proposes actions for improvement of the network and information security.

12. Proposes sanctions for the employees of the administration in cases of violation of the rules for security.

13. Develops and proposes for approval by the Head of the respective administration the instructions stemming from the Ordinance as well as all other instructions and procedures.

14. Observes for the implementation of the instructions and procedures related to the information security approved by the Head of the administration.

15. Updates the list of threats and potential risks for the respective administration.

16. Coordinates the assessment of the financial and other losses in case of occurrence of an identified threat.

17. Prepares reports and analysis for incidents that affect the network and the information security and proposes actions for compensating of the consequences and prevention of other similar incidents.

18. Observes for novelties for threats for the security taking into account the available software and hardware in the respective administration and shall organize the due installation of correcting software (patches).

19. In case of occurrence of any incident related to the information security the employee shall document it and shall immediately inform the Head of the respective administration and the National centre for actions in case of incidents in respect to the information security in information systems of the administrative bodies.

20. Develops and proposes innovative solutions and architectures for the improvement of the information security of the respective administration.

21. Observes for the occurrence of viruses and harmful code, spam, attacks and takes adequate measures.

22. Organizes tests for penetration, detects the bottlenecks in the network of the respective administrative unit and proposes measures for the improvement of the network and information security.

Annex 3 to Article 31, (2)

Actions for risk assessment and management

1. All administrative bodies shall be obliged to assess the risks for the security in accordance with the international standard ISO/IEC TR 13335-3:1998 and ISO/IEC TR 13335-4:2000 (in process of revision into ISO/IEC 27005).

2. In the meaning of this Annex the risk for the security shall be a factual status which creates threats for affecting one or several information assets which could lead to their damage or destruction.

3. The risk assessment shall be determined through the calculation of the probability for affecting on the basis of the efficiency of the existing and the planned security measures.

4. The threats for the network and the information security shall be classified using the following criteria:

a) by the elements of the information security (accessibility, completeness, confidentiality) to which they are directed;

b) by the components of the information system (equipment, software, data, supporting infrastructure) to which they are directed;

c) by the way of realization (random/deliberate actions, of natural/technological character, etc.);

d) by the location of the source (inside/outside the information system).

5. The actions for risk management have to cover assessment of its size, development of effective and economic measures for its reduction and assessment whether the resultant risk is in admissible limits. The risk management has to be completed through the successive application of two types of actions repeated in cycles:

a) assessment (reassessment) of the risk;

b) choice of effective and economic means for its neutralization.

6. When identifying the risk one has to undertake one of the following actions:

a) elimination of the risk (for example through elimination of the circumstances provoking it);

b) reduction of the risk (for example through the use of additional protection means);

c) acceptance of the risk and development of an action plan in the conditions of a risk;

d) readdressing of the risk (for example through the signing of the respective insurance).

7. The process of risk management has to include the following stages:

a) choice of objects that can be analyzed and the level of details of the analysis;

b) choice of a methodology for risk assessment;

c) identification of information assets;

d) analysis of the threats and their consequences, detection of the bottlenecks in the protection;

e) risk assessment;

f) selection of protection measures;

g) realization and verification of the chosen measures;

h) assessment of the residual risk.

8. The risk management process has to be a cyclic process. The last stage shall occur to be the start of a new cycle of assessment. The new cycle shall be done:

a) if the residual risk does not satisfy the management team of the administration;

b) after the elapse of a definite period determined in the Internal rules for the network and the information security of the administration.

Annex 4 to Article 31, (3)

Threats against the network and information security formulated in the international standard ISO/IEC TR 13335:2000

The types of threats which can endanger the confidentiality, integrity and accessibility are the following:

1. Eavesdropping expressed in access to official information through catching of electronic messages irrespective of the used technologies.

2. Electromagnetic radiation expressed in actions of a third person aiming to obtain knowledge for exchanged data through an information system.

