DOCTRINE OF INFORMATION SECURITY OF THE REPUBLIC OF BELARUS

SECTION I
GENERAL PROVISIONS

CHAPTER 1
WORLD SIGNIFICANCE OF THE INFORMATION SPHERE

1. At the current stage of world development, the information sphere plays a key role in the life of a modern person, society, country and has a comprehensive impact on the ongoing economic, political and social process in countries and regions. People's need for information has increased as a result of growing dynamism of social relations, global and regional events, enhanced general intellectual capacity.

The information society being formed on a global scale represents a new stage in civilization development with predominance of knowledge and information. In the information society information technologies affect all spheres of human activities. The role of information technologies is dramatically increasing in ensuring the human rights and freedoms.

Telecommunication industry has become one of the most dynamic and promising areas of global economy. National economic interests and promising investments are increasingly connected to information technologies.

2. At the same time, transformation of the society into the information community causes new risks, threats and challenges that directly affect national security including protection of information space, information infrastructure and information systems and resources.

CHAPTER 2
RELEVANCE AND IMPORTANCE OF THE DOCTRINE OF INFORMATION SECURITY OF THE REPUBLIC OF BELARUS

3. The creation of the information society in the Republic of Belarus with an information access, dissemination and use of knowledge for progressive development is regarded as a national priority and a state task.

4. The relevance and importance of the Doctrine of Information Security of the Republic of Belarus (hereinafter referred to as the "Doctrine") is determined by the following factors:

the increased importance of the information society development in the

Republic of Belarus, its' role in the socio-economic development of Belarus as a sovereign and independent state, the security of the implementation of national strategies and plans for creating a digital economy and scientific and technical progress in general;

the need for substantive and comprehensively conscious protection of national interests in the information sphere, defined by the National Security Doctrine of the Republic of Belarus, generalization of practically and scientifically based views on ensuring information security, concretization and specification of approaches to this activity;

the need to consider information security as a separate phenomenon and regulatory institution, as well as the legal consolidation of the foundations of the state policy aimed at the protection of national interests in the information sphere;

the creation of a new sphere of public relations to ensure information security;

the importance of improving the coordination and accountability of the entities' activities involved in the development of the information sphere and ensuring its' security, the sustainable and consistent functioning of mechanisms to respond to risks, threats and challenges of information security;

the need to inform both citizens and the international community on the views adopted in the Republic of Belarus in the field of information security and the priorities for ensuring it;

the integration of Belarus into the international information security system, the importance of increasing the conceptual and technological compatibility and synchronisation of the goals and objectives of the national information security system with the corresponding systems of other states and organizations.

CHAPTER 3
SUBJECT, PURPOSE, TASKS OF THE DOCTRINE, ITS' CORRELATION WITH THE OTHER DOCTRINAL DOCUMENTS

5. The Doctrine is a system of official views on the essence and content of ensuring national security in the information sphere, which determines strategic objectives and priorities in the field of information security.

The Doctrine provides an integrated approach to the information security, creates a methodological basis for better activities of its' strengthening, serves as a basis for the formation of public policy, creating measures of improving the information security system, constructive interaction, consolidation of efforts and improving the protection of national interests in the information sphere.

6. The Doctrine is based on the Constitution of the Republic of Belarus, the legislation of the Republic of Belarus in the areas of national security,

informatisation, the development of digital economy and the information society, science and technology, protection of intellectual property, and other legislative acts.

The Doctrine is based on the National Security Doctrine of the Republic of Belarus, namely:

refers to understanding of the main modern global trends, national interests in the information sphere defined in the National Security Doctrine, potential or real threats to the national security;

specifies goals, objectives and principles of ensuring national security in the information sphere, main directions of managing internal sources of threats and protecting national security in this area from external threats;

implies the implementation of these goals, objectives and principles as an inalienable part of the national security system.

7. The Doctrine also refers to geopolitical interests of the Republic of Belarus, its' place and role in the modern world. The Doctrine is based on the cooperation agreements in the information security sphere of the member states of the Commonwealth of Independent States, the Collective Security Treaty Organization allies, bilateral agreements and the other commitments of the Republic of Belarus in the field of the national information security, takes into account basic provisions of acts of international organizations, including resolutions of the United Nations General Assembly and recommendations of the Organization for Security and Cooperation in Europe.

8. For the purposes of the Doctrine, the following concepts and their definitions are used:

impact on information – an action aimed at changing the form of provision and (or) content of information;

state information system – a set of data banks, information technologies and complex (complexes) of software and hardware tools, which is financed from the republican or local budgets, state extra-budgetary funds, as well as from state legal entities' funds;

state information resource – a set of well-documented information, including databases and other sets of interrelated information in information systems, which is financed from the republican or local budgets, state extra-budgetary funds, as well as from state legal entities' funds;

destructive informational impact – an information impact on political and socio-economic processes, the public authorities' activities, as well as on individuals and legal entities in order to weaken the state's defence capabilities, disrupt public security, adopt and conclude faulty decisions and international treaties, deteriorate relations with the others states, create socio-political tensions or

prerequisites for a threat of an emergency, destroy traditional spiritual and moral values, prevent from the ordinary activities of the public authorities and harm the national security;

information protection – a complex of legal, organisational and technical measures, which are aimed at information confidentiality, integrity, authenticity, accessibility and security;

information security – a state of protection of balanced interests of individuals, society and state from external and internal threats in the information sphere;

information infrastructure — a set of technical means, systems and technologies for creating, transforming, transmitting, using and storing information;

