

Pursuant to Article 38 paragraph 1 of the Law on Planning System of the Republic of Serbia (*Official Gazette of the Republic of Serbia* No. 30/18),

the Government passes this

INFORMATION SOCIETY AND INFORMATION SECURITY DEVELOPMENT STRATEGY OF THE REPUBLIC OF SERBIA FOR THE PERIOD 2021-2026

INTRODUCTION

The Information Society and Information Security Development Strategy for the Period 2021–2026 (hereinafter referred to as the “Strategy”) is a cross-sectoral strategy setting out the objectives of and measures for the development of information society and information security.

With regard to information security, the Strategy is harmonised with the Network and Information Security Directive (NIS Directive), which provides for the adoption of a national Information Security Strategy setting out the strategic objectives and priorities with regard to network and information security.

The importance of information society development was recognised in the Republic of Serbia more than a decade ago, when the first Information Society Development Strategy of the Republic of Serbia by 2020 was passed (*Official Gazette of the Republic of Serbia* No. 5/10, hereinafter referred to as the “Information Society Development Strategy”), which covered all priority areas contributing to the development of information society, including: electronic communications, e-government, e-health and e-justice, ICT in education, science and culture, e-commerce, the ICT business sector, information security.

Information security, which was addressed as a topic in the Information Society Development Strategy, has gained prominence in recent years, as the use of new technologies gave rise and continues to contribute to the ensuing risks. Accordingly, in 2017 the Government adopted the Information Security Development Strategy for the period 2017-2020 (*Official Gazette of the Republic of Serbia* No. 53/17, hereinafter referred to as the “Information Security Development Strategy”), which set forth the principles of information security, the priority areas and the strategic objectives with regard to the safety of citizens, the economy and the state.

As these Strategies expired in 2020, the development of the next Draft of the Strategy for the period 2021-2026 commenced pursuant to an initiative of the Ministry of Trade, Tourism and Telecommunications. The new Strategy was intended to address both information society and information security, with a view to ensuring continuity in their development and adapting to the new circumstances stemming from rapid digitalisation and development of new technologies across all segments of the society.

Members of the following institutions took part in the development of the Strategy: the Ministry of Trade, Tourism and Telecommunications, the Ministry of Education, Science and Technological Development, the Ministry of Culture and Media, the Ministry of Health, the Ministry of Agriculture, Forestry and Water Management, the Ministry of Construction, Transport and Infrastructure, the Ministry of Justice, the Ministry of Economy, the Ministry of Foreign

Affairs, the Ministry of the Interior, the Ministry of Public Administration and Local Self-Government, the IT and e-Government Office and the Public Policy Secretariat.

PLANNING DOCUMENTS AND LEGAL FRAMEWORK RELEVANT FOR THE STRATEGY

In accordance with Article 12 of the Law on Planning System, the Strategy is cross-sectoral in its scope, informed by the relevant planning and strategic documents in the fields of next generation network development, digital skills, artificial intelligence, industrial policy development, smart specialisations, tourism, culture, agriculture, the judiciary, cybercrime, as well as regulations in the fields of electronic documents, electronic identification and trust services, information security and e-government and online safety for children.

Strategy for the Development of Next Generation Networks by 2023 (*Official Gazette of the Republic of Serbia No. 33/18*), which sets out as Serbia's primary goal the dynamic economic, technology, manufacturing and overall development of the society, capable of integrating with the EU's single market, and states that Serbia's sustainable growth and macroeconomic stability will be unsustainable without stable industrial growth, development of modern technologies, effective management and competitiveness of manufactured goods in foreign markets, all of which would contribute to a stable balance of payments.

The Strategy of Digital Skills Development in the Republic of Serbia for the Period 2020-2024 (*Official Gazette of the Republic of Serbia No. 21/20*), which seeks to improve digital knowledge and digital skills of all citizens, including members of vulnerable groups, to ensure the country keeps abreast of ICT developments across all areas and meets the demands of businesses and the labour market.

The Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the Period 2020–2025 (*Official Gazette of the Republic of Serbia No. 96/19*), which envisages the development of artificial intelligence which, when implemented, should result in economic growth, improved public services, more advanced human resources in science and development of skills for jobs of the future.

The Industrial Policy Strategy from 2021 to 2030 (*Official Gazette of the Republic of Serbia No. 35/20*), which sets out a set of objectives and measures pertaining to structure of the industry, with the aim of promoting overall economic growth.

The Smart Specialisation Strategy of the Republic of Serbia for the period 2020-2027 (*Official Gazette of the Republic of Serbia No. 21/20*) is part of a new innovation policy aimed at boosting competitiveness of businesses, ensuring economic growth and ensuring social progress through pooling of research, industry and innovation powers and resources and directing them to a limited number of prioritised economic areas.

The Tourism Development Strategy of the Republic of Serbia for the Period 2016-2025 (*Official Gazette of the Republic of Serbia No. 98/16*) sets out the business mission, vision and objectives of tourism development, identifies prioritised tourism products, proposes prioritised tourist destination and contains an analysis of impact on cultural heritage and natural resources and a draft tourism development policy.

The Cybercrime Strategy for the Period 2019–2023 (*Official Gazette of the Republic of Serbia No. 71/18*), which provides for the fight against cybercrime.

National Security Strategy of the Republic of Serbia (*Official Gazette of the Republic of Serbia No. 94/19*), which aims to protect national values and interests of the Republic of Serbia from challenges, risks and security threats across all areas of social life.

The Defence Strategy of the Republic of Serbia (*Official Gazette of the Republic of Serbia No. 94/19*), which aims to direct the development of normative, doctrinarian and organisational solutions in the defence system, defence planning and funding and deployment of the defence resources of the Republic of Serbia.

The Agriculture and Rural Development Strategy of the Republic of Serbia for the period 2014-2024 (*Official Gazette of the Republic of Serbia No. 84/14*)

The Judicial Development Strategy for the Period 2020–2025 (*Official Gazette of the Republic of Serbia No. 101/20*) governs the process of modernising the judiciary and better adapting it to the needs of the state and the society and provides for the development of e-judiciary and further improvement of e-services within the judiciary.

The Strategy for the Development of the Public Information System in the Republic of Serbia for the Period 2020-2025 (*Official Gazette of the Republic of Serbia No. 30/18*), which sets out *inter alia* measures aimed at affording a satisfactory level of information security to journalists and the media, as well as measures designed to improve human resource, organisational and technical capacities of government authorities to ensure future recognition and addressing of security threats in an online environment, including gender-specific threats, as well as activities designed to educate judges, public prosecutors, attorneys and relevant ministries on different forms of threats to the information security of journalists and the media, including gender/specific risks/threats.

The e-Government Development Programme of the Republic of Serbia for the period 2020-2022 and the Action Plan (*Official Gazette of the Republic of Serbia No. 85/20*) for its implementation, which aims to develop an efficient and user-oriented government in a digital environment.

The Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions (*Official Gazette of the Republic of Serbia No. 94/17*), which governs electronic documents, electronic identification and trust services, with the aim of contributing to improved electronic transactions, in particular with regard to electronic communication between government authorities, businesses and citizens.

The Law on Information Security (*Official Gazette of the Republic of Serbia No. 6/16, 94/17 and 77/19*), which governs security measures employed against security risks in information and communication system and the responsibilities of legal entities when managing and using information and communication systems and designates the competent authorities responsible for implementing the security measures, coordinating the stakeholders in the security sphere and monitoring proper implementation of the security measures.

The Law on e-Government (*Official Gazette of the Republic of Serbia No. 27/18*), which governs the performance of public administration duties using information and communication technologies. The Law sets out the necessary preconditions for public administration to be able to shift from a classic form of government to e-government. The Law provides for the following: the integrated e-government information and communication network, the public administration

gateway, the use of data contained in registers and records in an electronic form, the establishment and maintenance of the Metaregister, the e-mail accounts of authorised officers, the single electronic inbox and the e-Government Portal. Implementation of this Law will enable the development of e-government and e-services provided by public administration to citizens.

Law on Personal Data Protection (Official Gazette of RS, No. 87/18) which regulates the right to protection of persons in connection with the processing of personal data. As information security is a set of measures that enable data handled through information and communication systems to be protected from unauthorized access, it is inseparable from the right to protection of personal data, which represent a large part of data stored within the ICT system.

Decree on Safety and Protection of Children when Using Information and Communication Technologies (Official Gazette of the Republic of Serbia No. 13/20), which aims to raise awareness and knowledge of the advantages and risks of using the Internet and ways of using the Internet safely, to improve digital literacy of children/pupils, parents and teachers and to enhance cross-departmental cooperation in the field of online safety and protection of children.

During the development of this Draft of the Strategy, we also took into consideration the activities set out in the Draft Culture Development Strategy of the Republic of Serbia 2020-2029.

Content of the Strategy

The Strategy contains the following areas:

1) Background

- 1.1 Implementation of the Information Society Development Strategy
- 1.2 Implementation of the Information Security Development Strategy
- 1.3. Use of information and communication technologies in Republic of Serbia
 - o 1.3.1 Computer use
 - o 1.3.2 Internet use
 - o 1.3.3. Broadband internet connection – households, companies
 - o 1.3.4. Website ownership, use of cloud services, mobile phones and mobile internet for business purposes
 - o 1.3.5. Online commerce
 - o 1.3.6 e-skills
- 1.4 e-Government
 - o 1.4.1 e-justice, e-education, e-health and e-culture
 - o 1.4.2 e-transactions, e-commerce and e-tourism
 - o 1.4.3 e-construction, e-agriculture
 - o 1.4.4. e-mining and e-energy
- 1.5. ICT sector
- 1.6 Information security
 - o 1.6.1 Information security of citizens
 - o 1.6.2 Information security of businesses
 - o 1.6.3 Information security of ICT of special importance

2) Change achieved by the Strategy

- 2.1 Vision and desired change

- 3) Objectives of the Strategy
 - 3.1 Overarching objective of the Strategy
 - 3.2 Specific objectives and measures of the Strategy
- 4) Strategy implementation mechanism and results reporting arrangements
- 5) Stakeholder consultations held
- 6) Estimate of financial resources required for implementation of the Strategy and analysis of its financial effects
- 7) Action Plan on Implementation of the Information Society and Information Security Development Strategy in the Republic of Serbia for the period 2021-2026
- 8) Final section
- 9) Table of the Action Plan on Implementation of the Information Society and Information Security Development Strategy in the Republic of Serbia for the period 2021-2023

1. BACKGROUND

The background section deals primarily with the implementation of the Strategies previously implemented in the fields of information society and information security, as well as the state of play in these fields, specifically:

- The use of information and communication technologies in the Republic of Serbia;
- Public administration (e-government);
- The ICT sector, and
- Information security.

This background section draws on the following sources:

- Publication of the Statistical Office of the Republic of Serbia *Usage of Information and Communication Technologies in Serbia, 2020*;¹
- Publication of the Statistical Office of the Republic of Serbia *Usage of Information and Communication Technologies in Serbia, 2019*;²
- Cybersecurity Capacity Review Serbia by the World Bank and the Global Centre for Capacity Building, based on the Cybersecurity Maturity Model (CMM) Assessment;
- A questionnaire of the Ministry of Trade, Tourism and Telecommunications sent to all ministries, which included questions concerning electronic communications, e-services, application of the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions and projects in the field of digitalisation.
- E-Bulletin, Chamber of Commerce and Industry of Serbia, Electronic Communications and Information Society Association.
- *Development of the Information Technology Industry*, August 2019; Milovan Matijević, Mineco Computers.

¹ Upotreba informaciono-komunikacionih tehnologija u Srbiji, 2020, Republički zavod za statistiku <https://publikacije.stat.gov.rs/G2020/Pdf/G202016015.pdf>

² Upotreba informaciono-komunikacionih tehnologija u Srbiji, 2019, Republički zavod za statistiku <https://publikacije.stat.gov.rs/G2019/Pdf/G201916014.pdf>

- UNOPS project “Assessment of the cyber security ecosystem in the Republic of Serbia”

1.1 IMPLEMENTATION OF THE INFORMATION SOCIETY DEVELOPMENT STRATEGY

The Information Society Development Strategy adopted in 2010 aimed at developing an information society focused on harnessing the potential of information and communication technologies (hereinafter referred to as “ICT”) for increased work efficiency, economic growth, higher employment and improved quality of life for all citizens of the Republic of Serbia. It identified the following as the drivers of information society development:

- Open, universally accessible and high-quality Internet access;
- Developed e-transactions, including: e-government, e-commerce, e-justice, e-health and e-education.

In addition to the Ministry of Trade, Tourism and Telecommunications, implementing bodies for that Strategy were: the Ministry of Education, Science and Technological Development, the Ministry of Public Administration and Local Self-Government, the Ministry of Justice, the Ministry of Culture and Media, the Ministry of Education, Science and Technological Development, the Ministry of Health, the Ministry of the Interior, the IT and e-Government Office, the National Bank of Serbia, the Academic Network of the Republic of Serbia and Chamber of Commerce and Industry of Serbia.

Implementation of the Information Society Development Strategy through the Action Plan for the period 2018-2019 achieved the following results:

- 1) The area of e-government, e-health and e-justice:
 - Laws and secondary legislation adopted in the field of e-Government and electronic documents, electronic identification and trust services;
 - Improved functionalities, services and service gateway of the e-Government Portal;
 - Improved Health Information System;
 - A system for electronic data exchange in the judiciary and between the judiciary and other government authorities.
- 2) ICT in education, science and culture:
 - Improved ICT infrastructure in primary and secondary schools;
 - Improved ICT competences of teachers and employees in public administration;
 - Raised awareness of children, parents and teachers in the field of online safety for children;
 - Improved digital services in the field of culture;
 - Improved e-Education services;
 - Introduction of information technology and computer science in primary schools.
- 3) e-commerce:
 - Legislation in the field of e-commerce adopted;
 - A public list of qualified trust services formed and published;
 - Instant payment system – IPS NBS system.

An analysis of the implemented Action Plan seems to indicate that progress has been made in these three key areas, primarily with regard to e-government. Prerequisites have been established for future development of this field through the passing of relevant legislation, including the Law on e-Government and the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions, together with the accompanying secondary legislation. These laws introduce legal concepts which will facilitate future development of e-government and e-transactions.

Furthermore, in the field of health care and the judiciary, information systems have been developed to expedite the work processes, facilitate data exchange and cut red tape expenses.

A major achievement is the improvement of ICT infrastructure in the field of education, specifically in primary and secondary schools, as well as in the fields of science and culture, as a precondition for modernisation of education processes through the employment of new technologies which will drive the development of digital services.

In the field of e-commerce, normative obstacles to the development of e-commerce have been eliminated through legislative amendments, followed by activities to raise awareness, educate on and promote e-commerce to ensure its further progress.