3. Unwanted code which can lead to loss of confidentiality through the recording and the disclosure of passwords and to disturbance of the integrity in case of intervention by third persons, who have realized unregulated access with the help of such a code. An unwanted code can be used in order to evade verification for authenticity as well as all related protection functions. As a result the code can lead to loss of the accessibility when the data or the files are damaged by the person who has received unregulated access with the help of unwanted code.

4. Masking of the user identity can lead to evasion of the verification for authenticity and all services and related protection functions.

5. A wrong direction or redirection of the messages can lead to loss of confidentiality in case of an unregulated access by third persons. The wrong direction or redirection of the messages can also lead to disturbance of the integrity if the wrongly directed messages are changed and after that directed towards the initial addressee. The wrong direction of the messages leads to loss of the accessibility to those messages.

6. Software errors can endanger the confidentiality if the software is created with control of the access or for encrypting, or if an error in the software ensures possibility for unwanted access in information system.

7. The theft of information assets can lead to disclosure of information which represents official or other secret protected by the law. The theft can endanger the accessibility to the data or the information equipment.

8. Unregulated access to computers, information resources, services and applications can lead to disclosure of confidential data and to disturbance of the integrity of these data if their unregulated change is possible. The unregulated access to computers, data, services and applications can disturb the accessibility to the data if their deletion or erasing is possible.

9. An unregulated access to a carrier of data can endanger the data stored on it.

10. Damage of a carrier of information can disturb the integrity and the accessibility to the data being stored on this carrier.

11. Error in the maintenance. The failure to regularly maintain the information systems or errors made during the maintenance process can lead to disturbance of the accessibility to data.

12. Failures in the electric supply and air-conditioning installations can lead to disturbance of the integrity and the accessibility to data if as a result of the failures information systems or data carriers have been damaged.

13. Technical failures (for example failures of the network) can disturb the integrity and accessibility to information which is stored or disseminated through this network.

14. Errors during the transmission of the information can lead to disturbance of its integrity and accessibility.

15. The use of unregulated programmes and information can disturb the integrity and the accessibility to the data stored and disseminated through the information system in which such event has occurred and the programmes and the information are used in order to change existing programmes and data in a non-permitted way or if they contain an unwanted code.

16. User errors can disturb the integrity and accessibility to data through undeliberate or deliberate action.

17. Lack of conformation can endanger the integrity of the data. The protection measures for prevention of the non-confirmation have to be applied in the cases when it is important to obtain a proof for the fact that a given message has been sent and has been received/or has not been received as well as for the fact that the network has transmitted the message.

18. Interventions against the integrity of the data can lead to their serious damage and to impossibility for their further use.

19. Failures in the communication equipment and services can disturb the accessibility to the data transmitted through these services.

20. External effects from fire, water, chemicals, etc. can lead to disturbance or destruction of the information equipment.

21. The misuse of resources can lead to lack of accessibility to data or services.

22. Natural calamities can lead to the destruction of data and information systems.

23. The overloaded communication traffic can lead to disturbance of the accessibility to exchanged data.

Annex 5 to Article 32, (2)

Means for management of the access of the participants in the electronic exchange

1. The protection of the system resources of information systems of the administrative bodies is a process in which the use of the system resources is regulated in compliance with the policy in the field of the network and information security and is permitted only for authorized persons through the information systems used by them. This includes the prevention of an unregulated access to the resources including the prevention of an access to the resources in an unregulated way.

2. The management of the protection from unregulated access shall be classified in

several stages depending on the assessments of the potential consequences for the administration in case of disturbance of the confidentiality, integrity and/or accessibility as follows:

a) limited, when the organization continues to perform its functions but with reduced efficiency, insignificant damages have been caused to the information assets and the financial losses are insignificant;

b) moderate, when the efficiency of the basic functions of the administration is essentially reduced, significant damages are caused to the information assets and the financial losses are considerable;

c) high, when the loss of confidentiality, integrity and/or accessibility exercises heavy or incorrigible influence of the administration where it loses the capacity to perform its basic functions, heavy damages have been caused to the information assets and the financial losses are very big.