information sovereignty of the Republic of Belarus – inalienable and exclusive supremacy of the state's right to independently determine the rules of possession, use and disposal of national information resources, implement an independent external and internal state information policy, form a national information infrastructure, and ensure an information security;

information sphere – aggregate understanding of information, informational infrastructure, subjects carrying out the collection, forming, distribution and use of information, as well as of a system regulating public relations arising from such actions;

information space – sphere of activities connected with creation, transformation, transmission, use, storage of information, which are influencing, inter alia, individual and social consciousness and the information itself;

cyberattack – intentional impact of software and (or) combined software-hardware tools on objects of information infrastructure, telecommunications networks used for organizing the interaction among and between such objects, with the aim of disrupting and (or) termination of their functioning and (or) creating a security threat for information processed by such objects;

cybersecurity – a state of security of informational infrastructure and of information contained therein from external and internal threats;

cyberincident – an event which actually or potentially threatens the confidentiality, integrity, authenticity, accessibility and preservation of information, as well as itself constitutes a violation (threat of violation) of security policies;

cyberterrorism – attacks on information systems which threaten the health and lives of people and are capable of provoking serious disruptions in the functioning of critically important objects with the aim of influencing the decision-making of authorities or hampering political or other public activity, or intimidation of the population, or destabilizing public order;

cyber-sustainability – capability of an information system to foresee the changes in situation and adapt in a timely manner to them with the aim of successful prevention of negative consequences or prompt recovery after a cyberincident;

international information security – a state of international relations in absence of a breach in world stability and creation of a security threat in the information space for states and the global community;

provision of information security – a system of legal, organizational, technical and economic measures aimed at discovering threats for information security, preventing their actual implementation, suppression and elimination of consequences of implementation of such threats;

crimes in the information sphere – crimes against information security, specified by the Criminal Code of the Republic of Belarus (cybercrimes) or the other crimes that are carried out by information, information systems or networks;

data sovereignty – subordination of the relations referring to the digital form appearing in the territory of Belarus and falling within the national jurisdiction of the Republic of Belarus. The other terminology used in the Doctrine is correlated with the terminology of the legislation of the Republic of Belarus and international acts to which the Republic of Belarus is a party.

SECTION II
THE STATE AND DEVELOPMENT OF THE INFORMATION SPHERE IN THE REPUBLIC OF BELARUS

CHAPTER 4
THE HUMANITARIAN ASPECT OF THE INFORMATION SPHERE

9. The fundamental national interest of the Republic of Belarus in the information sphere from a humanitarian point of view is the realisation of the citizens' constitutional rights to receive, keep and distribute complete, reliable and timely information, freedom of opinion and expression and privacy.

10. Nowadays the state of the information sphere in the Republic of Belarus is characterised by the high level of access of the population to media information. The number of national mass media (hereinafter referred to as the "media") and internet resources both state and non-state are steadily increasing. The Belarusian information space is open for active work of the foreign media and internet resources. In the country the bandwidth of external access channels to the internet, the number of internet users and electronic network subscribers are increasing annually. The interaction between citizens in the information sphere is also developing. New networks for communication and exchange of information, for

sharing experience and knowledge, for public discussion of draft regulations are created. The crowdfunding is widely practiced. The role of public councils and independent experts in state authorities' decision-making process is increasing. To preserve the historical and cultural heritage and enhance legal awareness, the institutes of public self-control are being formed.

In general, the Belarusian information space is fully characterized by global trends of information, including transferring of the media to the digital format (digitalization), a combination of their various types (multimedia), the adaptation of the information product to distribution via the Internet, rapprochement and merging of various types of media (convergence).

11. At the same time, the global rise of information and communications technologies (hereinafter referred to as the ICT) leads to constant appearance of new information sources, which objectively reduces the share of domestic content in the information space and therefore requires more active promotion. Basing on this, it is necessary to take state level measures to increase the volume, diversity and quality of national content, the speed of its' delivery, raise public confidence to official information and state-run media, adapt the forms of information dissemination to the primary information needs of citizens, as well as achieve a balance among personal, public and state interests.

CHAPTER 5
THE TECHNOLOGICAL ASPECT OF THE INFORMATION SPHERE

12. The main trends of informatisation in the Republic of Belarus are development of transparent and effective public management system, support fast, convenient and secure lines of communication between the state, business circles and citizens, modernization of national information infrastructure, ICT implementation in the real economy, improvement of social sphere on the ICT bases, strengthening the information technologies sector.

13. Digital transformation of economy is an important component of the information society development and one of the main directions of development of the Republic of Belarus, as a result of which all sectors, markets, spheres of state activity should be reoriented in the coming decades to new digital economic models. In order to solve this task, a structure for managing informatisation and an architecture for an electronic government is set up in the country. Innovative digital technologies are developing based on artificial intelligence systems, neural networks capable of working with various information resources, including with big data blocks, distributed computing methods (cloud technologies), transaction block register technologies (blockchain).

Belarus consistently participates in the international processes of informatization, including through the Union State of Belarus and Russia, the Eurasian Economic Union, the Commonwealth of Independent States, the European Union and other systems of international political and economic cooperation.

14. At the same time, the application of information technologies in the real sector of the economy is not high. The degree of digitization of economic sectors varies, which reduces the expected synergetic effect of a synchronous informatization. Given that, it is worthwhile developing a digital policy for specific areas of public life, to aim pilot projects of digitization at a sector as such, to create hubs of digital transformation competence. It is necessary to shift e-government from simple provision of services at the request of citizens to proactive work with the population. Rapid development of ICT and the increasing information needs of society necessitate the adoption of new standards in the field of telecommunications, improving the productivity and reliability of network infrastructure.