While improvements in the field of information society have been notable, future efforts in this field will have to be stepped up, especially with regard to further improvement of infrastructure, development of electronic services and raising citizens' awareness and digital skill levels.

1.2 IMPLEMENTATION OF THE INFORMATION SECURITY DEVELOPMENT STRATEGY

The Information Security Development Strategy adopted in 2017 aimed to develop and improve information security in the Republic of Serbia and maintain an appropriate level of standards in this field through increased security of information and communication systems, fight against cybercrime and improvement of information security of national importance.

Implementation of the Information Security Development Strategy through the relevant Action Plan for 2018-2019 achieved the following results:

- 1) Area – safety of information and communication systems
 - A data exchange system for incident reporting and response established;
 - Information security staff recruited and trained;
 - Awareness-raising campaign on risks and incident response implemented;
 - Annual analysis of the National CERT on cyberspace threats in the Republic of Serbia conducted.
- 2) Area – safety of citizens when using technology
 - Activities of the National Contact Centre for Online Safety for Children conducted, annual IT Caravan campaigns, ICT Girls' Day, Digital Class and other similar activities implemented
 - The Law on Personal Data Protection passed;
- 3) Area – fight against cybercrime:
 - Judges and public prosecutors trained on acting in cybercrime cases

4) Area - information security of the Republic of Serbia:

- Information security system relevant for national security defined;
- CERTs for independent ICT system operators established.

The development of information security gained momentum with the passing of the Law on Information Security, which introduced, first and foremost, the main institutional prerequisites for the development of this field, as well as other prerequisites for a country to establish sound information security arrangements.

A key achievement of Action Plan implementation is certainly the establishment of an incident reporting and response data exchange system, as a mechanism to monitor the state of play in this field.

As awareness raising and improved knowledge of information security, coupled with capacity building of the relevant staff, were identified as paramount, numerous activities have taken place (including seminars, conferences, trainings and panels) to raise awareness of incident risks and incident responses.

Major progress has been achieved with regard to information security of children through the operation of the National Contact Centre for Online Safety for Children.

Implementation of activities under the Action Plan marked the beginning of efforts to build the capacities of ICT systems of special importance, although it should be noted that there is much room for improvement in this regard, which will require investment in infrastructure, staff capacity building and improving the level of knowledge in this field.

Based on the implementation of these Strategies in recent years, the activities and measures foreseen therein have been identified as appropriate and it is therefore recommended that the current Strategy build on them and continue with the same efforts towards achieving the stated objectives.

1.3 USAGE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE REPUBLIC OF SERBIA

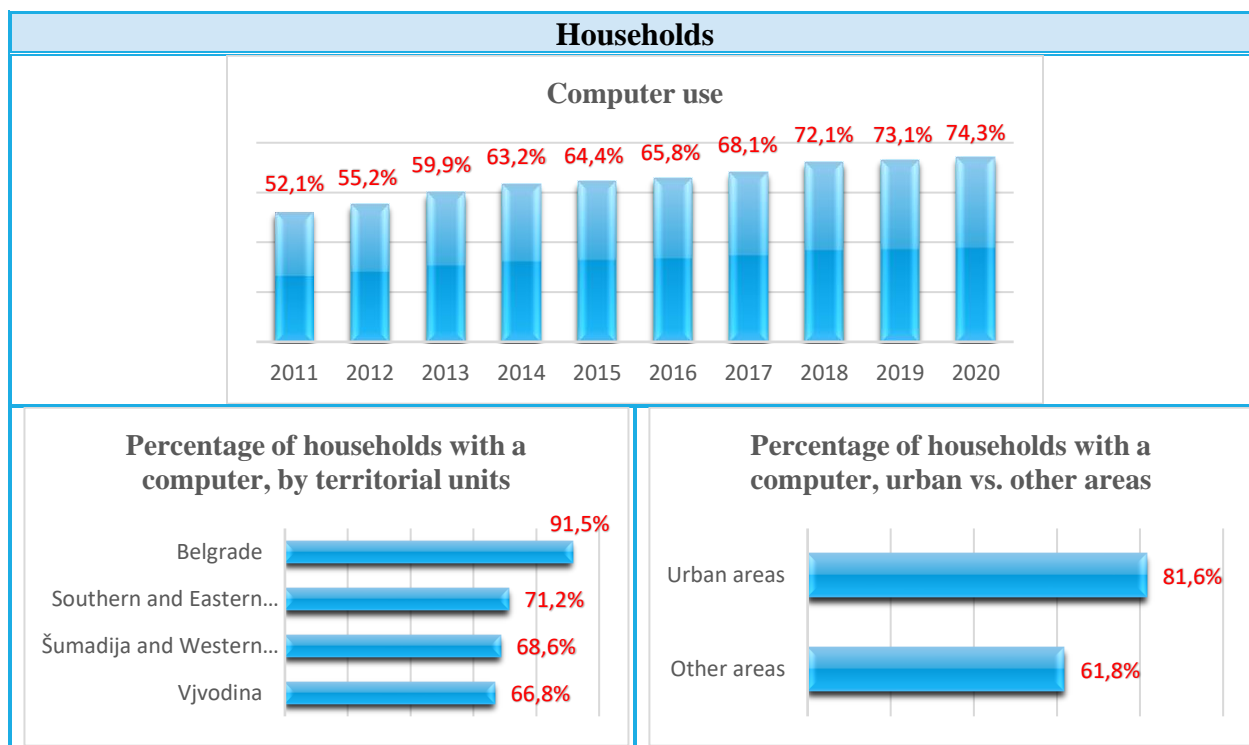
Details of the use of ICT in the Republic of Serbia, as the fundamental indicators of information society development, are provided in the publication of the Statistical Office of the Republic of Serbia entitled *Usage of Information and Communication Technologies in Serbia, 2020*.

1.3.1 Computer Use

Computer use by households – Based on the main findings of this survey, 74.3% of households in the Republic of Serbia own a computer, which is an increase of 1.2% relative to 2019 and 2.2% relative to 2018. The share of households with computers varies between territorial units: in Belgrade it is 91.5%, in Vojvodina 66.8%, in Šumadija and Western Serbia 68.6% and in Southern and Eastern Serbia 71.2%.

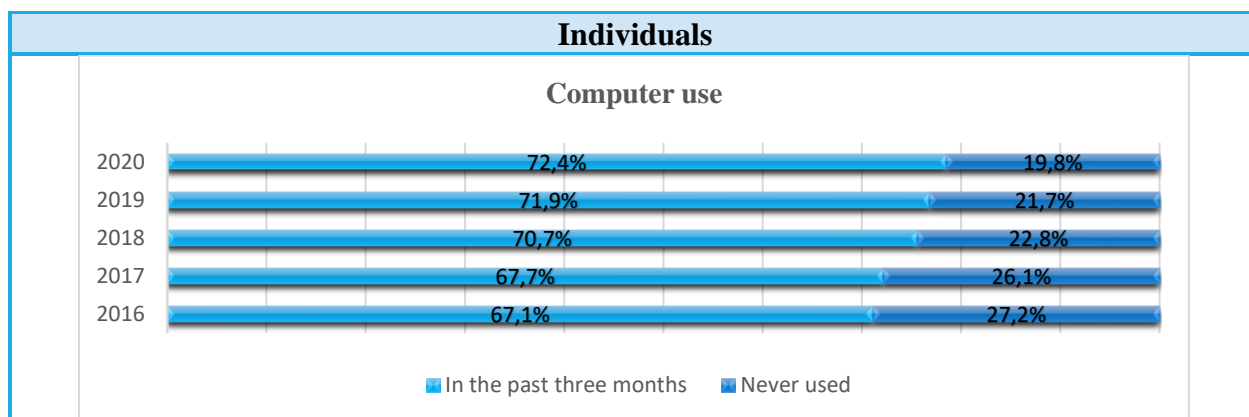
Differences in terms of households with computers are also noticeable between urban and other areas of Serbia: 81.6% vs. 61.8%. Relative to 2019, this gap has seen a mild increase.

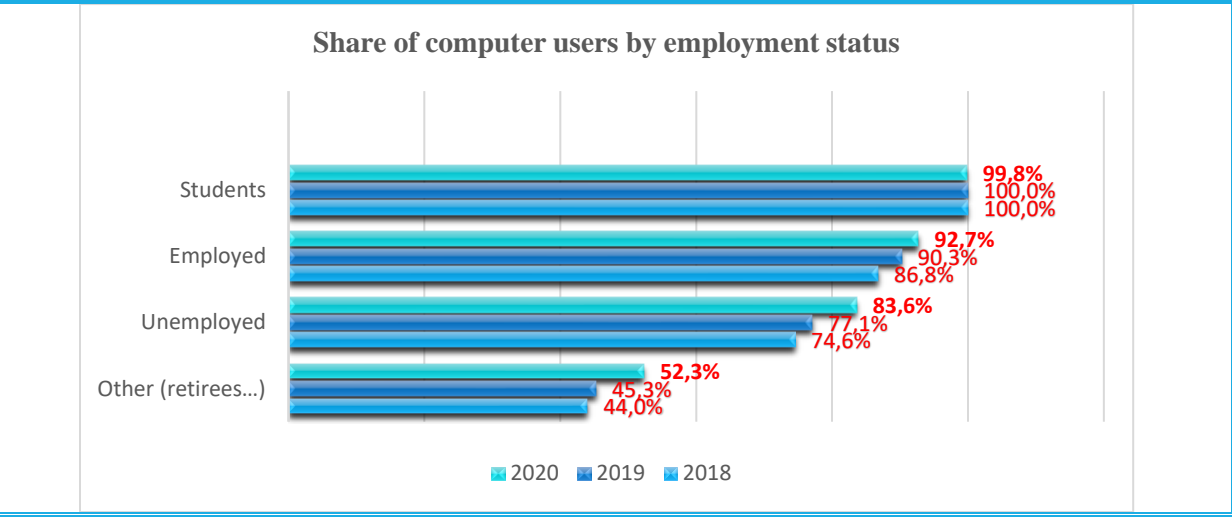
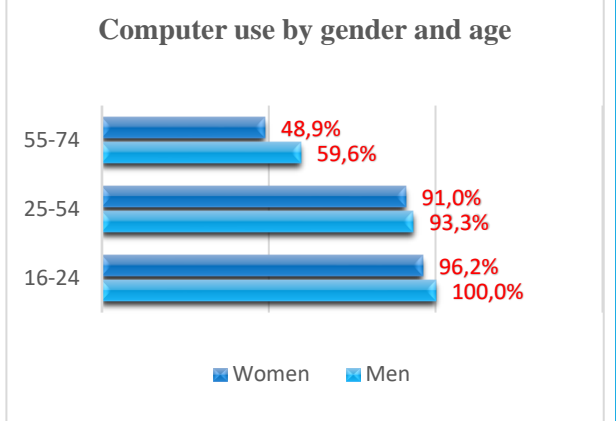
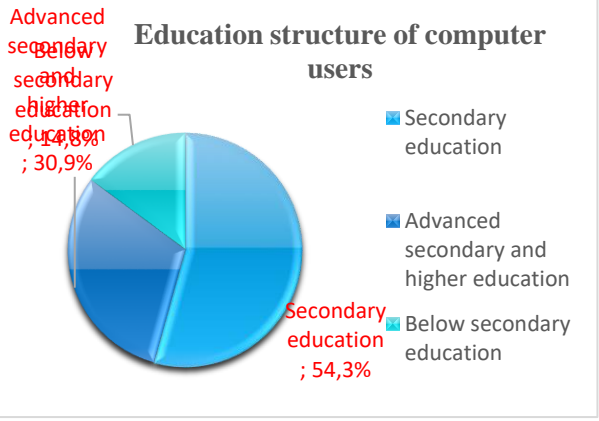
This is supported by the rates of increase in computer availability in urban and other areas of Serbia. In urban areas, the rate of increase is 2.1%, while other parts of Serbia have seen a decline relative to 2019 by 0.3%.

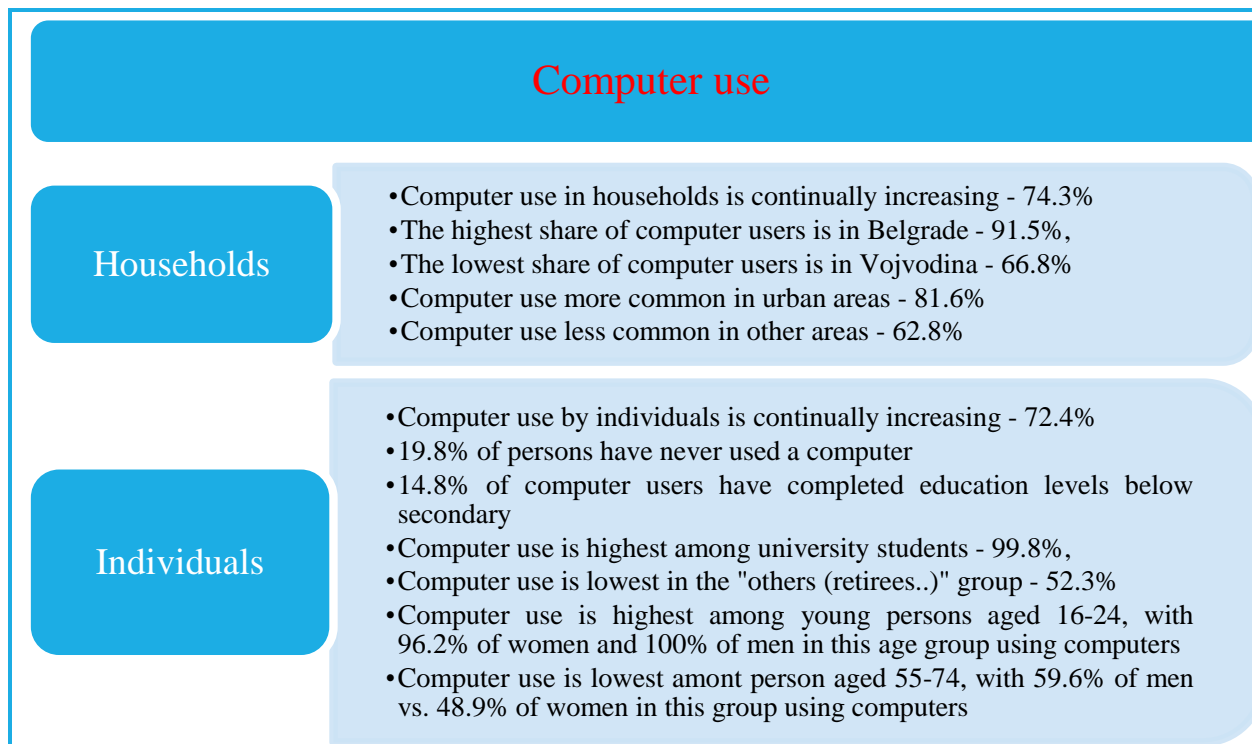


Computer use by individuals – In the Republic of Serbia, 72.4% of persons used a computer in the past three months, 1.5% of persons last used a computer more than three months ago, while 6.4% of persons last used a computer more than a year ago. As many as 19.8% of persons have never used a computer. The number of computer users has increased by 2%, 3.1% and 6.4% relative to 2019, 2018 and 2017 respectively.