3. The means for management of the access permit to determine and control the actions which various users of information systems and processes in them can perform in respect of the information resources. The logic management of the access has to permit that a majority of admissible operations be determined for every user or process and to control the enforcement of the established rules.

4. The means for management of the access of the participants in the electronic exchange have to include three categories of functions:

a) administrative functions – creation and accompanying of attributes for management of the access;

b) auxiliary functions – servicing of the processes of access of the users;

c) information functions – gathering of information for the processes of access in view of improvement of the interaction.

5. Every individual unit of the administration shall manage the identifiers of the users of the information systems through:

a) unique identification of every user;

b) verification of the identifier of every user;

c) regulation of the administrative procedures for distribution. Replacement of lost, discredited or damaged identifiers;

d) termination of the action of the identifier after a specified period of lack of activity;

e) keeping of an archive of the identifiers.

6. The information systems of the administrative bodies have to hide the echo image of the identifying information in the process of verification of the identity with the aim to protect it against the use on the part of unauthorized persons.

7. In case of verification of the identity using cryptographic modules the information system has to apply methods corresponding to the standards entered into the section "Information security" from the Register of the standards.

8. In order to formulate internal rules for the network and information security in the administrations the following content of the section related to the management of the access of the participants in the electronic exchange shall be recommended:

a) documented policy for management of the access including objectives, scope, obligations, coordination of the organization structures;

b) documented procedures for appropriation of privileges, accounts and other rights in compliance with the policy;

c) determination of limitations of the amount of unsuccessful attempts of the user to

enter into a system for a defined interval of time after which its account shall be locked;

d) determination of the warning messages informing the consumer before the provision of access about:

- the general limitations imposed by the system;
- the possible monitoring, keeping a protocol and audit of the use of the system;
- the necessary consent of the user for monitoring and keeping protocol in the case of use of the system;
- the prohibitions and the possible sanctions in case of unapproved use of the system;
- the possible actions of the user which can be performed by the information system without the necessity for authentication and authorization.

9. In compliance with the procedures referred to in p. 3 the Heads of the administrations shall organize the conducting of the following events:

a) organization of delivery of services to all citizens and organizations with equal priority;

b) recording in the lists of participants kept by the system of all citizens and organizations which have participated in the information exchange in the information systems of the administrative bodies;

c) storage of archive information for a period of one year for all participants who have used electronic administrative services from the public information systems;

d) organization of the access of the employees through a system of individual passwords; the passwords have to be changed periodically and at least once at every 6 months;

e) making a review and updating of the rights for access of the employees who maintain the work of the information systems in the administrations.

10. Every employee in the administration recorded in the respective directory LDAP server (central or local) has to receive a unique user name and a password for access only to the information systems which are necessary for him/her to fulfil his/her official duties. The password has to contain between 8 and 16 alphabetic-digital symbols and to require change every month.

Annex 6 to Article 35

Classification, control and management of the information assets

1. The cards of the available information resources in the respective administration have to determine unambiguously:

a) a specific employee for what information resources he/she is responsible (computers, equipment, software products/systems, data base);

b) a specific software product/information system and/or what data base on what computers and equipment are used.

2. The inventory lists for the available information resources in the respective administration have to include:

a) for hardware facilities (without the ones with quick depreciation, such as mice, keyboards and others of the kind) the minimum set of data which have to be kept shall include:

- serial number;
- factory number;
- model;

- description of the basic technical parameters (processor/frequency, size of the memory and kind/type, disk model and size, power feed – power and model/type, list of the accessories to the facility, etc.);
- date of acquisition;
- date of commissioning into exploitation;
- date of taking out of exploitation;
- date of sale/discarding/donation;
- location of the facility;
- name of the employee responsible for the functioning of the facility;
- name/names of the employee/employees using the facility;
- dates of servicing and repair of the facility;
- description of the service/repair made;
- what are the facilities that this facility is connected to;
- the work of what facilities depends on the correct functioning of this facility;
- what are the facilities from the operation of which the correct functioning of this facility depends;
- what working processes are being serviced by this facility.