SECTION III
THE STATE POLICY OF INFORMATION SECURITY

CHAPTER 6
THE GOALS AND DIRECTIONS OF THE STATE POLICY

15. The purpose of information security is to achieve and maintain such a level of protection of the information sphere, which ensures the implementation of the national interests of the Republic of Belarus and its' progressive development.

Ensuring information security is carried out in accordance with the state policy in this area, which includes the formation, improvement and implementation of organizational, legal, scientific and technical, enforcement and economic measures to ensure national security in the information sphere. The development of the latter guarantees its' security.

16. At the state level, monitoring, analysis and assessment of information security are carried out, and indicators of its assessment are used. Priority directions of information security threats prevention, minimization of their destructive impact and localization of the consequences are determined.

A complex of strategic and tactical measures to prevent and neutralize information risks, challenges and threats is developed and implemented.

17. The constitutional right of citizens to freely search for, receive, transmit, produce, store and distribute information in any legal way, the right to privacy protected by law, protection of personal data and copyrights are secured, as well as

the balance between the rights and restrictions related to national security. Legal, organizational and technological conditions are formed for the safety of the functioning of national mass media; state and public control over their activities is carried out.

Citizens and organizations enjoy maximum access to state electronic services, administrative procedures, information resources of state bodies and organizations.

Citizens and society's awareness of threats to national security and of state safeguard measures, as well as their involvement in ensuring the security of the information sphere, are increasing.

18. The state promotes the security of national information systems and of the software used by citizens and organizations. In order to improve the resilience of the public sector to information risks, advanced technologies are developed, new means and methods of ensuring information security are introduced.

Information security standards are developed to conduct the auditing of state information security systems. The smart design of information security solutions is developed. At the normative level, critical informatization objects (hereinafter – CIO) are identified and regulated. The development of security technologies in business and life activity is encouraged.

19. Activities inflicting significant damage to legally protected interests in the information sphere or creating a danger of such damage are criminalized in accordance with the existing worldwide approaches. Steps shall be taken to reduce the threats of cybercrime, including cyber-terrorism, investigate and curb the actions of individuals involved in terrorist activities, block channels of terrorism propaganda, as well as attracting and recruiting supporters, encouraging and provoking terrorist activity, and financing terrorism.

Legal regimes of information and information resources security, technical conditions and security policies are introduced. Identification and bringing to justice of persons harming the state information systems will be exercized, the state protection of the interests of citizens and organizations, regardless of their form of ownership, pursued.

20. The state, the public, the business community, the media foster interaction in order to timely detect risks and challenges to information security, to hinder cyber attacks and actions of destructive information impact and to increase the effectiveness of law enforcement.

21. The personnel potential is of paramount importance for ensuring information security. Individuals, providing information security, cooperation between government bodies, educational institutions and specialized enterprises in selection, training and employment of such personnel, integration of information security topics into educational programmes at all levels, are trained at the modern

educational and technological level, undergo special training, retraining and professional development. The state forms an order for such training.

22. Information security equipment shall be produced. The scientific potential and funding of the research and creation of new solutions in the field of information security, including technical protection of information, cryptology, criminology, criminalistics, increase. The state finances priority areas in information security, primarily through government programmes. Innovative methods and technologies to protect information resources and systems are developed.

23. Efforts are made to improve the effectiveness of international law and the observance of moral norms of responsible behavior. Development and implementation of confidence-building measures in the information space are supported. International exchange of experience and data on threats to particular national interests, including on information system vulnerabilities and incidents in information infrastructures, is built up and developed.

24. The security of the information sphere and the state of informatization in the Republic of Belarus in general are assessed according to international ratings and established criteria, indexes and indicators including basic indicators of social and economic development, national security as well as those reflecting other state activities connected with the sphere in question.

CHAPTER 7
INFORMATION SOVEREIGNTY

25. In the context of aggravating international contradictions, it becomes problematic to work out effective and generally accepted rules for the behavior of the world community in the information space. The approaches of various countries to assessing threats in the information sphere and countering them do not coincide but are polarized in individual areas.

In this regard, the most important target of information security is the information sovereignty of the Republic of Belarus.

26. Information sovereignty is achieved, first of all, through the formation of a legal regulation system of relations in the information sphere, which ensures a safe sustainable development, social justice and harmony.

27. Within the framework of this system, the state ensures the development of national media and telecommunications, modern ICT, the national industry of information technology, as well as the protection of national markets for information and telecommunications services, which reduce dependence on foreign technologies and digital inequality. The society cultivates and stimulates a critical attitude to manifestations of disrespect for national attitudes, traditions and

violations of moral norms and rights in the information sphere, intolerance for disinformation, information manipulations and other implicit information-psychological influences.

28. Legal conditions and boundaries of activities of foreign and international actors in the national information space are formed to meet the needs of citizens in external information exchange without cultural and information expansion, interference in the internal affairs of the Republic of Belarus.

29. The necessary conditions for the construction and safe development of a functional, technologically self-sufficient, reliable and sustainable information infrastructure are being created. Information resources, including state secrets, other protected information and personal data are being protected which ensures political independence of the state, protection of human living space, preservation of the spiritual and cultural values of the Belarusian society, scientific and technological advantages and the realization of other national interests. The Republic of Belarus is implementing the principle of "data sovereignty".