Among computer users, 54.3% have completed secondary education, 14.8% have completed education levels below secondary, while 30.9% have completed advanced secondary and higher education.







1.3.2 Internet Use

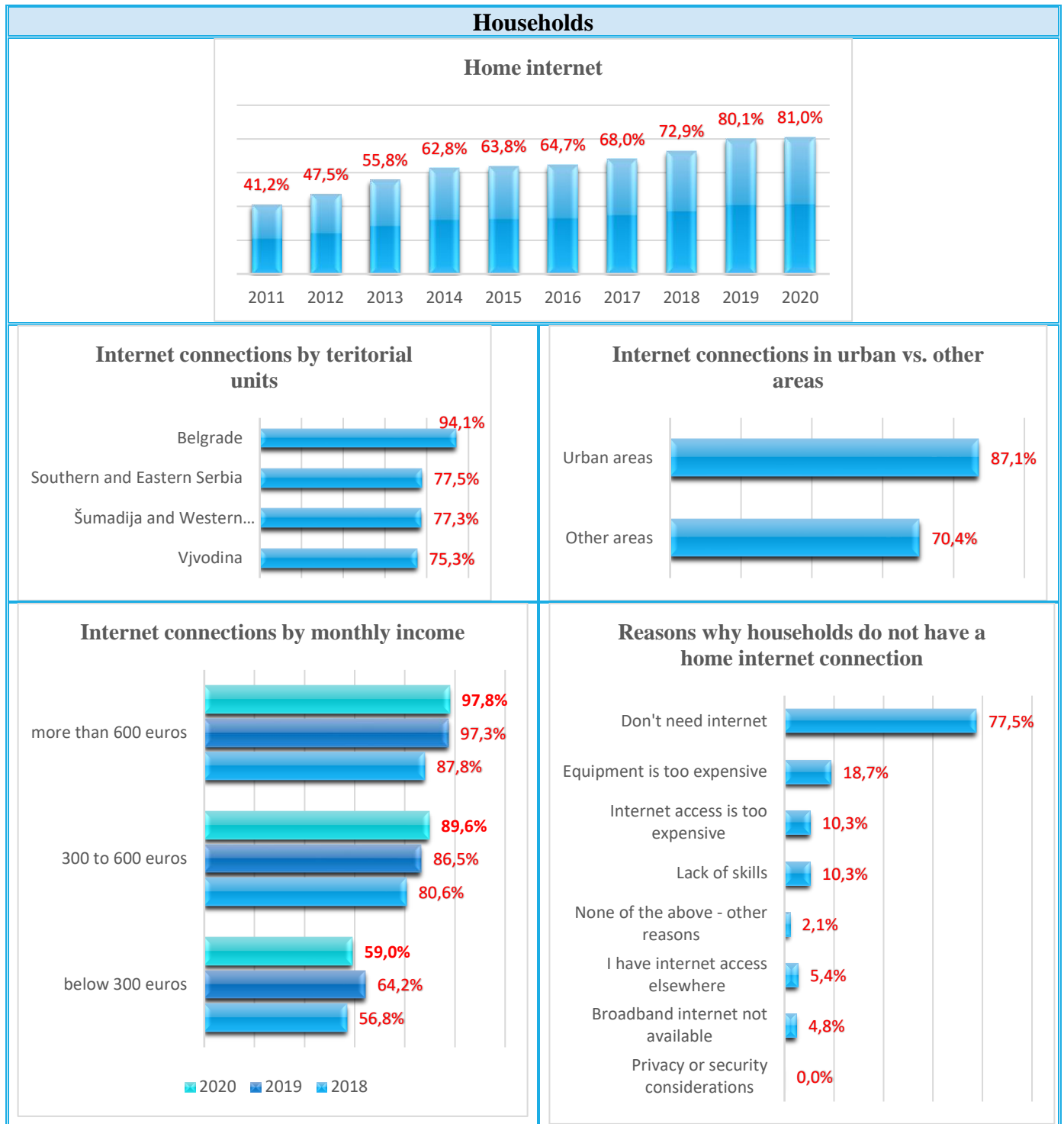
Internet use in households – In the Republic of Serbia, 81% of households have an internet connection, which is an increase of 0.9% and 8.1% relative to 2019 and 2018 respectively.

The share of households with an internet connection is highest in Belgrade, at 94.1%. In Vojvodina it is 75.3%, in Šumadija and Western Serbia 77.5% and in Southern and Eastern Serbia 77.3%.

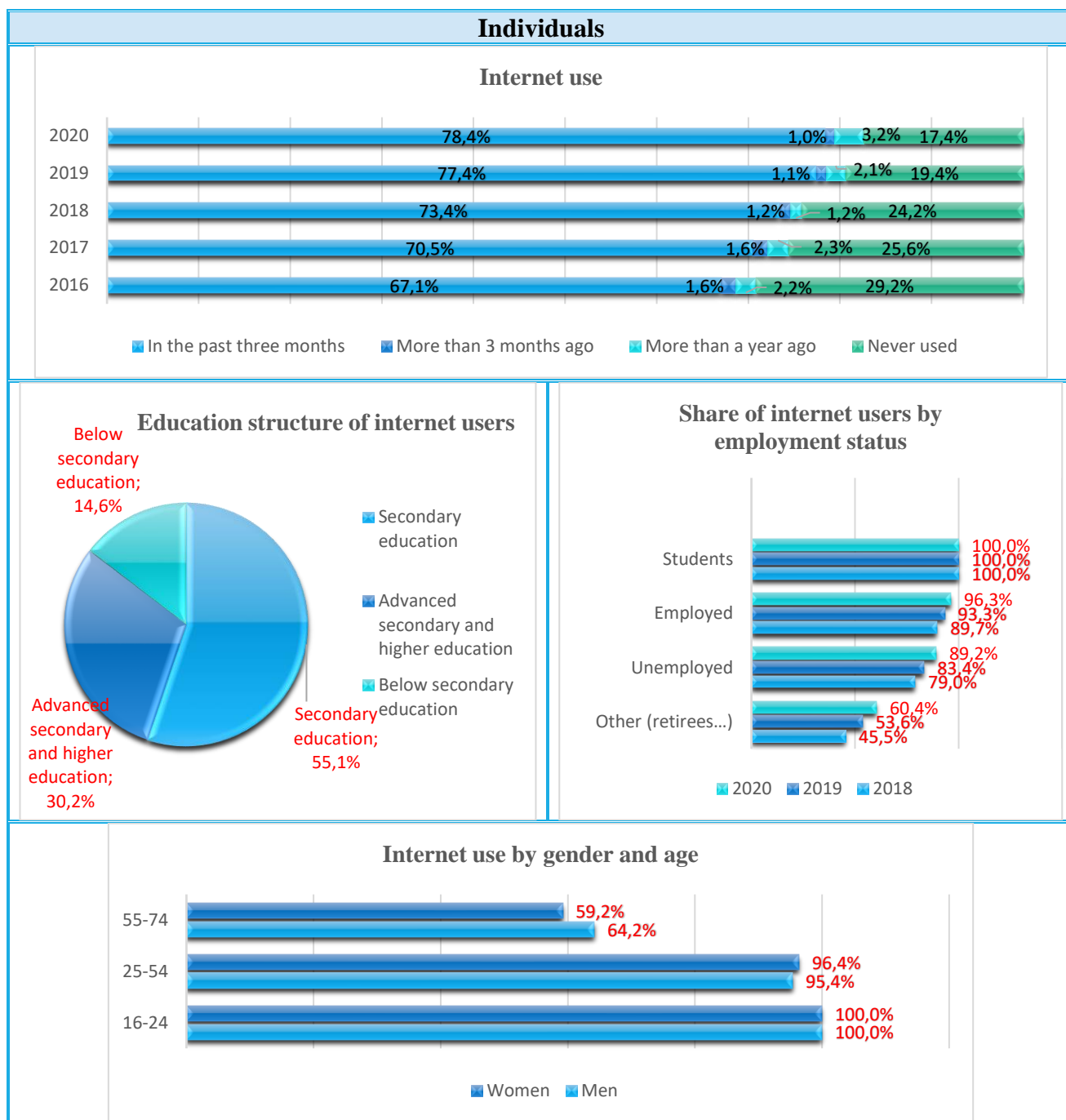
There are also considerable differences in terms of household internet connections between urban and other settlements in Serbia: 87.1% vs. 70.4%. Relative to 2019, in urban settlements the rate of increase is 1.3%, while in other areas of Serbia it is 0.1%.

Similarly as in the case of computers in households, there is also a huge gap in terms of internet connections. Looking at the structure of households measured by monthly income, those with an internet connection are mainly households with monthly income of more than 600 euros (97.8%), while the share of households with income of up to 300 euros is a mere 59%.

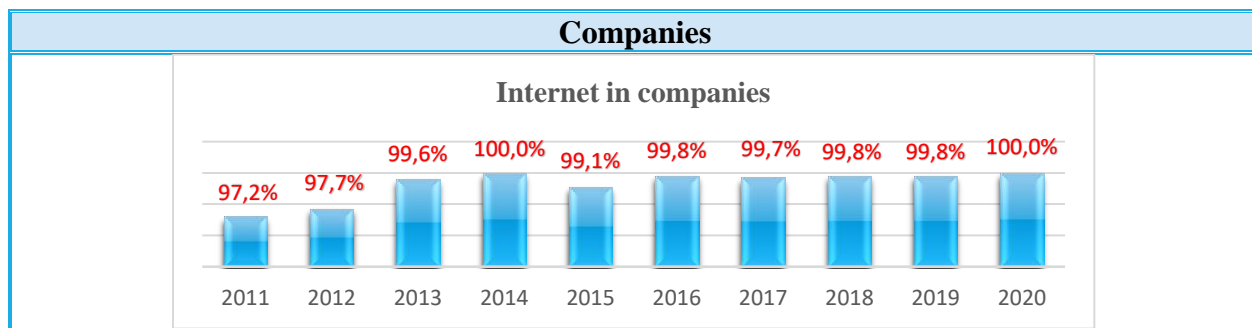
In response to the question about the reason why households do not have a home internet connection, 77.5% replied they did not need the internet, 18.7% replied the cost of equipment was too high, while 10.3% of households quoted lack of skills as the reason.



Internet use by individuals – In Serbia, 78.4% of persons have used the Internet in the past three months, 1.0% of the respondents last used the Internet more than three months ago, while 3.2% of the respondents last used the Internet more than a year ago. As many as 17.4% of the respondents have never used the Internet. The number of internet users has increased by 2%, 6.8% and 8.2% relative to 2019, 2018 and 2017 respectively.



Internet use in companies – In the Republic of Serbia, 100% of companies have an internet connection. In 36.0% of companies, between 1% and 24% of employees use the Internet, while in 35.7% of companies between 75% and 100% of employees use the Internet.



Internet use

Households

- Internet use in households is continually increasing - 81.0%
- The highest share of internet users is in Belgrade - 94.1%,
- The lowest share of internet users is in Vojvodina - 75.3%
- Internet use more common in urban areas - 87.1%
- Internet use less common in other areas - 70.4%
- Internet use is highest among households with monthly income of more than 600 euros - 97.8%
- Internet use is lowest among households with monthly income below 300 euros - 59.0%
- Key reasons for not having an internet connection include: not having a need for it, expensive equipment or connection and lack of skills.

Individuals

- The share of internet users among individuals is 78/4%
- 17.4% of persons have never used the internet of internet users have completed education levels below secondary
- Internet use is highest among students, at 100%,
- Internet use is lowest in the "others (retirees..)" group - 60.4%
- Internet use is highest among young persons aged 16-24, with 100% of men and women in this age group using computers
- Internet use is lowest among person aged 55-74, with 64.2% of men vs. 59.2% of women in this group using computers

Companies

- 100% of companies use the internet

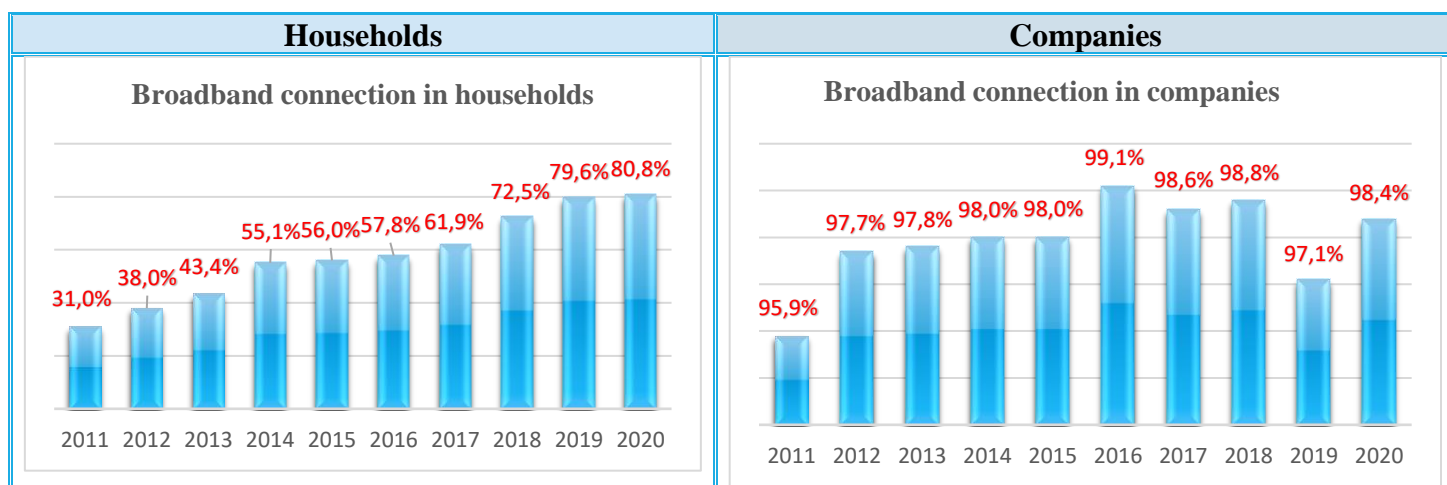
1.3.3 Broadband Internet Connection – Households, Companies

A broadband internet connection enables more than just faster internet access: it is a paradigm shift in the way a person uses the internet, with much faster download rates compared to

the traditional dial-up connection. Accordingly, a key indicator of ICT uptake in the European Union since 2005 has been the share of households with this type of internet connection. In Serbia, 80.8% of households have a broadband connection, which is an increase of 1.2% and 8.3% relative to 2019 and 2018 respectively. This type of internet connection is most widely used in Belgrade, with 93.9%, followed by Vojvodina (74.7%), Šumadija and Western Serbia (77.5%) and Southern and Eastern Serbia (77.3%).