b) for software products the minimum set of data which have to be maintained shall include:
- name of the product;
- version of the product;
- list of the minimum requirements towards the hardware for the normal operation of the product;
- date of acquisition;
- date of installation and adjustment;
- date from which the license for use of the product starts to expire;
- machine/machines where the product is installed;
- date of taking out of exploitation;
- date of expiry of the license for use of the product;
- date on which changes have been made on the adjustment or in the product itself;
- description of the changes made;
- name of the employee who has installed the product;
- name of the employee who has made the adjustments;
- name of the employee who has made the changes;
- name of the file in which the state before the changes is being stored;
- what working processes are being serviced by this product;
- the operation of what software products depends on the correct functioning of this software product;
- on the operation of which software products the correct functioning of this software product depends.

3. On the workstations and the servers in the administrations only software products shall be installed for which the respective administration is having a license for use.

4. All information systems which are commissioned into exploitation in the administrations have to be accompanied with detailed documentation for:

a) all functions of the client, the application and the data base;

b) the administrative means for access and adjustment;

c) schemes of the data bases with detailed description of the tables and the

connections;

d) the controls during the entry and exchange of data;

e) the controls during the processing and the processing results;

f) the application with all modules, "use cases", UML schemes and interfaces.

The installation and the adjustment of new software and hardware products has to be planned and all persons using the concerned resources have to be informed no less than 3 days before the installation or the adjustment has been made.

6. Before installation reserve copies of the software, the files and the data bases have to be made and a "roll back" plan has to be developed.

7. The installation, the adjustment and the maintenance of new software and hardware products has to be made in periods of minimum loading of the respective resources.

8. Before installation in the operationally functioning systems of new software and hardware products they have to be tested in a test environment which is close to the maximum to the real working conditions.

9. The employees in the administrations shall bear material liability for the mobile units made available to them for use. The mobile units shall be received by the employees who are using them against a signature in a document containing the full description of the mobile unit and the installed software.

10. The services for an active analysis of the level of protection of the system (active scanners of the level of protection) shall permit to detect and eliminate deficiencies in the system for protection of the information assets before their use by ill-intentioned persons.

Annex 7 to Article 37

Management of the exploitation processes

1. The creation of zones of security in the information system stemming from the international standard ISO/IEC 15408-2 "Common Criteria" is recommended as main means for the management of the exploitation processes in the information systems of the administrations for ensuring information security.

2. The security zones shall be areas of the software architecture of the system in which a specific complex of measures has been defined that ensure a specific security level. The zones shall be adequately separated one from the other and the transfer of data from one zone to the other shall be strictly regulated and shall be realized through control objects as protection walls, proxy-servers, etc.

3. When developing the security a demilitarized zone (DMZ) has to be maintained – a network area located between the public uncontrollable part of the network (usually connected to the Internet) and the internal protected part of the system. The demilitarized zone has to organize information services towards the two parts of the network while protecting the internal part against unregulated access.

4. The security measures in the management of the exploitation processes in information systems of the administrations have to include:

a) in project planning of the information systems preference has to be given to systems with multi-layer architecture in which the client, the application and the data shall be logically and physically separated;

b) Instruction for reserving and archiving of data and files has to be developed and approved;

c) reserve copies have to be made regularly of the data bases and the files in the file servers; the schedules for reservation shall be determined depending on the character of the activity of every administration; reservation every day shall be recommendable;

d) storage of the reserve copies has to be provided in a special separate premise/location/fireproof cash-box;

e) regular renovation of the carriers on which reserve copies are recorded has to be ensured (at a period of 2/3 of their expiry date);

f) regular preparation of archive copies of the data bases and the files in the file servers has to be ensured; the schedules for reservation shall be determined depending on the character of the activity of every administration; reservation made every month shall be recommendable;

g) regular renovation of the carriers on which archive copies are recorded has to be ensured (at a period of 2/3 of their expiry date);

h) the archive copies have to be stored in another building in a fireproof cash-box;

i) the access to reserve and archive copies shall be made under the control of the employee responsible for the information security.