30. The aspiration of information sovereignty does not disagree with the international legal principles of ensuring the rights and freedoms that guarantee competitive and free development in the context of global digital transformation.

CHAPTER 8
INFORMATION NEUTRALITY

31. In international relations, the information sovereignty of the Republic of Belarus is ensured on the basis of the principle of information neutrality, which provides for a peaceful external information policy, respect for the universally recognized and generally accepted rights of any state in this field, exclusion of intervention in the information sphere of other countries aimed at discrediting or challenging their political, economic, social and spiritual standards and priorities, as well as damaging the information infrastructure of other countries and participating in their information confrontation. At the same time, the Republic of Belarus defends its own national interests in the information sphere using all available forces and means.

32. To ensure the policy of information neutrality, the level of Belarus's presence in the global information space is increasing, international information exchange is expanding, the establishment and regulation of universal rules of conduct in this area are being supported, and agreements are being concluded to ensure international information security.

CHAPTER 9
STATE RESPONSE TO RISKS, CHALLENGES AND THREATS IN THE INFORMATION SPHERE

33. The state responds to risks and challenges in the information sphere in order to prevent their transformation into threats to national security, the development and scaling of harmful effects.

Responding to risks and challenges in the information sphere is carried out by all state bodies and organizations without exception in accordance with the scope of their activities and according to their direct purpose as fully and efficiently as possible. The state acting on behalf of these agencies and organizations ensures the timely adoption of security measures, immediately notifies interested parties, minimizes damage and localizes the consequences, determines the persons and organizations involved, accumulates experience in counteracting threats.

34. The state's response to risks, challenges and threats in the information sphere involves collecting information on the technologies used, methods of destructive information impacts and committing cybercrime, analyzing, assessing and predicting the security status of this area, identifying the challenges and threats, localization of negative consequences and restoration of the caused damage. The security and stability of information security objects, including information infrastructure, information resources, individual, group and mass consciousness to the threats, is determined.

Conditions for the occurrence and realization of risks, challenges and threats to information security are identified and excluded.

35. Scenarios and plans for crisis response to cyber-attacks, computer incidents, acts of destructive information impact, other threats to information security are being prepared and implemented, and exercises and training of response forces are conducted.

The policy of information restraint is being implemented, which is expressed in the demonstration of a reliable readiness to repel destructive information effects, a sufficient possibility of technological, organizational, legal counteraction to threats in the information sphere and the identification of their sources.

36. In the event of a significant complication of the information environment, including the need to ensure the military security of the country, additional measures are taken to protect the information sphere by legal, information technology, technical and other methods (informational confrontation), the priority interaction of the military organization of the state and the civil sector is provided.

37. Armed Forces of the Republic of Belarus, other military formations take measures to maintain information security within the scope of the mission assigned

to them using modern and high-technology forces and means.

38. Belarus participates in international response to potential risks, challenges and threats to information security in the framework of concluded treaties and agreements, carries out international cooperation in analyzing risks, challenges and threats to information security, exchange of experience and joint practical events.

SECTION IV
SECURITY OF INFORMATION SPACE AS ONE OF CRUCIAL CONDITIONS FOR THE DEVELOPMENT OF A SOVEREIGN, DEMOCRATIC SOCIALLY ORIENTED STATE

CHAPTER 10
CONDITIONALITY OF MEASURES TO GUARANTEE SECURITY IN INFORMATION SPACE

39. Global increase of the role of information in public relations, openness of information space and higher level of informatization of the population create conditions for new security measures in information field for a state to guarantee full realization of its sovereign rights and interests of socio-economic development.

40. Mechanisms of destructive informational and psychological influence on a personality are constantly being improved, and massive manipulation of mass conscience becomes as topical as battles for territories, resources, and markets. Through information space are carried out deliberate discrediting of constitutional foundations of states and their structures of power, dissolution of national mentality and uniqueness, engagement of people in extremist and terrorist activities, fomenting of interethnic and interconfessional strife, shaping of radical and protest potential. Information factor plays an increasingly significant role in interstate conflicts and latent actions aimed to disrupt sovereignty, territorial integrity of states and to arrest their development. As a result of information influence, connections of a person in society, way of thinking, methods or communication are significantly altered.

Of growing concern is active circulation of false, questionable and prohibited information in information space. Lower level of critical acceptance by information users to fake messages of news portals in social media and other online platforms creates preconditions for deliberate use of disinformation for destabilization of public perception for political, socially challenging and other similar reasons.

41. In view of this, of particular importance is responsible behavior of all stakeholders of information processes, as well as elaboration of common rules of communication in information space based upon the recognition of identical nature

of rights and obligations in existing reality (physical world) and virtual reality.

CHAPTER 11
MAIN DIRECTIONS OF SECURITY IN THE INFORMATION SPACE

42. For the Republic of Belarus main sources of threats of informational and psychological nature are information rivalry among main world's centers of power, as well as deliberate creation inside and outside a country of information grounds to discredit state foreign domestic and internal policies.

43. With that in mind, ensuring security of informational and psychological component of information sphere mainly implies preservation of information sovereignty and information neutrality policies, as well as creation of stable immunity against destructive informational and psychological effects on public mass consciousness and counteracting them when necessary.

44. For that, it is primarily needed to ensure formation, use and development of information space at state level exclusively for purposes of social, economic and cultural development, as well as constant, active and effective activity of government institutions, organizations, scientific and expert community in information space with special emphasis on reinforcing their activity in Internet.