There are also significant differences in terms of the share of this type of internet connection in urban and other settlements in Serbia: 87.0% vs. 70.1%.

According to the survey's results, out of the total number of companies with an internet connection, 98.4% have a broadband connection.



Broadband internet connection

Households	<ul style="list-style-type: none"> 80.8% of households have a broadband connection Belgrade has the highest share of broadband connections - 93.90% Vojvodina has the lowest share of broadband connections - 74.7%
Companies	<ul style="list-style-type: none"> 98.4% of companies have a broadband connection

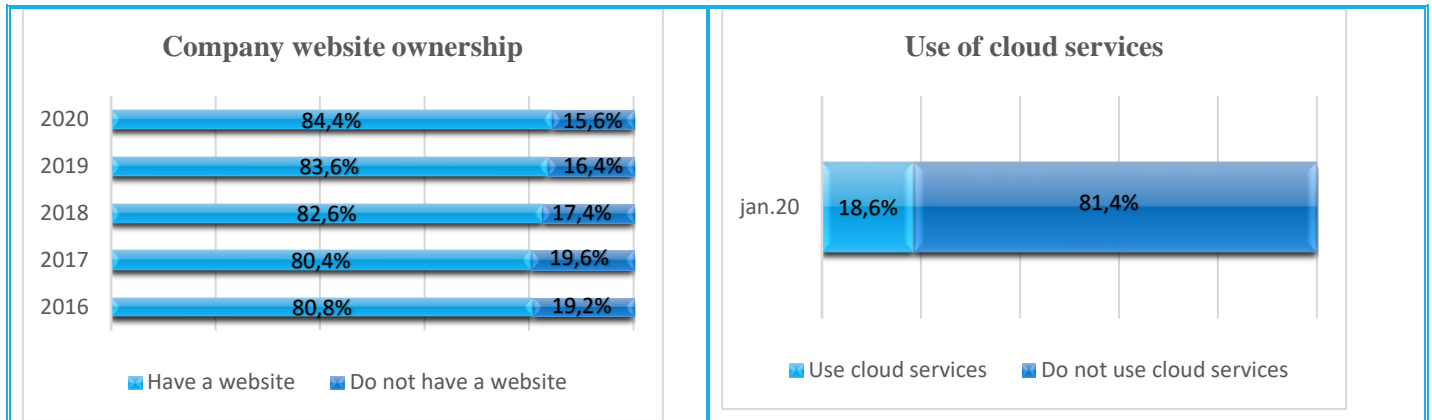
1.3.4. Website Ownership, Use of Cloud Services, Mobile Phone Use and Use of Mobile Internet for Business Purposes

Website ownership – 84.4% of companies have their own website, which is an increase of 0.8% and 1.8% relative to 2019 and 2018 respectively. In terms of the structure of companies by size, the results are as follows:

- 99.0% of large companies have a website;

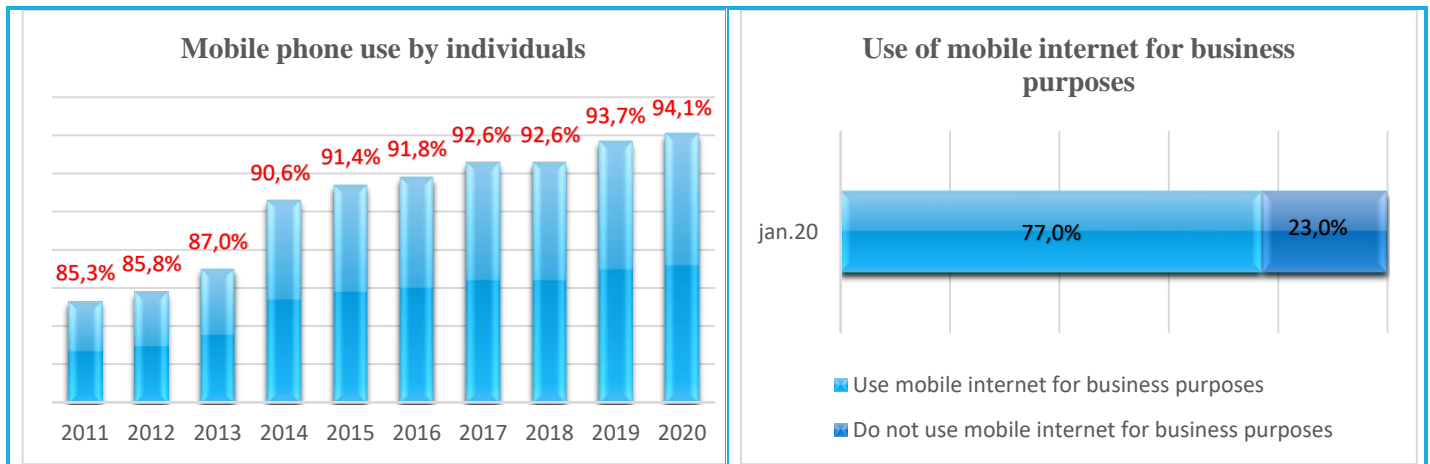
- 89.1% of medium-sized enterprises have a website;
- 82.8% of small enterprises have a website.

Use of cloud services – 18.6% companies pay for the use of online cloud services.



Mobile phone use by individuals – The survey has revealed that 94.1% of the population use a mobile phone, versus 93.7% in 2019.

Use of mobile internet for business purposes – In the Republic of Serbia, 77% of companies use a mobile internet connection on mobile devices (smartphone, laptop, tablet...).



Website / cloud service / mobile phone / mobile internet

Website ownership

Cloud use

- 84.4% of companies have a website
- 18.6% of companies pay for cloud services

Mobile phone use

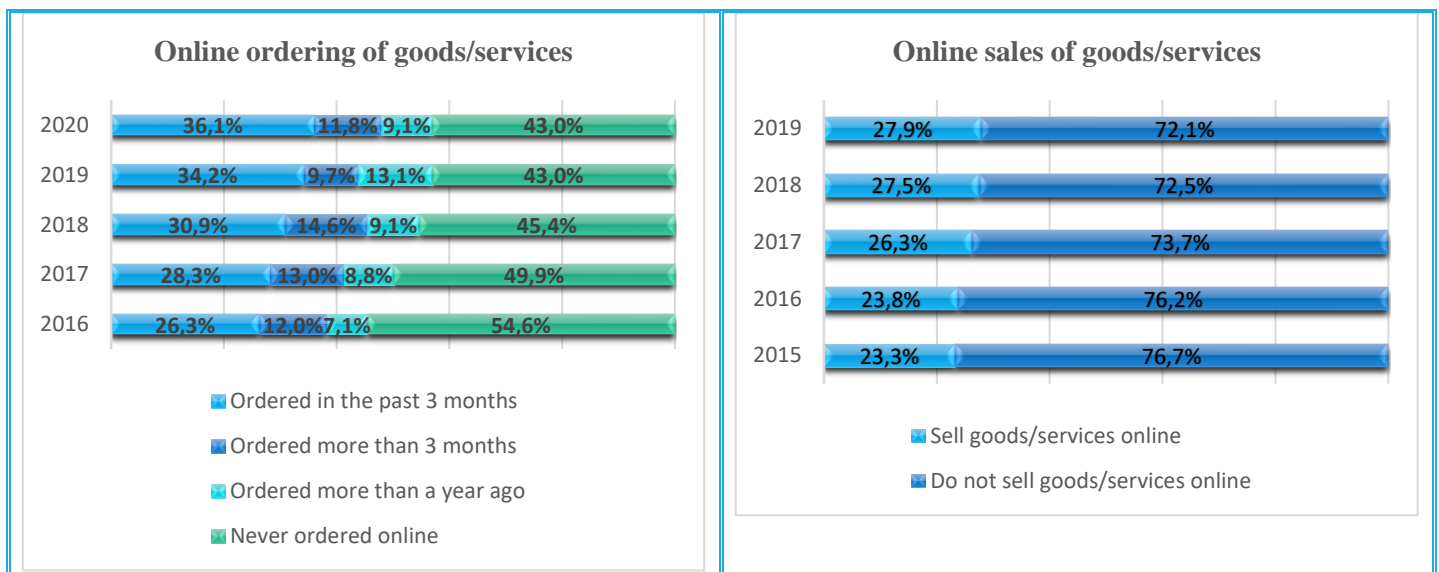
Mobile internet use

- 94.1% of the population use a mobile phone
- 77% of companies use a mobile internet connection on mobile devices (smartphone, laptop, tablet...)

1.3.5. Online Commerce

As regards the timeframe in which internet users purchased/ordered goods or services online, 36.1% of users made a purchase/ordered goods or services in the past three months, 11.8% last did so more than three months ago, while 9.1% did so more than a year ago.

Forty-three percent of internet users have never purchased/ordered goods or services online. In 2019, 27.9% of companies in the Republic of Serbia sold goods/services online.



Online Commerce

Online ordering of goods and services

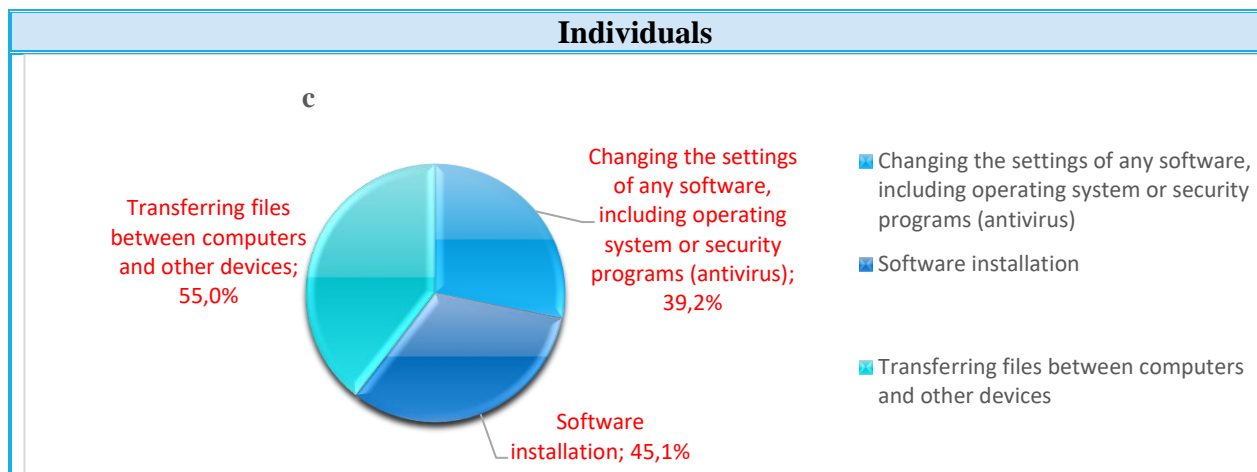
- 57% of internet users have ordered goods at various intervals
- 43% of internet users have never ordered goods or services online

Online sales of goods and services

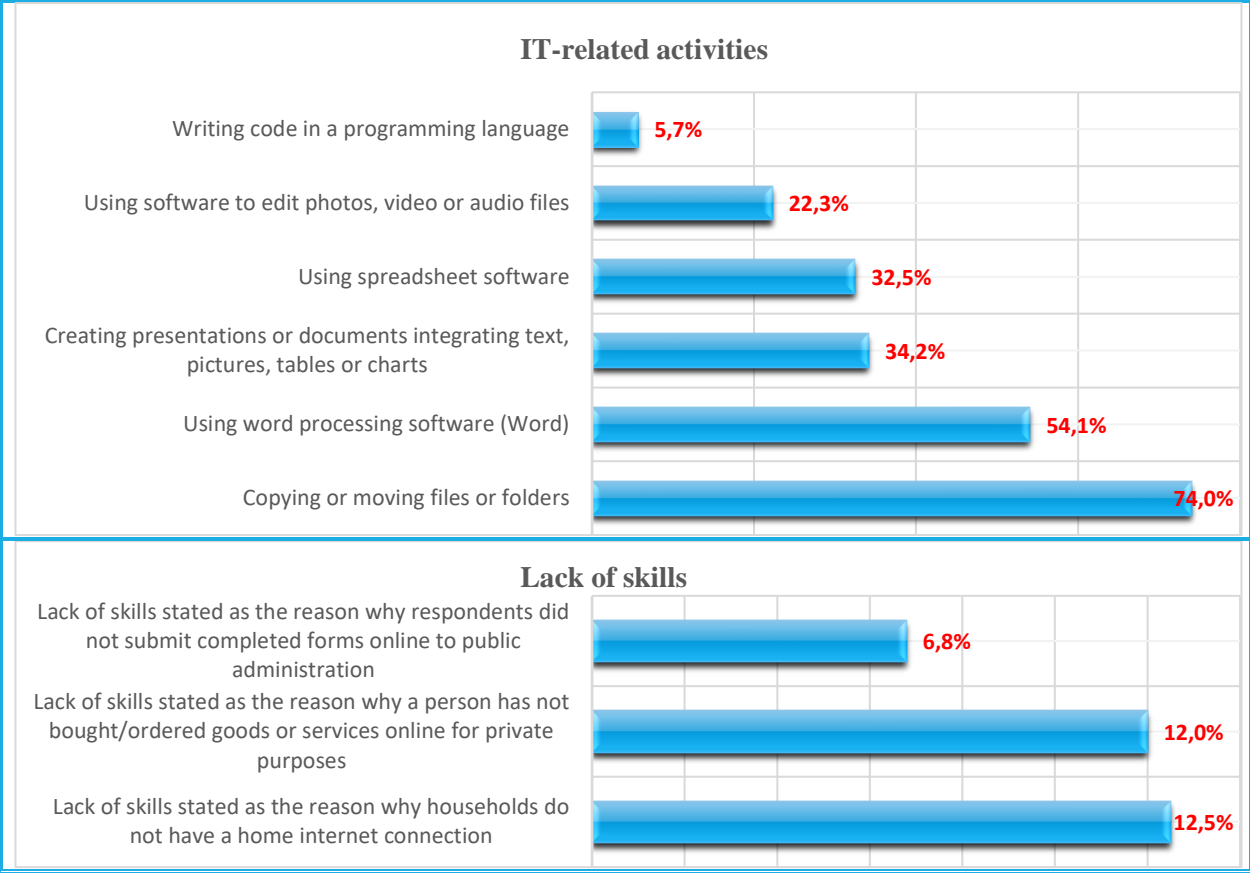
- 27.9% of companies have sold goods and services online