Annex 8 to Article 37

Management of electronic messages

1. The management of the electronic messages in the administrations shall be made in accordance with Recommendation X.700 of the International Telecommunication Union (ITU) and shall be realized through:

a) monitoring of the components;

b) control (i.e. formulation and realization of managing effects);

c) coordination of the work of the system components.

2. The systems for management have to:

a) give possibility of the administrators to plan, organize, control and record the use of the processes related with the provision of network and information security;

b) permit adjustment of the system to changes of the requirements for security;

c) provide predictable behaviour of the system at various circumstances.

3. The management of the network security shall be based on recommendations X.800 and X.805 of the International Telecommunication Union (ITU).

4. In accordance with the recommendations referred to in p. 3 for the realization of the functions of the network security the following mechanisms and their combinations have to be used:

a) encrypting;

b) digital certificates;

c) mechanisms for access management;

d) mechanisms for control of the integrity of the data, including the integrity of the flow of messages;

e) identification mechanisms;

f) mechanisms for supplementing the traffic;

g) mechanisms for management of the route directions;

h) mechanisms for marking and recording of the communication characteristics.

5. The protection of the electronic messages in the Internet shall include:

a) protection wall;

b) protection against viruses and unwanted code;

c) protection from spam;

d) verification of the enclosed files for viruses and unwanted code;

e) protection against DoS (denial of service) attacks;

f) protection from HA (harvesting attacks);

g) protection of the e-mail addresses from searching robots;

h) protection from outflow of information;

i) protection against spy software (spyware);

j) protection of IM (instant messaging);

k) protection of the voice communications (Skype, ICQ, etc.);

l) verification for conformity with the policies enforced in the respective administration;

m) verification for conformity with the adopted normative documents;

n) control on the exchange (sending/receipt) of big files in compliance with the adopted policies;

o) prioritization of the incoming and outgoing mail depending on the profile of every employee;

p) redirection of the mail depending on the adopted policies;

q) automatic encrypting of the outgoing mail when necessary in compliance with the adopted policies;

r) automatic addition of a text to incoming/outgoing messages in compliance with the adopted policies.

6. Received messages automatically classified as a spam or containing an unwanted code have to be recorded in specialized folders and to be accessible for control and processing by authorized persons (the employee responsible for the information security, specialists from the National centre for action in case of incidents in respect to the information security in the information systems of the administrative bodies, etc.).

7. For the protection of the "routing-infrastructure" and the "routing-protocols" the Recommendations of the Work groups RPSEC (Routing Protocol Security Requirements) and SIDR (Secure Inter-Domain Routing) of the international organization IETF (Internet Engineering Task Force) have to be used.

8. A "system for the management of the domain names (DNS)" with a modification of the DNS protocol with enlargements for identification (DNSSEC) which is based on the specification of the IETF PFC 4033 has to be used for management of the names and the domains in the infrastructure in Internet.

9. Protocol SSL ("Secure Socket Layer") version 3.0, formulated from IETF ("Internet Engineering Task Force") or VPN ("Virtual Private Networking") solutions for secure encrypting of the sessions shall be used for realizing a protected exchange along the protocols HTTP, LDAP, FTP and others.

10. Protocol XMLENC, formulated by the W3C consortium has to be used for encrypting of XML base messages at "session" level.

11. Protocol XAdES (XML Advanced Electronic Signature), formulated in Recommendation TS 101 903 of ETSI (European Telecommunications Standards Institute)

and based on Recommendation XML DSIG of Working group "XML-Signature Working Group" of the W3C consortium has to be used for the electronic signing of XML based documents.

12. Protocol XKMS ("XML Key Manipulation Service"), based on the Recommendation XKMS 2.0 of the W3C consortium has to be used for operation with the public keys during electronic signing of XML based documents.

13. A copy of the whole official electronic mail of the employee shall be stored on the mail server of the respective administration for no less than two years after the employees have left.