45. As a matter of priority, it is necessary in the society to preserve traditional social norms and values, open and comprehensive information support and maintenance of state policy, as well as to lawfully prevent distribution of unlawful and questionable mass information.

CHAPTER 12
PRESERVATION OF TRADITIONAL NORMS AND VALUES

46. Increasing resistance of society to destructive information influence implies efforts focused on preserving traditional fundamental values of the nation formed in public consciousness, which are among the main elements of ensuring the nation's unity and pre-conditions for steady development of the state.

47. Information policy of the Republic of Belarus aims to promote such life priorities as humanism, peacefulness, good neighborliness, justice, mutual assistance, strong family relationships, healthy lifestyle, creative work as well as moral norms and positive legal awareness in Belarusian society. The information sphere fully reflects equal rights of all nationalities inhabiting the Republic of Belarus without exception, respectful attitude towards all traditional religions and beliefs. Support and comprehensive development of civic and patriotic ideology is of utmost importance.

48. The Belarusian language, along with constitutionally established bilingualism in the state, contributes to enhancing national identity of the Belarusian society and formation of its spirituality. Expansion of social functions and communicative possibilities of the Belarusian language, its full and comprehensive development alongside other elements of national culture act as guarantor of the state's humanitarian security.

49. Further consistent implementation of state historic policy is required. The policy should be aimed at consolidating in Belarus and abroad the national concept of the country's historical past and of Belarusian memory model developed in accordance with this Concept as the dominant one.

CHAPTER 13
INFORMATION MANAGEMENT AND SUPPORT OF THE STATE POLICY

50. Information management and support of the state policy aims at the development of mass political consciousness of citizens, enhancing the capacity and quality of public administration, strengthening the perception of Belarus in global information space. These activities are carried out through bringing, in transparent and prompt manner, reliable and full information to the public of the Republic of Belarus and world community on work of public authorities of Belarus, measures taken to improve social and economic relations, pending and adopted legislation and other legal and regulatory acts in domestic and foreign spheres.

51. The State shall provide development of constructive and comprehensive information interaction between authorities, mass media and public at all levels.

52. The competitiveness of state-owned mass media, including through national production of high-quality content and the development of a modern media measurement system, is of particular importance.

53. The State shall provide legal support to the domestic mass media aimed at improving quality of audiovisual products and expanding thematic and genre diversity of programmes, creating other additional development opportunities, including through legislative regulation of amount and quality of foreign broadcast in the Republic of Belarus, regulation of amount of advertising services, determination of the optimal conditions of registration.

54. Authorities, other State bodies and organisations, academic institutions, educational and cultural organisations, officials and representatives of the scientific and expert community carry out active, high-tech and wide-range activities in information space, including national and foreign electronic mass media, other internet resources and means of internet communication, as well as create

conditions for the formation of modern domestic media analytical, scientific and discussion platforms.

CHAPTER 14
MASS INFORMATION SECURITY

55. Relations in the field of mass media are based on the principles of legality, credibility, respect for human rights and freedoms, diversity of views, protection of morals and others. Along with the constitutional provision of freedom of speech in the Republic of Belarus, in order to comply with these principles legislative requirements for the dissemination of mass information consistent with world practice and generally accepted social standards are established. Public control over the dissemination of illegal and unreliable information in the information space is carried out.

56. The dissemination of information aimed at promoting war, extremist activities or containing calls for such activities, consumption of narcotic drugs and similar substances, pornography, violence and cruelty, other information prohibited by law, is not permitted. At the state level, measures are implemented to prevent the dissemination of information that could harm national interests, and unreliable information, as well as to reduce anonymity in the information space. When content is broadcast, it is not allowed to use hidden technological techniques that affect people's subconscious or have harmful effects on their health.

57. The dissemination of information without marking its age category is limited by law, and parental controls measures for the usage of information technology by children are encouraged.

SECTION V
INFORMATION INFRASTRUCTURE SECURITY

CHAPTER 15
CONDITIONALITY OF THE SECURITY MEASURES FOR INFORMATION INFRASTRUCTURE

58. Digital transformation of the economy and innovations in the field of ICT, together with global development and building of technological capabilities in interaction between people, business and public institutions make necessary the adoption of special measures that provides confidence and security in establishing and usage in modern information society of information infrastructure and data in information systems.

59. Political, socio-economic spheres, public and military security are becoming increasingly vulnerable to deliberate or accidental technological impacts, including in the face of inadequate global mechanisms for coordinated and effective prevention and containment of cyber incidents in the Internet.

The widespread operation of industrial facilities, transport, energy, telecommunications, health and life support systems by using automated control systems puts the life and health of the population, environmental and social security in direct relation to their reliability and security. Cyber-attacks on information infrastructure are considered as one of the world's most significant security threats.

Many national armed forces create and develop cyber troops while cyber operations are included in doctrinal and strategic documents. At the same time, the possibility of responding to cyber-attacks as an armed aggression is now being widely considered. Given the fact that it is almost impossible to accurately identify sources (initiators) of such cyber-attacks, it can lead to an unproved and arbitrary interpretation of the sufficiency of any response military actions.

The number of cybercrimes is steadily increasing. Information systems and resources become both the subject of crimes and the means of their commission. A total dependence of the financial sector and other sectors on the reliability of electronic storage, processing and data exchange systems is growing.

60. However, neither globally nor regionally, has it been possible to effectively prevent the development and dissemination of tools deliberately intended to destroy, block, modify, steal information in networks and resources or neutralize measures to protect it. The development of legal, procedural, technical and organizational measures against cyber interference in information resources remain behind the development of real and potential threats to their implementation.