1.3.6 e-Skills³

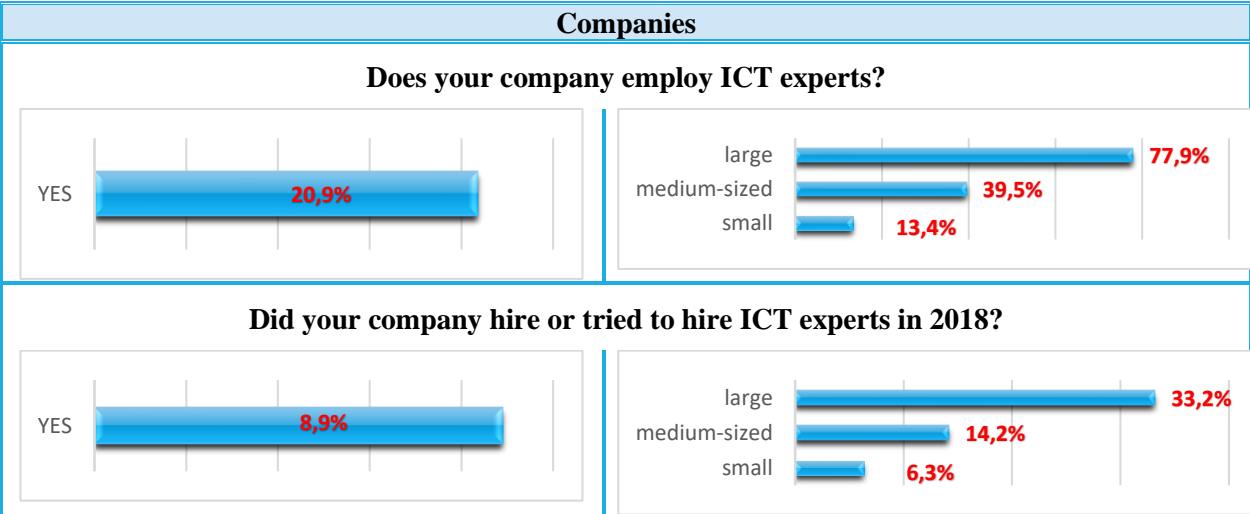
e-skills of individuals – As part of the SORS survey, the respondents also answered questions about the activities they had carried out using computers and mobile phones and the IT-related activities they had performed. In response, 55% of them stated “Transferring files between computers and other devices” as the activity they had performed, while 74% of the respondents replied the IT-related activity they had performed was “Copying or moving files or folders”.



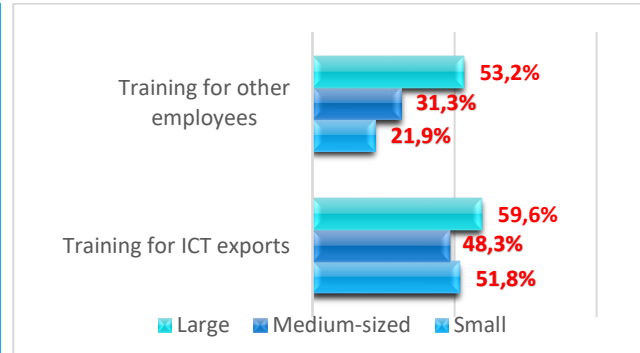
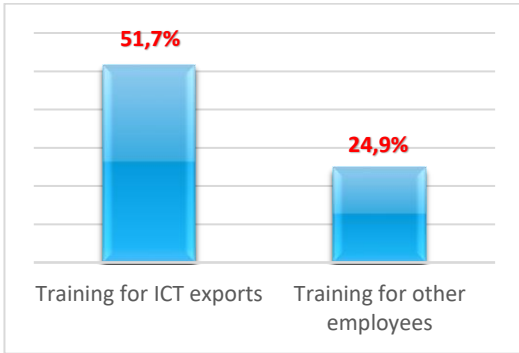
³ The source of data on e-skills is the publication of the Statistical Office of the Republic of Serbia *Usage of information and communication technologies in the Republic of Serbia, 2019*
<https://publikacije.stat.gov.rs/G2019/Pdf/G201916014.pdf>



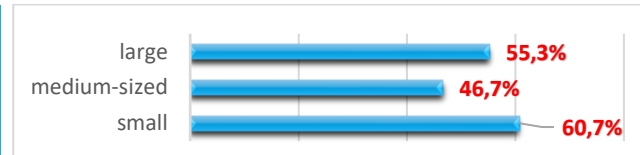
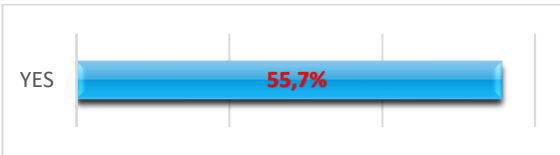
ICT experts and skills – The demand for ICT experts in this day and age is self-explanatory, as evident from the fact that 20.9% of companies employ ICT experts, 55.7% had job vacancies for ICT experts, while as many as 77.1% outsource their ICT functions.



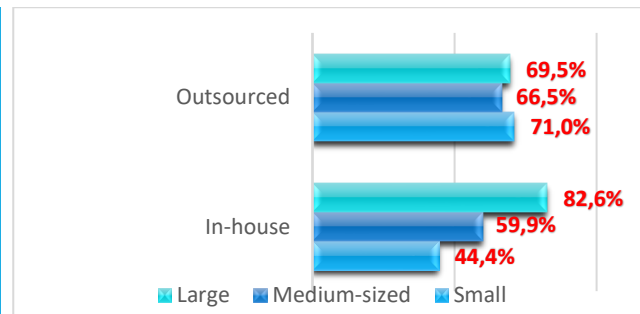
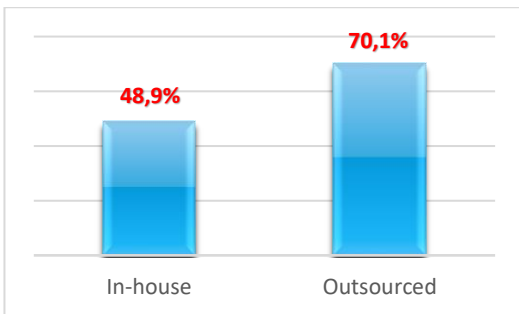
Did your company provide any form of employee training for ICT skills development in 2018?

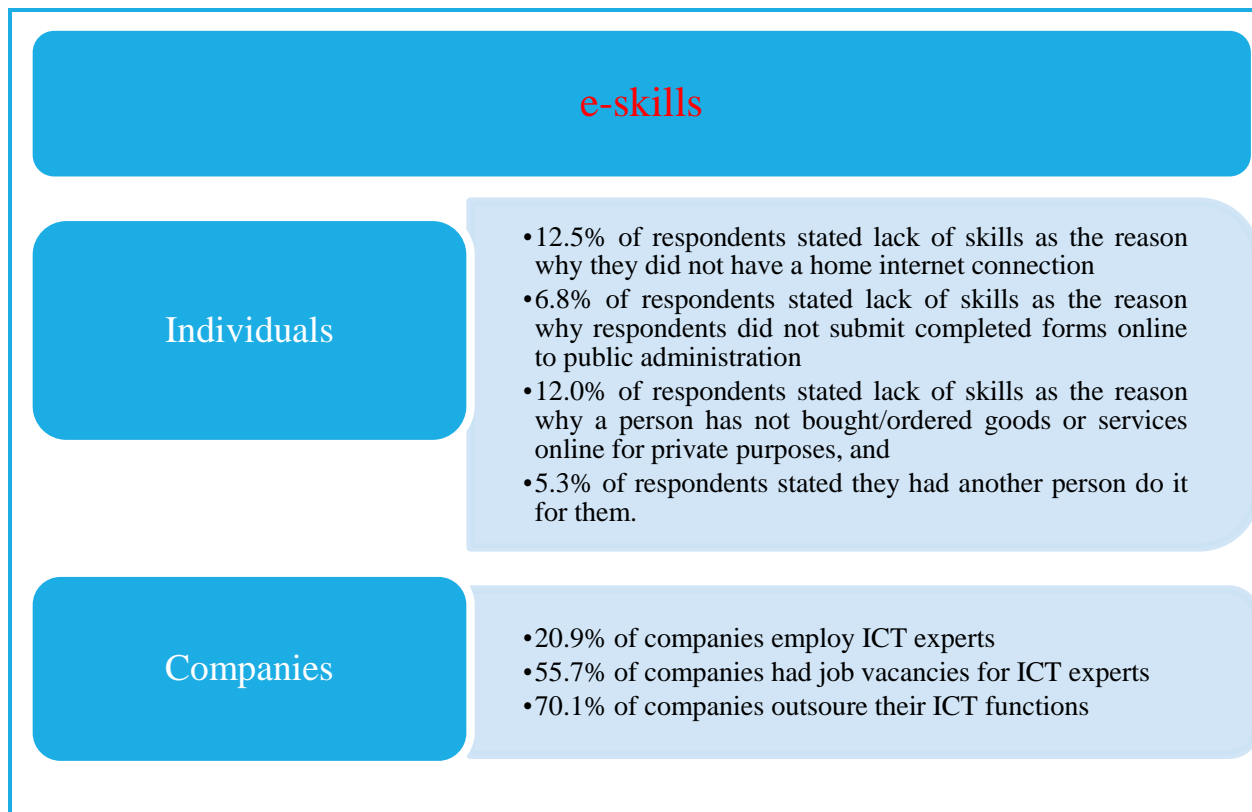


Did your company have job vacancies for ICT experts that were difficult to fill in 2018?



Please specify how ICT functions were performed at your company in 2018

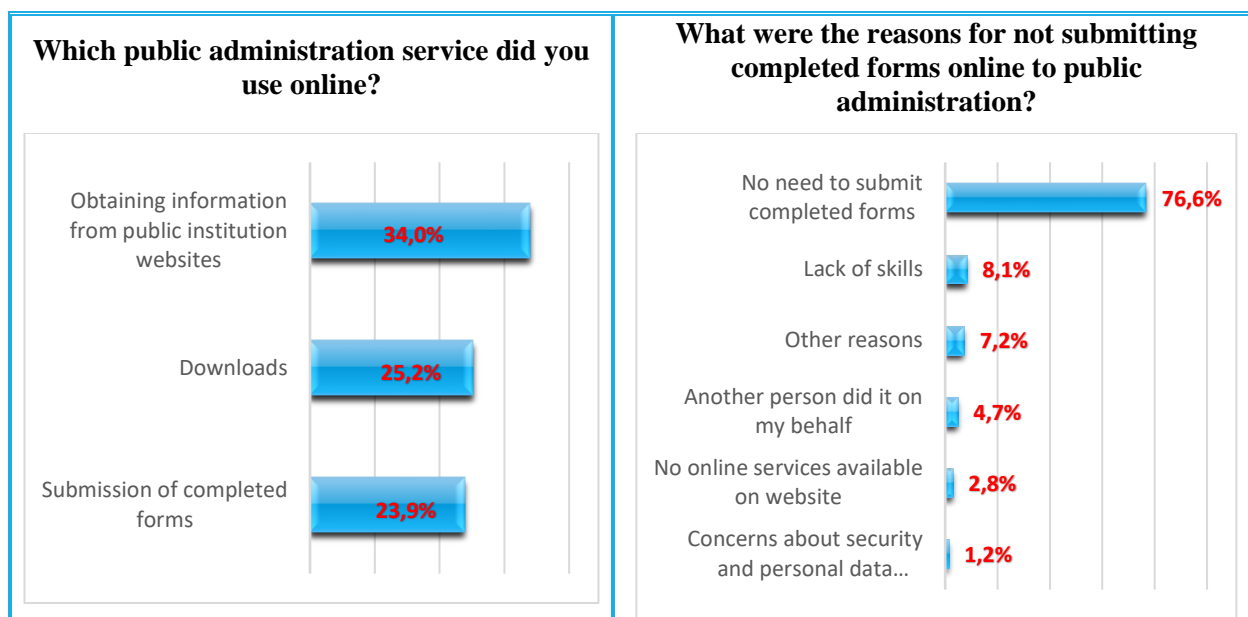




1.4 PUBLIC ADMINISTRATION (E-GOVERNMENT)

According to the SORS survey, 37.0% of the internet population use online services instead of making personal contacts or visiting public institutions or administration authorities. It is claimed that 1,415,000 persons use a public administration website/application to obtain information.

As part of the SORS survey, the section “Use of e-Government” provides data on e-government services, with an overview of e-government services used by respondents and reasons why they did not submit completed forms online.



Based on the survey data, it appears that, while the share of persons obtaining information from websites of public institutions is high (34.0%), online communication with public administration is evidently less common (23.9%) since the availability of this service is relatively modest, given that 76.6% of respondents replied they had no need to submit completed forms.

The Republic of Serbia has created preconditions for the development of e-government by passing legislation to regulate this area, as well as by forming the IT and e-Government Office, as the authority responsible for providing the services of the e-Government Portal. The e-Government Portal is the gateway for e-services for all citizens, businesses and public administration employees and enables users to perform from their home, without physically coming to a service desk, certain public administration tasks that have hitherto required them to come to public administration offices.

The e-Government offers numerous services provided by various institutions, including:

IT and e-Government Office	“Welcome to the world, baby!”
	Local tax administration
Ministry of the Interior	Vehicle registration renewal at authorised inspection garages (service intended for individuals)
	Temporary residence registration for foreign nationals
	Application for a certificate of (no) criminal convictions
	e-Appointment – qualified electronic certificate, available in 57 municipalities in Serbia
	Renewal of firearm registration certificates/firearm surrender (natural persons)
	e-Appointment – identity card of passport, available in 80 municipalities in Serbia

	Renewal of firearm registration certificates/firearm surrender (natural persons)
Ministry of Education, Science and Technological Development	e-Gradebook
	e-Enrolment – Electronic enrolment of first-graders
National Health Insurance Fund	Application for issuance of a medical insurance card and replacement of a medical insurance booklet with a medical insurance card
Medicines and Medical Devices Agency of Serbia	Browsing of medicinal products approved for human use for which the Agency issued a marketing authorisation
	Browsing of medicinal products approved for veterinary use for which the Agency issued a marketing authorisation
	Browsing of medical devices
	Browsing of certificates for batches of medicinal products approved for human use
	Browsing of certificates for batches of medicinal products approved for veterinary use
	Downloading open data on approved clinical trials
	Downloading open data on generic names of medical devices
City of Loznica City of Valjevo City of Sremska Mitrovica City of Niš	Registers of Births

To ensure further development in this field, e-Government Development Programme of the Republic of Serbia for the period 2020-2022 and the Action Plan for its implementation were adopted pursuant to a proposal by the Ministry of Public Administration and Local Self-Government, as the ministry responsible for the development of e-government. The Programme envisages public policy measures which will have a major impact both on the operation of the entire public administration, which is required to act in accordance with the Law on e-Government, and on all citizens and businesses.