14. The employees in the administration can use only their official electronic mail for receipt and sending of official correspondence.

15. Electronic messages sent by employees in the public administration shall contain compulsory identifying information for contact with the respective employee:

a) name;

b) telephone;

c) electronic mail;

d) position;

e) institution.

16. At the end of every outgoing electronic mail a disclaimer has to be automatically attached and instructions for the addressee for actions in case of wrong receipt.

Annex 9 to Article 41

Protection against unwanted software

1. The unwanted software which can exploit the vulnerability of one or several information assets and to provoke disturbances of their normal work, damage or destruction shall include the following main programmes:

a) computer viruses;

b) network worms;

c) Trojan horses;

d) logical bombs.

2. The protection against unwanted software in the information systems of the administrative bodies has to be oriented in two main directions:

a) through prohibition for the use of unregulated software;

b) through compulsory use of approved for the whole administration antivirus software and software for the discovery of unregulated changes of information assets.

3. The administrator of the unified national network has to apply means for detection of attempts for penetration at different levels and perimeters of the network.

4. The programme products designed for detection of attempts for penetration have to distinguish the following suspicious actions in the network:

a) attempts to use services blocked by protection walls;

b) unexpected applications, especially from unknown addresses;

c) unexpected coded messages;

d) exclusively active traffic from unknown servers and units;

e) considerable changes of previous actions of the network;

f) attempts for the use of known system errors or vulnerabilities;

g) attempts for entry from unknown consumers from unexpected addresses;

h) unsanctioned or suspicious use of administrator functions;

i) considerable changes in the usual actions of a consumer, etc.

5. In case of clear attempts for penetration it will be necessary to:

a) inform the system administrator to undertake adequate measures;

b) include or to limit the network services related to the information asset – object of the penetration.

6. Every unit which is included in the network of the respective administration has to be automatically checked for viruses and unwanted software before obtaining access to the resources of the network.

Annex 10 to Article 43, (2)

Actions during monitoring of the events and the incidents in the information systems of the administrations

1. When storing information for events and incidents related to the information systems of the administrations the following records have to be created:

a) date and time of occurrence of the event;

b) unique identifier of the user – initiator of the action;

c) type of the event;

d) result from the event;

e) source of the event;

f) list of the affected objects;

g) description of the changes in the protection system resulting from the event.

2. The Heads of the administrations must determine exact procedures for monitoring of the use of the system with which they will ensure the realization only of regulated processes on the part of the users. The monitoring procedures have to ensure:

a) realistic assessment and measures for risk management;

b) following of exceptions or abnormal behaviour of users for a specified period;

c) ensuring records both of the successful and refused attempts for access in the system.

3. The Heads of the institutions have to ensure the maintenance of uniform time in the information systems according to the Ordinance for the electronic administrative services, adopted by Decree Nr. 107 of the Council of Ministers of 2008 (State Gazette, Nr. 48 of 2008) to ensure precision and completeness of the records of the logs which can be used for investigation of illegal actions or for the needs to use court evidence.

Annex 11 to Article 45, (2)

Parameters of the physical security

1. For ensuring physical protection of information systems the Heads of the administrations shall undertake the following measures:

a) measures for management of the physical access;

b) fireproof measures;

c) protection of the supporting infrastructure;

d) protection of the mobile systems.

2. It is recommended for the measures for physical protection to include the following infrastructure components:

2.1. The buildings and the premises in which the technical equipment is located, the software and the archives, necessary for the information systems of the administrative bodies have to satisfy the following architectural-construction requirements:

a) the premises have to have concrete or brick walls;

b) the plots have to be from reinforced concrete with a thickness of 0,15 (m);

c) the premises should have special movable openings which shall protect from overpressure;

d) the double floor should have a height no less than 0,30 (m);

e) the suspension ceiling should have a height of no less than 0,50 (m);

f) the air-conditioning systems for the premises should permit management from alarm signals of a fire extension system;

g) a separate room to be ensured next to the premises in which the acting and the reserve battery bottles with fire extension agent have to be located.