CHAPTER 16
MAIN DIRECTIONS TO ENSURE INFORMATION INFRASTRUCTURE SAFETY

61. The most probable sources of threats to cybersecurity are considered hardware failures and software malfunction in information and telecommunication systems, unlawful activities of individuals and criminal groups, deliberate actions and mistakes of information systems personnel (as a result of violation of established procedures for information systems operation and information processing rules) and Belarus' dependence on other software and hardware producing countries in the sphere of creating and developing information infrastructure.

62. The Republic of Belarus has a strategic goal of developing a cybersecurity

system based on advanced international risk management approaches and designed to implement long-term measures to reduce them to an acceptable level.

63. The national cybersecurity system should implement a full range of legal, organizational and technical measures to ensure security of the national information infrastructure (including information systems), as well as to secure confidentiality, availability and integrity of information, being able to easily transform and adapt to changing environment by means of constant analysis for compliance with current cybersecurity risks.

64. First of all, it is necessary to ensure cyber-resistance of the national Internet segment, critical objects of informatization and state information systems, as well as effective reaction to cybercrime.

CHAPTER 17
SECURITY OF THE NATIONAL INTERNET SEGMENT

65. The sustainable functioning and controllability of the national Internet segment is a prerequisite for the implementation of citizens' rights in the information sphere, maintaining a high level of information exchange, and providing information services. The cybersecurity of the national Internet segment in the Republic of Belarus is achieved mainly by repulsing the bulk of cyber-attacks on information systems and data transmission networks through blocking malicious communications between subjects and targets.

66. The State maintains and encourages the use of best cybersecurity practices. The most promising task is to create a unified state system for monitoring the national Internet segment while simultaneously creating a cloud platform for providing integrated information security services to public sector and business community in order to automatically register cyber incidents and ensure rapid exchange of information on them between authorized government agencies, telecommunication operators and computer incident response teams (CERT / CSIRT). It is also necessary to create in the future an ecosystem for the development and operation of a national certification authority, whose root certificate will be a proxy for major operating systems and web browsers.

67. At the same time, it is necessary to organize the operation of the IP address reputation service to provide to the Internet service providers a real-time information on the addresses used for cyber-attacks.

68. It is necessary to achieve and maintain a balance between reliable identification of users and registration of their actions on the one hand and creation of conditions for secure collection, processing, provision, storage and dissemination of personal data in the national Internet segment on the other hand, as well as to

promote the development and growth of national cyber risk insurance markets and intrusion testing services.

CHAPTER 18
CYBER-RESISTANCE OF CEOI (CRITICALLY ESSENTIAL OBJECTS OF INFORMATISATION) AND GOVERNMENTAL INFORMATION SYSTEMS

69. Ensuring the security of the information infrastructure is performed by identifying the most significant informatisation objects, the failure of the operation or disruption of which may lead to significant negative consequences for national security in political, economic, social, informational, environmental and other areas.

In order to achieve cyber stability of CEOI, a special complex of legal, organisational and technical measures is implemented in the Republic of Belarus, based on the development of criteria for assigning objects to this category and taking appropriate targeted and comprehensive protective measures in relation to them. This approach allows to create an individual security model for each CEOI, taking into account systematised general security requirements; to effectively identify and assess risks; to maintain high preparedness for preventing and localising the effects of cyber attacks, and also to conduct an external assessment of created security systems.

70. Improving the effectiveness of CEOI's security needs is to be achieved by integrating industry-wide cyber threat monitoring and control systems into the state monitoring system of the national segment of the Internet.

In ensuring cyber resistance of CEOI, Belarus is interested in using international standards and best practices. Regular cyber-exercises and competitions, that involve operating personnel, owners, proprietors and external actors engaged in ensuring cyber security, are of practical importance.

71. The State is interested in protection against risks, challenges, and threats of state information systems. For these purposes, the order of their creation and operation, inclusion in information networks and rules for the exchange of information are determined, and special procedures of state registration are applied.

In the future, the achievement of the required level of protection of e-government services and cyber-stability of state information systems should be provided mainly through their safe design and operation, rather than through adoption of subsequent protective measures, as well as through the introduction of their reasonable unification in the construction and modernisation of these systems.

72. The use of regularly updated, genuine licensed software obtained from

trusted sources is an integral part of ensuring security of CEOI and state information systems.

CHAPTER 19
COUNTERING CYBERCRIME

73. In the Republic of Belarus, a system of prevention, detection, suppression and comprehensive investigation of cybercrimes has been created. The compliance of the norms of the Criminal Code of the Republic of Belarus in this area with the level of social development, world tendencies in legal regulation trends and advanced foreign experience is ensured.

In connection with the emergence of new socially dangerous acts in the information sphere, criminal and other liability is established for their commission. The continuous improvement of forms and methods of preventing, identifying, suppressing and investigating cybercrime is ensured, the timeliness and quality of the operational-investigative activities is increased.

74. Belarus is interested in the convergence and unification of approaches to countering cybercrime at the international level, the development of common standards in law enforcement, international exchange of experience and practical interaction. Regional and international cooperation in the field of cybersecurity, tracking the activities of criminal groups and individual criminals operating in cyberspace.

75. The increase in trust between law enforcement agencies, public and private sector organizations, educational and scientific institutions, combining their efforts in the prevention, detection, suppression and investigation of cybercrime is important in countering cybercrime. One of the effective measures to prevent and avert cybercrime is to reduce the motivation to commit them by eliminating the conditions for the creation of illegal schemes.