The e-Government Development Programme states that a key challenge for successful digital transformation of Serbian public administration is laying the foundations to ensure activities remain on track and to ensure implementation of the planned measures across all segments of public administration, in a way which will enable efficient and coordinated functioning of that system.

1.4.1 e-Justice, e-Education, e-Health and e-Culture

E-JUSTICE – The importance of e-judiciary is also recognised in the Judicial Development Strategy for the Period 2020–2025 (*Official Gazette of the Republic of Serbia* No. 101/20), through the specific objective “Development of e-judiciary”, which envisages further

improvements of judiciary e-services to ensure access to justice, improved quality of acting and decision-making, efficient resource management, statistical monitoring and reporting on the work of the judiciary and transparency in the work of judicial authorities. The draft Strategy also states that the use of modern ICTs, standardised software and centralised case management systems at courts and public prosecutors' offices is necessary in order to implement the key principles of an effective judiciary: independence, impartiality, accountability, professionalism, efficiency and transparency. This calls for continual development of the e-judiciary system, as a mechanism that facilitates the attainment of all strategic objectives.

In accordance with the Guidelines on ICT System Development in the Judiciary, by implementing the measures and activities set out in various action plans (including those pertaining to the Government's priority objectives, Chapter 23 of EU accession negotiation, reform of the Judicial Development Strategy and the fight against the shadow economy), the Ministry of Justice strives to apply state-of-the-art information and communication technologies in judicial authorities and the judicial professions through the implementation of various projects.

Significant progress has been achieved in recent past regarding judicial ICT systems improvement through projects implemented by the e-Justice Division of the Ministry of Justice, which enable the provision of various e-services.

Judicial Information System – The Judicial Information System was commissioned in late 2017, enabling electronic data exchange between judicial authorities, the judicial professions and other state institutions. The Judicial Information System gives all courts, public prosecutors' offices, notaries public and bailiffs access to data contained in various registers and records maintained by the competent institutions (Central Register of Compulsory Social Insurance, Misdemeanours Records, Administration for the Enforcement of Penal Sanctions, Ministry of the Interior, Civil Registries, Business Registries Agency, Republic Geodetic Authority, courts of general jurisdiction, Pension and Disability Insurance Fund, Property Transactions Register, National Bank of Serbia and Tax Administration.

According to the statistics of the Ministry of Justice, since the commissioning of the system, users have submitted 4,000,000 electronic inquiries. This expedites the average judicial proceeding by approximately 3 to 6 months.

ProNep application – The ProNep application has been used since 2018 for the submission of data and documents by notaries public to the Cadastre, with the functionality of submitting data and documents to the competent tax authorities was introduced in 2020, making this a “one-stop shop” for procedures involving property transactions. The ProNep information system has been established to simplify the procedure and save time and money in administrative procedures conducted in connection with the transfer of title, including in particular through purchase, sale and gifting of real estate, as well as probate proceedings etc.

System of electronic communication with the Administrative Court – e-Court – The e-Court system, commissioned in 2018 and accessible online, enables all parties – both attorneys and citizens – to fully conduct an administrative dispute electronically. It is planned to include commercial courts in the e-Court system in the near future, followed by courts of general jurisdiction. For citizens and attorneys, this system effectively means the court operates 24 hours a day, 7 days a week, and they no longer have to physically come to the court's building to deliver a submission or examine a case file, as everything is available online.

Electronic notice board – e-Board – The electronic notice board was commissioned on 1 January 2020 for enforcement proceedings and gives citizens swift and simple online access to an integrated notice board used in enforcement proceedings. The e-Bord now gives citizens and legal entities access to all writs in enforcement proceedings which were not successfully served on them in person by a court or a bailiff.

e-Auction in property foreclosures – The e-Auction system for public online auctioning of foreclosed property, which is scheduled to be commissioned in 2020, ensures a transparent procedure for the online sale of foreclosed properties and availability of information to all who are interested in participating in such procedures.

Central case management system – SAPO (Standard Application for Prosecution Offices) and SAPA (Standard Application for Prison Administration) – The SAPO case management information system was implemented to increase the efficiency and transparency of public prosecutors’ offices and penal and correctional facilities in the Republic of Serbia. While the system has not yet been implemented at all prosecutors’ offices, the Ministry of Justice, with the support of EU funds under IPA 2015, is currently implementing the SAPO software in the remaining public prosecutors’ offices. The SAPO software allows case management throughout the entire lifecycle of a case, from the initial submission to the passing of a final decision and its archiving. Furthermore, the same system is also used to implement the SAPA (Standard Application for Prison Administration) system in all penal and correctional facilities.

e-Payment+ - The Ministry of Justice, in collaboration with the IT and e-Government Office, has established a system that gives citizens and legal entities, as well as foreign natural persons, the option of paying electronically, i.e. online, their misdemeanour fines included in the Register of Outstanding Fines and Other Pecuniary Amounts.

Case and content management software – LURIS – Luris is a case management application for international assistance which provides case management functionalities and covers the entire course and lifecycle of a case, from the receipt of a petition to the preparation of a final outgoing document and archiving.

With a view to further improving e-services in the judiciary sector, which would ensure access to justice, improve the quality of proceedings and decision-making and enable efficient case management, statistical monitoring and reporting on the work of the judiciary and transparency in the operations of judiciary authorities, reform measures have been envisaged which are implemented under the Judicial Development Strategy.

E-EDUCATION – The importance of digitalisation in the field of education is witnessed by the fact that the Ministry of Education, Science and Technological Development has a Department for Digitalisation in Education and Science and has been working to facilitate digitalisation, primarily by purchasing ICT equipment for primary and secondary schools to use electronic education systems, which has resulted in the establishment of 10,000 digital classrooms.

“Connected Classrooms” project – the Ministry of Trade, Tourism and Telecommunications has equipped 550 primary and secondary school with WLANs and this activity continues within the framework of the “Connected Classrooms” project, which will provide reliable and safe internet access in all teaching and administration rooms at schools, for each pupil in the education system.

e-Gradebook – The e-Gradebook has been designed for and implemented in all primary and secondary schools in the Republic of Serbia, after appropriate staff trainings necessary for proper and secure use of the e-Gradebook, which also gives parents/other legal representatives of pupils electronic access to pupils' achievements via the “my.e-Gradebook” module.

e-Learning service – The e-Learning service currently offers 13 online courses, with available expert literature, as teaching support for 53 IT classes for pupils with special needs learning computer science and information technology at general secondary schools in the Republic of Serbia. The courses are available on the online platform of the Institute for the Advancement of Education, which is publicly available, and the material includes syllabuses taught in the 1st, 2nd and 3rd grade of general secondary schools.

e-Enrolment – Services enabling electronic enrolment of pupils in the first year of primary school and the first year of secondary school have been established in cooperation with the IT and e-Government Office.

EMIS – To lay the foundations for more efficient resource planning and management and monitoring of activities in the education system across all levels, activities have been initiated to establish an Education Management Information System (EMIS).

In the coming period, numerous activities aimed at digitalisation in the field of education will be continued, as elaborated and specified in the Education and Science Development Strategy by 2030 and the Action Plan for implementing the programme of the Government of the Republic of Serbia pertaining to the development and application of the Education Management Information System, improvement of ICT infrastructure of education institutions, digital capacity building of all education levels below university, improved digital competences of employees in the education sector, implementation and promotion of innovative pedagogical approaches involving ICT integration in the teaching and learning processes, establishment of a system for continual monitoring of digital education development, building of pupils' digital competences and establishment of a digital environment for the development of open education resources, digital services and teaching and learning support materials.

E-HEALTH – A key priority for the Serbian government is digitalisation of the health care system, given that it has been recognised as one of the most complex and vital systems, as corroborated during the COVID-19 pandemic.

Numerous activities aimed at digitalisation in this field have been implemented recently, including:

e-Prescription – e-Prescription was implemented in March 2019 in all primary health care institutions, in secondary and tertiary health care institutions where the competences of the chosen physician are assigned by the law to a specialist physician, as well as in social welfare institutions. Together with e-Prescription, the e-Therapy service was also implemented to allow chronic patients to obtain medication for 2 to 6 months, depending on their health status, which reduced the number of required visits to physicians and pharmacies.

National Prevention and Diagnostics Medical Platform (e-Radiology) – Through the project of the National Prevention and Diagnostics Medical Platform, the Ministry of Health has ensured the implementation of a central information system in radiology, which connects all diagnostic devices, where possible, and gives the radiologist, the chosen physician and the patient access to images in the form of an electronic medical record, which contributes to cost savings on image development and increases work productivity.

e-Health portal for patients – The e-Health portal of the Ministry of Health is designed to give patients access to their medical information (reports, prescriptions, radiology images etc.), the possibility of scheduling appointments, communication with a physician (via video call), information on PCR tests and information on COVID-19 vaccination.

In addition, activities which are already underway and are scheduled to be completed include:

Electronic Medical Record – The Electronic Medical Record will enable the exchange of all medical information relating to patients vertically across the health care network and will give physicians access to all medical documentation of a patient. The system is expected to be put into production in June 2021.

e-POS – A system for electronic registration of deaths, which will enable the submission of data to a registrar for entry in the Register of Deaths, as well as to the Public Health Institute “Batut” and the Statistical Office of the Republic of Serbia.

e-SickLeave

Extension of the e-Prescription to include medical aids

A platform for phone consultations between physicians and patients

The Government of Serbia has also formed the Coordination Body for Health Case System Digitalisation, with the aim of ensuring a strategic approach to e-health development. This body is tasked with developing a National e-Health Development Programme with an Action Plan, improving the legislative framework and implementing state-of-the-art technology in this sector.

E-CULTURE – The Draft Culture Development Strategy of the Republic of Serbia 2020-2029 recognises the importance of digitalisation in culture and, accordingly, sets “Digitalisation in Culture” as a specific objective, which should systemically regulate the process of digitalisation of cultural heritage and build the capacities of cultural institutions for implementing this process. The focus will in particular be on digitalisation of archives and development of e-archives, improved operation of integrated software solutions in the field of culture for the protection of cultural assets, as well as contemporary artworks.

The following digitalisation activities have recently been implemented:

- All four areas of culture – libraries, museums (galleries), archives and institutes for the protection of monuments – use integrated software solutions for keeping documentation on their inventories and cultural assets;
- The Cultural Heritage Browser has been developed, which aggregates data from all four databases of the integrated software solutions and presents them to the general public;
- In cooperation with the Republic Geodetic Authority, a map of cultural institutions and cultural monuments visible on the Serbian Geoportal has been developed;
- In cooperation with the Ministry of Trade, Tourism and Telecommunications and the Academic Network of the Republic of Serbia (AMRES), connecting of cultural institutions to AMRES is implemented as an ongoing activity;
- Development of an information system for keeping integrated field archaeology documentation is at the final stage;
- The first dataset in the map of archaeological sites of the Republic of Serbia has been developed and posted;

- In cooperation with the Ministry of Justice, the Ministry of the Interior and the Customs Administration of the Ministry of Finance, efforts are underway to develop an electronic database on stolen and disappeared artwork and historic items;
- Draft Decree on Uniform Technical and Technological Requirements and Procedures for the Keeping and Protection of Archival and Documentary Material in Electronic Form is currently being prepared;
- The e-Museum application has been developed to help modernise content presentation and connect schools and museums. It can also be used in education and in teaching courses.

The objective of the Strategic Priorities for the Development of Culture of the Republic of Serbia 2021-2025 in the digitalisation sphere is to close the existing gap in the purchase and use of modern information and communication technologies, train the staff of cultural institutions and identify the actual needs for digitalisation of cultural heritage and contemporary artworks.

This objective is implemented through:

1) Normative bylaws governing the digitalisation process, which set out the responsibilities and competences of cultural institutions and stakeholders in the digitalisation process:

- The Decree on Uniform Technical and Technological Requirements and Procedures for the Keeping and Protection of Archival and Documentary Material in Electronic Form, which will set forth the procedures for e-archiving and permanent keeping of electronic documents, creation of e-archives and harmonisation of the process of digitalisation of archival material and the existing Integrated Archiving Software Solution (ARHIS) with the e-archive.
- Guidelines on digitalisation of cultural heritage of the Republic of Serbia aim to define the technical standards and metadata for uniform and interoperable implementation of the process of digitalisation of cultural heritage in the Republic of Serbia. Adoption and implementation of the Guidelines will ensure uniformity in the work of conservation institutions the digitalisation process.
- The Bylaw on Security of ICT Systems in Cultural Institutions, which is planned to be adopted, would include all security measures provided for in the Law on Information Security. It is necessary to adapt the model to reflect the specific nature The model needs to be adapted to reflect the specific nature of the systems and the actual state of play regarding system security needs to be determined; furthermore, the current state needs to be brought in compliance with the recommendations and standards set forth in the Law and the Decrees.

2) Implementation and development of new services on an artificial intelligence platform, which would be applied to datasets available in the databases of the Integrated Software Solutions in the field of culture;

3) Networking of existing integrated software solutions for museums, archives, libraries and institutes for the protection of cultural monuments and development and upgrading of new ones;

4) Capacity building of cultural institutions in the digitalisation process through purchase of modern technology and hiring of digitalisation staff.

1.4.2 e-Transactions, e-Commerce and e-Tourism

E-TRANSACTIONS – The cornerstone for developing a more comprehensive and widespread e-transactions in the Republic of Serbia was laid down with the passing of the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions, as well as the Law on e-Government. These two laws set forth the main legal concepts that enable e-transactions between public authorities, citizens and businesses.

Electronic document – The Law that the validity, evidentiary power and written form of a document cannot be contested just because it is in electronic form. This is a crucial provision, since it reflects the applicable principle and ensures that electronic documents are recognised on an equal footing with paper-based ones. The provision is also important because it implies that both paper-based and electronic forms of documents are considered to be made in writing.

The Law also provides for digitalisation of paper-based documents and grants such documents equal evidentiary power as the original, by providing that documents may be digitalised by the body passing the document, a notary public or a person designated for digitalisation and provides for digitalisation in a procedure before a public authority.

These legal arrangements enable the conduct of procedures before public authorities electronically instead of using paper-based documents, which cuts the use of hard-copy documents, increases document accessibility and facilitates document searches and use, which ultimately results in lower costs of hard copies and archiving.

However, while legal prerequisites for wider use of electronic documents and e-transactions have been provided, replies to a questionnaire which was distributed to all ministries and which 11 ministries answered, have shown that the level of electronic communications with parties remains relatively low. Namely, 7 ministries have electronic addresses for the receipt of electronic submissions, while 4 ministries have no such address; also, seven ministries provide electronic services, while three ministries do not. It was also found that two ministries applied Articles 11 and 12 of the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions, which provide for the digitalisation of paper-based documents and almost full transition to electronic communication and transactions with electronic documents.