2.2. The premises which shall accommodate the technical equipment, the software and the archives necessary for the information systems of the administrations shall be equipped with the following technical systems for protection, safety and safeguard:

a) fire extinguishing system which has to satisfy the requirements of EN 14520;

b) air conditioning;

c) reserve power supply;

d) systems for television video monitoring;

e) systems for control of the access.

3. The meetings between the visitors and the employees in the administration have to be made in specialized premises.

4. In the cases referred to in p. 3 a list has to be kept of the visitors when and whom they have met and on what issue. The list shall be stored for no less than one year from the date of the visit. The list can also be kept only in electronic form.

5. It shall be compulsory for the employees using portable computers to use passwords for access to the resources of the mobile units (disc units, system plugs, software, etc.).

Annex 12 to Article 48

Management of incidents related to the information security

The planning of the activity for management of incidents related to the information security has to include the following stages:

a) identification of the critically important functions of the system and setting of the priorities for the rehabilitation jobs;

b) identification of the resources necessary for the realization of the critically important functions;

c) determination of a list of the possible incidents with a probability for their

occurrence proceeding from the risk assessments;

d) development of strategies for rehabilitation jobs;

e) preparation of events for realization of the strategies.

2. The cycle of incident management should include the following basic stages:

a) preparation;

b) detection and analysis;

c) restriction of the effect, elimination of the cause, rehabilitation;

d) activity after the incident.

3. Critical element of incident management is the immediate restoration of the activity of the system.

4. The policy for protection against incidents and rehabilitation jobs of the respective administration which results from the risk assessment referred to in Chapter three, section III of the Ordinance, has to clearly identify the means for reservation and rehabilitation in view of covering a level of reservation above five according the classification of Share Association.

5. The means referred to in p. 4 can be:

a) parallel recording or mirror replication of the stored data (technologies "Disk Mirroring" or "RAID" ("Redundant Array of Independent Drives");

b) establishment of a centre for rehabilitation after incidents (the so called "Disaster Recovery Centre"), in which a constant archive storage is made ("back-up") of the information from the system so that its activity to be restored after an incident;

c) establishment of a reserve calculation centre in which a replicated status is maintained of the critically operationally acting systems so that their activity to be immediately undertaken by it.

6. The plan for actions in case of incidents of the respective structure in the administration should include events which to be held after the rehabilitation and to aim at avoidance of similar incidents. These could be measures for:

a) increasing the level of control of the access;

b) change of the configurations of the security zones;

c) change of the regime of physical access;

d) installation of additional modules for protection to the software of the system;

e) reconstruction and declassification of the carriers, etc.

Annex 13 to Article 51

Measures for security in respect of the personnel

1. In order to achieve information security in respect of the personnel the Heads of the administrations shall be obliged to undertake the following measures for identification of the employees and their authorization to perform specific actions in respect of the exploitation of the information systems:

a) the access of the employees in the administration to their workstations and the general information systems should be realized with official username and password;

b) the access of the employees in the State administration to the specialized information systems should be realized with an official user name, password and certificate for

a public key;

c) the granting of rights to access for various groups of employees and Heads to the resources of the information systems in the respective administration should be made on the basis of the approved profiles in accordance with Article 52 of the Ordinance;

d) belonging to a profile corresponding to his/her official duties specified in his/her job description has to be defined for every employee in the administration;

e) the employees in the administration should have the right to access to those resources of the information systems of the administration in which they work or to the systems of other administrations only as far as they need them for the performance of the official duties in accordance with their job description;

f) refresher courses in network and information security to be passed by all employees in the administration should be organized every year;

g) all employees in the administration should pass training for actions in case of incidents with the network and information security.

2. The application for verification of certificates for public keys (including electronic signatures) must use the procedure for verification through Certificate Revocation Lists (CRL), based on the specification RFC 3280 of IETF (Internet Engineering Task Force) or according to Protocol OCSP (Online Certificate Status Protocol), based on the specification RFC 2560 of IETF.