76. In addition, one of the priorities for the authorised governmental authorities is prevention of cybercrime, based on popularisation among the population, especially among young people, of intolerance to antisocial behavior in the information space, conducting explanatory work in the media and the Internet in order to create a safe national information ecosystem . To increase legal awareness and reduce vulnerability to cyber attacks, citizens are trained in the basics of behavior in the information sphere.

SECTION VI
ENSURING SECURITY OF INFORMATION RESOURCES

CHAPTER 20
DEPENDANCE OF SECURITY MEASURES OF ENSURING THE SAFETY OF INFORMATION RESOURCES

77. The emerging of wide and accessible possibilities for collecting, storing and processing large amounts of data, creation of technologies for direct access to information, makes necessary to consider it as an independent and valuable resource. Information resources are becoming a priority object of crimes and cyber-incidents, are subject to theft, modification, destruction, blocking and other interactions.

78. The importance of technical protection of information of limited distribution is increasing, while means of abduction, illegal blocking and other impact on information resources are universally used for political, military, intelligence, economic, criminal and other purposes.

Multiple threats and risks of illegal and unjustified interference with the privacy of citizens, theft of personal data, compromising of access details and excessive profiling narrow a person's personal space and violate his privacy. Disclosure of personal information has become an integral attribute of acquisitive crimes and crimes against the person.

An illegal database market is being formed, the demand for which stands behind efforts to steal information files, accompanied by violations of copyrights.

CHAPTER 21
MAIN PRIORITIES IN SECURING INFORMATION RESOURCES

79. The main sources posing threats to the securing of information resources in the Republic of Belarus should be considered individuals, criminal groups, unfair national or foreign organizations, entities and communities that seek to gain unlawful access to these resources for political, military, commercial and personal ends, which is obtained by means of bypassing an established order in breach of conventional norms of morality and ethics, as well as in violation of the functioning information infrastructure.

80. The main state policy objective in securing information resources is to ensure their accessibility, integrity and confidentiality.

81. The system for securing information resources is predicated on the strategic principle of striking a balance between freedom of information and the

right to secrecy, state guarantees for the dissemination and provision of publicly available information. The state provides for the expansion of safe access to information resources for bona fide users, for the development of qualitative and convenient information provision services, for the refinement of its data systems.

82. It is necessary at this stage to ensure credible and comprehensive protection of restricted information, security of personal data and of state information resources.

CHAPTER 22
PROTECTION OF STATE AND OFFICIAL SECRECY

83. Data regarded as state and official secrecy is protected in accordance with national legislation on state secrets. Legal prohibitions restrict the circulation of information that contains information regarded as state secrets, and the obtaining of secret information by individuals. Storage and processing of information in publicly available forms, including in information systems with access to the Internet and other open computer networks is prohibited. Responsibility is introduced for the violation of legal prohibitions and prescriptions in the field of state secrets.

84. Along with this, the classification of information as state secrets is the exclusive right of a strictly defined list of state organs and organizations and is realized on the basis of harm (damage) assessment arising from the disclosure, theft or loss of such information. Organizational, material and other expenses for securing this information cannot exceed the amount of the above harm (damage), while conclusions on the scale and size of which are reached on the basis of concrete figures (indicators) or accepted practices.

The state, proceeding from the assumption of the free dissemination of information, and with the view of enhancing the openness of socio-economic and other public relations has an interest in phasing out the number of state organs and organizations empowered to classify information as secret while simultaneously guaranteeing effective protection for secret information. Expansion and tightening of regime measures, not arising from systemic shortcomings in the protection of state secrets that resulted in harmful consequences is not allowed.

85. There is the need to adjust the institution of secrecy to the development of informatization. Along with organizational and legal measures to secure information the role for efforts to protect it by technical methods is increasing. In the area of technical and cryptographic methods for protecting state secrets the utmost consideration is given to available information on means, methods, technologies for obtaining unsanctioned access to protected information resources, to the results of operational search and counter espionage activities, to scientific

research and experimental designs, as well as to comprehensive knowledge of modern ICTs and specific situations in the field of national security.

State bodies empowered to determine the sequence whereby state secrets are protected from being leaked through technical channels ensure that it is adequate and proportionate to possible risks.

CHAPTER 23
SECURITY OF INFORMATION OF RESTRICTED CIRCULATION AND PROTECTION OF PERSONAL DATA

86. In accordance with normative legal acts of the Republic of Belarus official information of restricted circulation is compiled and protected, while under protection falls information that constitutes commercial, professional, banking or any other lawfully secured secret, information pertaining to a private life of an individual, personal data, other information, access to which is restricted by the legislative acts of the Republic of Belarus.

87. If it is impossible and infeasible to separate fully information systems and resources containing these data from the Internet and other publicly available networks for individuals and legal entities, it is, then, necessary to undertake adequate legal, organizational, administrative and technical measures that bring to the minimum the number of cyber incidents and the resulting harm for the systems.

88. The state, on its part, should improve information security requirements, including by continuing to develop systems that confirm compliance of technical and cryptographic information protection means, as well as the licensing of activities in the field of technical protection of information.

89. Protection of personal data is attained and safeguarded by balanced state policy that determines requirements for various subjects of information relations involved in the collection, processing and storage of this data.