Electronic identification – The Law also provides for electronic communication, i.e. the procedure of using personal identification data which enable natural persons or legal entities to access electronic services.

The Register of Electronic Identification Schemes has been established pursuant to the Law, with two such schemes registered thus far by the IT and e-Government Office.

The Law provides for three levels of confidence of electronic identification schemes and it is paramount to have as many such schemes included in the Register as possible, given that such schemes may be used in communication with public authorities, since an electronic identification scheme with a high degree of confidence replaces a party's signature on a submission, although this does not preclude the application of other levels of confidence in cases where the law allows public authorities to use lower confidence levels.

Qualified trust services – Before the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions came into force, the Republic of Serbia used qualified electronic signature and qualified electronic timestamp services. The new Law

regulates also the use of other trust services which may be applied and guarantee the authenticity and integrity of data in a far wider range of e-transactions, including electronic stamp, electronic delivery, electronic archives, website authentication, cloud signature etc.

Namely, there are seven providers of trust services in the Republic of Serbia, although it should be noted that most of them have been issuing qualified electronic signatures and qualified electronic timestamps.

The underlying concept of qualified trust services is that the service provider guarantees the authenticity and integrity of individual pieces of data created in various legal affairs and transactions conducted electronically. In electronic transactions, confidence in the authenticity of data is paramount, to minimise the risks of abuse and data integrity breaches, which is why qualified trust services have been introduced and granted the highest level of legal guarantees, based on the high-level technical, security and organisational conditions under which they are provided. As these services currently include mostly electronic signatures and timestamps, it is crucial that new trust services gain traction in practice, especially cloud signatures and qualified electronic delivery services.

As of February 2021, more than 650 thousand valid qualified electronic certificates have been issued, with approx. 850 thousand certificates issued in total. For this number to increase, it is necessary on the one hand to popularise the use of certificate, while also enabling the use of an increasing number of services accessible through qualified electronic certificates. It is expected that the use of cloud signatures will boost mass acceptance of signatures, as it facilitates access to services from mobile phones, unlike the previous means of generating electronic signatures, which many users found to demanding to install and use.

E-COMMERCE – The legislative framework regulating e-commerce comprises the Law on Commerce (*Official Gazette of the Republic of Serbia*, number 52/19), the Law on e-Commerce (*Official Gazette of the Republic of Serbia*, No. 41/09, 95/13 and 52/19) and the Law on Consumer Protection (*Official Gazette of the Republic of Serbia*, No. 62/14, 6/16- new law, and 44/18 – new law).

The new Law on Commerce, passed in 2019, regulates e-commerce in the Republic of Serbia. This Law introduces for the first time the concepts of “e-shop”, whereby a retailer sells its goods directly to the consumer, and “online platform”, which connects sellers with buyers. Furthermore, the Law also recognises for the first time the business model of “dropshipping” (which has been used in practice for quite some time), whereby the goods do not physically reach the retailer and are instead shipped directly from the manufacturer/importer to the consumer. A major legislative novelty is the introduction of the concept of “mystery shopper”, whereby an inspector is authorised, in the event of reasonable suspicion that a retailer is unregistered, to carry out mystery shopping and thus obtain evidence. The Law also provides for the possibility of granting incentives to e-retailers, which is to be regulated in detail by a bylaw passed by the Government, with a view to boosting e-commerce development and combating the shadow economy in the online market.

To promote the development of digital economy and eliminate obstacles to e-commerce development in the Republic of Serbia, the Government has passed the e-Commerce Development Programme in the Republic of Serbia for the Period 2019-2020 with the Action Plan. It is the first

public policy document in the field of e-commerce development in the Republic of Serbia for the period 2019-2020. The e-Commerce Development Programme in the Republic of Serbia for the Period 2019-2020 sets out the specific objectives of improving e-commerce in the domestic market, as well as programme measures and activities designed to contribute to an improvement across all segments in the process of online ordering of goods/services, such as payment, logistics, customs, e-consumer rights etc., which are essential for continued growth and development of this form of commerce. The set of measures and activities included in this programme document will provide a boost to all stakeholders in the ecosystem. Specifically, these measures and activities include: strengthening customers' trust in e-commerce (media campaigns, consumer guide, improved non-litigious dispute resolution in e-commerce), strengthening the position of e-retailers (development of guides for retailers, support to female entrepreneurship, educational courses for retailers), media education, improved operation of courier services, promotion of electronic payments, improved work of inspection authorities and greater involvement of the academic community through stronger cooperation in this field.

The adoption of this Programme was preceded by a comprehensive survey conducted within the framework of the project "Strengthening e-Commerce in the Republic of Serbia", the results of which have identified the key barriers, both on the supply side and on the demand side (the survey results are incorporated in the section of the Programme providing the background on e-commerce – the *ex ante* analysis). The measures and activities set out in the Programme have been defined to respond to the key challenges and barriers identified by the survey.

E-TOURISM – The Tourism Development Strategy of the Republic of Serbia for the Period 2016-2025 (hereinafter referred to as the "Tourism Development Strategy") was adopted in 2016. The section providing the background states that implementation of previous Strategies did not make sufficient use of the possibilities and advantages of information and communication technologies, the Internet, social networks and platforms to promote Serbia's tourism offer, as well as platforms for the development of new SMEs and their services.

Accordingly, the Tourism Development Strategy sets out the following objective: improvement and harmonisation of statistical data collection and processing methodology and procedures with the international standards and practices, building on the relevant legislative grounds.

In accordance with the Tourism Development Strategy and taking into consideration the priorities of digitalisation of Serbian economy and continued development of e-government, the Law on Hospitality (*Official Gazette of the Republic of Serbia* No. 17/2019) provides for the implementation of a central information system in the field of hospitality and tourism (e-Tourist), as an integrated and centralised electronic information system containing all relevant data on accommodation providers and accommodation facilities, which will be used for their recording and for entry of other data resulting from hospitality, nautical tourism hunting tourism and general tourism activities.

The primary goals of e-Tourist implementation are to integrate all data on accommodation providers, accommodation facilities and hospitality establishments, to shorten and cut the number and costs of administrative procedures, to improve cooperation and data exchange between the competent state institutions, to increase efficiency of the accommodation charge collection and

payment control system and consequential increase in revenues for local self-government budgets and the national budget, to reduce shadow economy and illegal work (especially by natural persons providing accommodation services), to improve statistical monitoring of the movement of tourists, to implement an active marketing policy and to increase competitiveness of Serbia's tourism offer.

These activities will result in digitalisation of tourism and hospitality through implementation of modern technologies in the operations of both economic operators and the public sector.

1.4.3 e-Construction, e-Agriculture

E-CONSTRUCTION – As regards e-construction, significant progress has been made recently with regard to electronic building permits. Implementation of an electronic building permit issuance system is based on the new Law on Planning and Construction, and as such poses a key reform challenge. The key effects of implementation of the electronic building permit issuance software include faster and cheaper obtaining of permits and a one-stop shop for all permit-related procedures.

Activities are underway to improve the software and enable faster and easier obtaining of electronic building documents by adding new functionalities and upgrading the existing ones, based on needs stated by system users and an analysis of e-document issuance.

Numerous activities are also underway within the mandate of the Ministry of Construction, Transport and Infrastructure to digitalise processes and procedures concerning Energy Performance Certificates, spatial and urban planning, inland waterway transport and navigation safety.

E-AGRICULTURE – The Agriculture and Rural Development Strategy of the Republic of Serbia for the period 2014-2024 identifies, as an activity aimed at achieving the strategic objectives, the development of all types of analytical information systems supporting agriculture, including any missing parts of agricultural statistics, the public reporting and forecasting service system, market information, registers etc.

The Directorate for Agrarian Payments plans to digitalise the procedure for granting subsidies to farmers by implementing an IACS. Subsidies will be granted according to the procedures and in the manner set forth in the IACS (Integrated Administrative and Control System), which is used for granting, controlling and monitoring agricultural subsidies (all direct payments and rural development payments linked to the surface area of agricultural land).

The Directorate for Agricultural Land operates an information system comprising three web-based applications and one desktop (client-server) application. The two web-based applications are used in the development and implementation of the Annual Protection Programme and regulation and use of agricultural land by all local self-government units in the territory of the Republic of Serbia and the Directorate for Agricultural Land, while one application provides public access and services, as well as viewing of information on state-owned agricultural land. Plans are underway to upgrade the existing information system, in order to complete the full set of affairs and processes within the purview of the Directorate for Agricultural Land.

The SCAP (Security Content Automation Protocol) project, financed from a World Bank loan, has also been planned.

In 2020, the Ministry of Agriculture, Forestry and Water Management also began implementing the PHRD Grant project “Building Agricultural Sector Capacity for Data-Based Decision-Making, which will be implemented over the course of 3 years, during which period software will be purchased to facilitate management of collected data and the process of reporting on agricultural policy and rural development.

1.4.4 e-Mining and e-Energy

E-MINING – The field of mining in the Republic of Serbia falls within the mandate of the Ministry of Mining and Energy. The following information systems containing data in this field have been developed in recent years:

Geological Information System of Serbia (GeolISS) – In the past ten years, the line ministry has worked on the development of the Geological Information System of Serbia (GeolISS) as a strategic project, built as an extension on the GIS software platform that is fully user-friendly, both in terms of system updating with new data and in terms of timely obtaining of necessary information on Serbia’s geological resources. The aim of GeolISS establishment is to enable digital archiving of digital data and information and provide a modern and efficient information basis for all activities involved in planning, designing and decision-making in the field of geology. Users of this system include the Serbian Geological Institute, the Ministry of Mining and Energy and the Faculty of Mining and Geology, while the web-based application makes it available to all interested institutions and citizens of the Republic of Serbia.

The web-based application is scheduled to be further developed and made publicly available online, whether on a commercial basis or with unlimited access; while this will commercialise the service, the benefits of this move will be reflected in increased usability of the system.

Central Information System for Geological Exploration and Mining (CIS GEM) – Under the project “IMIS - Integrated Management Information System”, the Ministry of Mining and Energy has developed and implemented the Central Information System for Geological Exploration and Mining (CIS GEM). The project has been developed on the GIS software platform, as a modern information system used for maintaining a cadastre of exploration and mining fields in the territory of the Republic of Serbia. The CIS GEM provides for the generation, classification, maintenance, presentation and distribution of numeric, descriptive and spatial databases on: approved geological explorations; certificates of reserves; mining approvals; cadastre of exploration and mining fields; cadastre of ore deposits and balance of mineral raw materials; cadastre of mining works and facilities; cadastre of mining waste and disused, rehabilitated and closed mines; archival documentation and approvals, licences and certificates etc. The web-based GIS application found on the Ministry’s website enables access and searching by public users, as a testament to transparency of the Ministry’s operations.

E-ENERGY – In addition to mining, the Ministry of Mining and Energy is also responsible for public administration affairs pertaining to the energy sector, energy policy and energy development planning. Information systems have been developed in this field as well, including:

Central Register of Pressure Equipment (CROPP) – Development of the Central Register of Pressure Equipment began in 2012 under the auspices of the Ministry of Mining and Energy. It is a database of pressure equipment and includes data on inspections and tests of pressure equipment carried out by designated bodies. In this way, the Ministry of Mining and Energy, which incorporates the Pressure Equipment Inspectorate, has complete access to information on the state of pressure equipment in the entire country, with the exact characteristics and location of each item of pressure equipment and with the possibility of searching pressure equipment data based on any criterion (e.g. municipality, equipment manufacturer, year of manufacture, equipment owner, type of pressure equipment or any other criterion). Last year, the CROPP was linked to the Business Register Agency's system.

Energy Management Monitoring and Implementation Information System (SEMIS) – The SEMIS is an information system used for monitoring energy management system implementation operated by the line ministry, which comprises data on the obligations of obligors in accordance with the Law on Energy Efficiency and Rational Energy Use. Furthermore, the system also collects and stores excerpts from energy inspection reports, as well as information on licensed energy managers and licensed energy advisors. In parallel with this, the SEMIS enables the Ministry to compile analytical reports on energy consumption and other parameters of the energy management system.

Information System for Energy and Water Consumption Monitoring and Analysis (ISEM) – The ISEM is an information system for energy and water consumption monitoring and analysis in public buildings. It is used for energy management purposes and is administered by the line ministry. The ISEM is intended primarily for monitoring and analysis of data on consumption and costs of energy, fuel and water in public buildings under the responsibility of local self-governments, provinces and the central government and is also used for the establishment of a national database on energy, fuel and water consumption in public buildings.

Integrated Management Information System (IMIS) – The IMIS is a database used for collecting and obtaining energy data relating to the production, imports, exports and consumption of energy and fuel in the territory of the Republic of Serbia and serves as the basis for the development of the Energy Balance of the Republic of Serbia. Data are collected electronically on a monthly and annual basis from energy operators in the fields of electricity, heating, renewables, coal, oil, oil products and natural gas. It is also used in the compiling of monthly Reports submitted by the Statistical Office of the Republic of Serbia to Eurostat in compliance with the EU Regulation 1099/2008 on Energy Statistics.

Information system for monitoring and verification of realized final energy savings – MVP (monitoring and verification platform) is an information system for systematic monitoring of energy savings as a result of implementation of plans and programs in the field of energy efficiency in accordance with the Law on Energy Efficiency and Rational Energy Use. The application is intended for online data entry from projects on energy efficiency measures and automatic calculation of energy savings, CO₂ emissions and investments by local governments and public institutions and companies.

1.5 ICT SECTOR

A key distinguishing feature of the ICT industry, apart from the fact that it has been the fastest-growing sector in the past 10 years, is its applicability across all other sectors.

The main characteristics of this sector are described in the “E-Bulletin” of the Electronic Communications and Information Society Association of the Chamber of Commerce and Industry of Serbia⁴, which covers employment, salaries, foreign trade and foreign direct investment.

Trends concerning the number of IT companies, the capital of the Serbian IT industry, exports of computer services and the state of play and outlook for start-ups in this field have been adapted from the survey *Development of the Information Technology Industry*.⁵

Employment – The total number of employees in electronic communication and information society industries in Q3 2020 according to SORS figures was 94,105, which was a 9.5% increase relative to the same quarter of 2019. Employees in the electronic communication and information society account for 4.4% of total employment. In terms of industrial activities, the highest share of employment was reported in computer programming, consulting and related activities (36,430), with a 13.7% increase. High numbers of employed persons were also reported in postal activities (18,239) and telecommunications (16,017). The lowest number of employees was reported in information services (4,470), where year-on-year employment growth was 20.3%. (source: *e-Bulletin of the Chamber of Commerce and Industry of Serbia*).