The state focuses its attention on refining the relevant normative legal basis. The state regulates the collection, processing, storage, provision and dissemination of personal data with due regard to advanced international experience, and in compliance with the provisions of interstate acts. Personal data protection approaches that emerge in Belarus are predicated on the principle of “security by default”.

90. An important measure for strengthened control in this field is the work of a state-empowered subject (subjects) that protects the rights of individuals in the processing of their personal data.

CHAPTER 24
SECURING STATE INFORMATION RESOURCES AND PUBLICLY AVAILABLE INFORMATION

91. The state provides protection to information resources, which are at the disposal of state organs and organizations, it provides legal regulation for the use, possession and disposal of information resources. To this end, a single system for the accounting and storage of information is created, and special procedures for state registration are applied.

92. State organs protect publicly available information from unlawful destruction, modification, legitimate access blocking, unjustified secrecy, concealment, untimely distribution or provision. The state prohibits censorship, provides guarantees for timely provision of publicly available information by means established by law, expands the scope for appropriate services, implements the "open data" concept. The state is interested in maintaining the balance between citizens' requirements for publicly available information, their right to receive such information, and the need to protect it from illegal encroachment.

SECTION VII
MECHANISMS FOR THE CONCEPT IMPLEMENTATION

CHAPTER 25
USE OF CONCEPT PROVISIONS FOR PREPARATION OF NORMATIVE LEGAL ACTS AND OTHER DOCUMENTS

93. The Concept provisions are used in the drafting of normative legal acts, state programmes, future and current work plans of state organs, in the implementation of projects by relevant public organizations and citizen initiatives, as well as in appraising the state of national security and in clarifying its indicators.

94. Development and implementation of measures aimed at strengthening information security, consistent with the Concept, are predicated on scientific support, including on basic and applied research, as well as on the results of practical work.

95. In the field of legal support for information security the Concept serves as the basis for special legislative acts that determine the legal status of subjects that provide for information security, regulate relevant activities of state organs, formulate norms and rules for legitimate conduct in the information sphere, necessary regulations, restrictions and prohibitions that attach other norms in order to protect the information sphere and the interests of an individual, society and state.

CHAPTER 26
PUBLIC-PRIVATE PARTNERSHIP IN THE SPEHERE OF INFORMATION SECURITY

96. Efforts at effectively addressing the goals related to information security are to be facilitated through targeted collaboration between the public sector and commercial organizations in the form of public-private partnerships with the view to attracting competence, human resources, technology, private companies' capital, increasing the impact from the use of budgetary funds and enterprises' assets, jointly developing and implementing investment and other projects on information security.

97. Public-private partnership on information security is regarded as legally registered cooperation between a state organ and a business entity of non-state ownership based on resource pooling and risk sharing and implemented for the purpose of ensuring information security with the assistance of private investment and competence.

98. An important area for implementing public-private partnership related to information security is support provided to national information systems and information security systems software manufacturers.

Alongside efforts to overcome Belarus' dependence on other software and hardware manufacturers the implementation of infrastructure projects and projects directly related to ensuring information security through the mechanism of partnership between the state and national private companies should facilitate an emerging market demand for import-substituting information technology products and their higher quality.

99. The state has an interest, in cooperation with IT-companies, Internet providers, telecom operators and external experts in renewing and developing mechanisms for the identification of threats, by means of IT-audit, posed to information security, monitoring of cyber-risks, search for vulnerabilities and urgent tools for protection, development of rules of conduct in the Internet.

100. Public-private partnership contributes to the training of personnel skilled in the provision of information security, development of necessary training programs for relevant specialists, implementation of new educational and professional standards in the field, as well as to enhancing overall public computer literacy, including training in computer skills, rules for the use of personal data, ability to working safely in the Internet provided to old and middle-aged people.

101. Given the ongoing transformation of public relations in the information field, public-private partnership is becoming a most effective blueprint in the provision of information security. In its context, the state determines the objectives,

strategic tasks and regulative approaches, whereas the business community provides technology, expertise and resources to this end. With this in mind, the state is keen to provide guarantees for technological neutrality and protection for private organizations (and their investment) from possible risks.

CHAPTER 27
PARTICIPATION OF THE REPUBLIC OF BELARUS IN PROVISION OF INTERNATIONAL INFORMATION SECURITY

102. The purpose of ensuring international information security is to identify, prevent and eliminate external risks, challenges and threats posed to information security. International cooperation in the field of information security at the regional, bilateral, multilateral and global levels aims to reduce the risks arising from the use of information and communications technologies that are aligned to hostile acts and acts of aggression against Belarus.

103. With the view to ensuring international information security vigorous, comprehensive, mutually beneficial international, including interagency, cooperation is required and realized.

The Republic of Belarus takes part in the activities of international organizations, relevant international treaties, bilateral relationships with other states, other forms of interstate cooperation aimed at developing mechanisms for international cooperation to combat the threats posed to international information security.

104. The key tool for achieving the goals of ensuring international information security is support and advancement of relevant initiatives that meet the interests of the Republic of Belarus in the information field.

Belarus supports the promotion of confidence building measures in the field of international information security and stands for responsible conduct of governments in the information field that would serve, first and foremost, the purpose of preventing, rather than resolving, conflicts therein. States should refrain from targeted destructive information impacts on other countries, prevent the use of their territory for initiating cyber-attacks, as well as combat the use of hidden malicious functions and software vulnerabilities in software and hardware, while ensuring their safety for users.

105. The Republic of Belarus takes part in international information exchange on the basis of international treaties and agreements, while working within its jurisdiction to provide for its security.