Salaries – Between January and October 2020, the highest average monthly salary was reported in computer programming, consultancy and related activities – RSD 212,093 (158.5% above the national average) and in the field of telecommunications – RSD 126,226 (53.8% above the national average). The lowest average monthly salary was reported in gambling and bookmaking – RSD 63,703, which was 22.4% below the national average; this activity also had the lowest year-on-year salary growth at 3.1%, with a 1.5% salary increase in real terms during the same period (source: *e-Bulletin of the Chamber of Commerce and Industry of Serbia*).

Foreign trade – According to the NBS figures, income generated from exports of computer, information and postal services in 2020 reached approx. EUR 1.5 billion (identical to the figure for the same period of 2019), of which 91.4% was generated from exports of computer services (approx. EUR 1.3 billion), while 6.7% was generated from exports of telecommunications services (EUR 96.7 million). Imports were also comprised mainly of computer services (75.7%, or EUR 409.0 million), with the total value of imports of telecommunications, computer, information and postal services reaching EUR 540.6 million in the same period. A surplus of EUR 909.4 million was reported (up 14.2% from 2019). According to the SORS figures, exports of computers, communication equipment and software in 2020 reached EUR 108.9 million, while imports stood at EUR 648.4 million, with an export-to-import ratio of 16.8%.

Foreign direct investment – According to the preliminary NBS figures, total net FDI inflow into Serbia from investment by non-residents in 2020 reached EUR 3,014.2 million. In 2020, the Information and Communications Sector generated net FDI inflow from investment by

⁴ E-bilten IV kvartal 2020, Privredna komora Srbije, Udruženje za elektronske komunikacije i informaciono društvo;

⁵ Razvoj industrije informacionih tehnologija, avgust 2019; Milovan Matijević, Mineco Computers

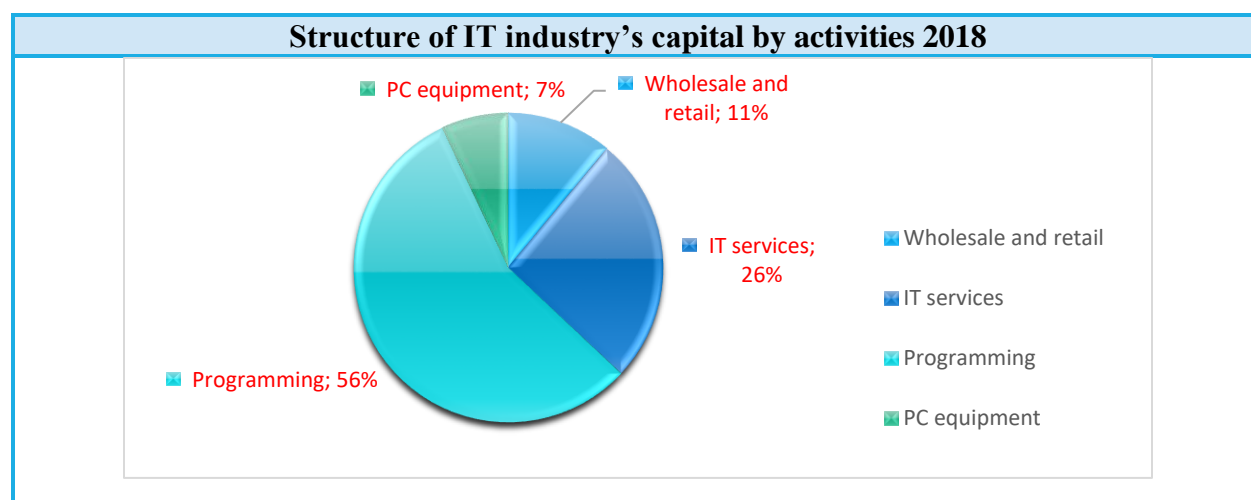
non-residents of EUR 41.8 million, while the Manufacture of Computers, Electronic and Optical Products received EUR 10.8 million in investment. (source: *National Bank of Serbia*).

Number of IT companies – In 2018 there were 2,349 active companies in Serbia with an individual annual income of more than one million dinars. In terms of business activities, the highest number was that of programming companies (1,483), which accounted for 63% of the total number. In terms of size, a majority of IT companies are micro businesses (with fewer than 10 employees), which accounted for 77.9%. On the other hand, only 11 companies were categorised as large (with more than 250 employees).

Relative to 2011, the total number of active IT companies in 2018 increased by nearly 700. Of more than 200 new companies registered each year, half of them (about 100) begin operating, while some 50 will either withdraw from the IT sector or file for liquidation due to bankruptcy or merger. New companies will emerge from new ideas, innovation, in incubators etc.

Effectively, it can be said that programming companies are the sole drivers of IT industry’s vitality. Following year after year of growth, the number of active companies currently stands at 1,483, which accounts for 63% of the total number – far more than 32% of the total number as reported in 2011 (source: survey *Development of the Information Technology Industry*).

Capital of Serbian IT industry – In 2018, the IT industry had EUR 674 million of own capital, with an annual growth of 16.0%. For the second consecutive year, IT industry’s capital has seen double-digit growth. Furthermore, relative to 2006, when own capital amounted to approx. EUR 150 million, Serbian IT industry is now worth 4 times more. This trend is spurred by foreign capital, which is already highly represented in the Serbian IT scene (source: survey *Development of the Information Technology Industry*).

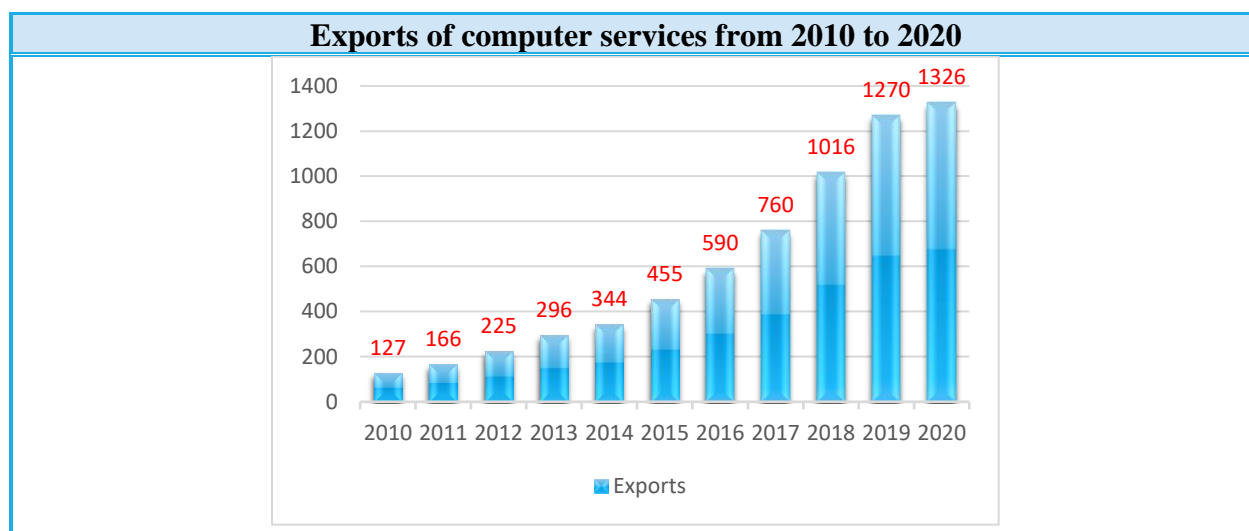


Programming companies have the highest capital – more than EUR 376 million – accounting for 56% of IT industry’s total capital. A distant second (EUR 173 million; 26%) is the IT services sector.

Of the 100 largest IT companies, nearly half are foreign-owned. Foreign companies bring international standards to the Serbian IT sector; however, this also requires adaptation and, in some

ways, localisation of foreign IT companies, if they wish to be successful in the Serbian IT market (source: survey *Development of the Information Technology Industry*).

Exports of computer services – Computer services are used globally as an indicator for international comparison between countries and their respective levels of technological development. Serbia’s domestic IT services market has been growing at an annual rate slightly higher than 10%, while on the other hand exports of computer services have grown at a rate of more than 30% per annum. This improves Serbia international image, from a country of cheap labour to a country with high-quality human capital (source: survey *Development of the Information Technology Industry*).



According to WTO figures, global exports of computer services between 2014 and 2017 increased at an annual rate of 10%, reaching EUR 300 billion in 2017. In 2014 Serbia ranked 40th, while 2016 figures ranked it 38th, and estimates for 2017 indicate it progressed further by one or two places. In comparison with the neighbouring countries, measured by the value of exports of computer services, Romania, Hungary and Bulgaria rank higher, while all other neighbouring countries rank below Serbia.

Serbia accounts for approx. 0.3% of global IT services exports and there is room for further growth; however, this will require IT experts, who are in short supply. For example, to reach EUR 2 billion in IT services exports, assuming the existing operating model, the sector will need to hire 30,000 additional IT experts (source: survey *Development of the Information Technology Industry*).

Start-ups: state of play and outlook – As regards start-ups, it can be said that the “start-up virus” is beginning to spread across Serbia, as evident from the fact that 188 programming companies had been registered in 2015, while 2017 already saw a significantly higher number of start-ups (253), followed by 281 in 2018; thus, it can be expected with a high degree of certainty that 2019 will set an all-time record with more than 300 programming start-ups. A majority of new companies are oriented towards the global market. However, starting a business is not all plain sailing, as evident from the fact that, out of the 749 programming companies formed from 2016 and 2018, 311 still have no employees and no income. In terms of conditions for growth, an even

more significant indicator is the fact that most Serbian IT enterprises take more than a decade to develop from a start-up to a large company. On average, every year about ten micro enterprises grow to become small enterprises, three small enterprises become medium-sized, while only one enterprise succeeds in becoming a large company with 250 or more employees (source: survey *Development of the Information Technology Industry*).

Challenges – It would appear that Serbia provides a sound foundation for starting a business in the IT industry, as it boasts a high-quality workforce; however, local workforce is capable of driving the growth of domestic companies only up to a certain level. On the other hand, foreigners come to this market primarily for the high-quality IT human resources, while all other sources of their growth are found outside of Serbia.

For these reasons, the largest battle between IT companies in the local market is for attracting appropriate workforce: until a year or two ago, they competed for the best experts, while currently they compete for the best interns, as labour demand exceeds by far the supply. In such a situation, salary figures become the main “competitive edge” of an employer, and in this regard capacity takes precedence over quality, with international companies still offering more attractive packages. This, in turn, answers the question why domestic IT companies grow at a slower rate than the foreign-owned ones, which also bring access to international markets and finished or semi-finished solutions. Foreign employers tend to aim for maximum productivity at a minimum cost, while the value added chain of their operations is usually located outside of Serbia (source: survey *Development of the Information Technology Industry*).

1.6 INFORMATION SECURITY

With the development of new technologies and services, which are increasingly provided electronically, there is an increased demand for stepping up the level of information security. In Serbian legislation, the concept of information security was primarily associated with the information security of ICT systems of special importance in accordance with the Law on Information Security; however, it is increasingly becoming an important segment for both citizens and businesses, coupled with growing awareness of its importance. However, information security risks affect both the government, specifically the ICT systems of special importance, and citizens and businesses, who bear the brunt of cybercrime attacks.

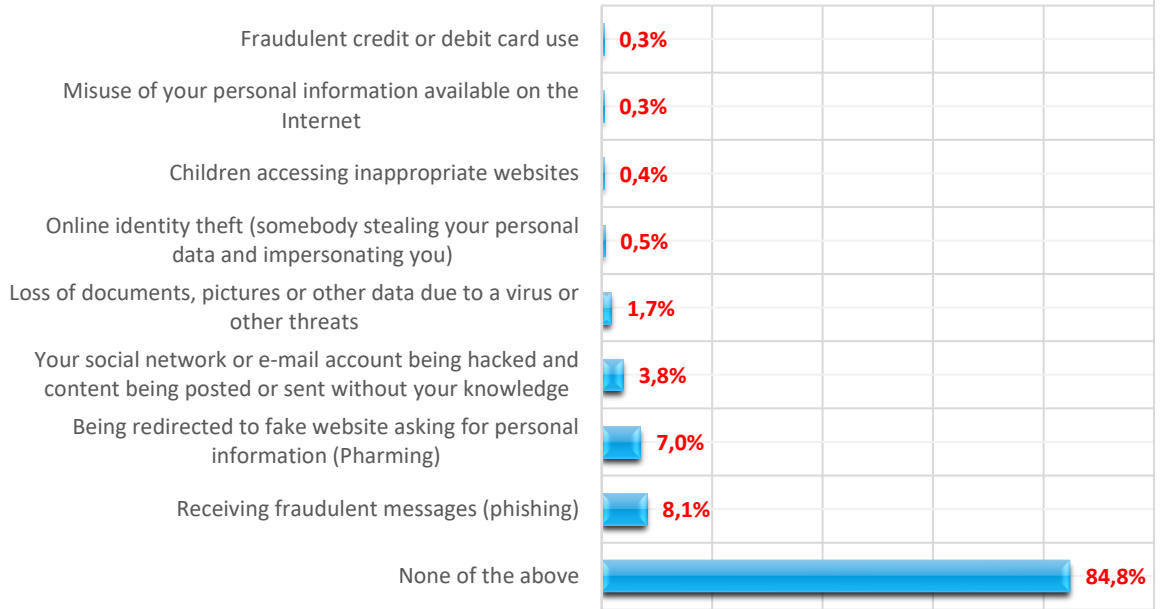
1.6.1 Information security of citizens

The module “Trust, Security and Privacy” in the SORS survey provides data on information security of citizens and the risks and threats to which they have been exposed.⁶

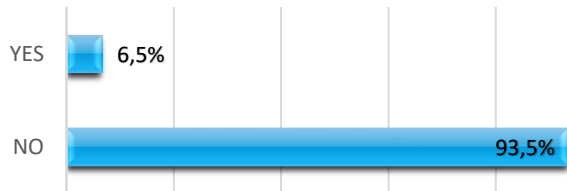
The survey asked the following four questions:

⁶ The source of data on e-skills is the publication of the Statistical Office of the Republic of Serbia *Usage of information and communication technologies in the Republic of Serbia, 2019*
<https://publikacije.stat.gov.rs/G2019/Pdf/G201916014.pdf>

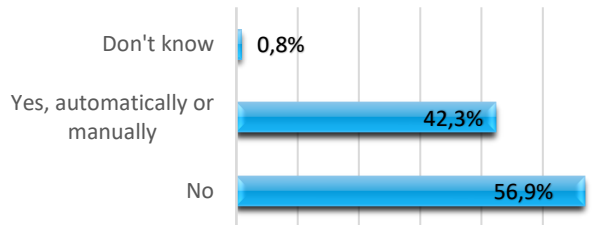
Have you experienced any of the following security-related issues when using the Internet for private purposes in the past 12 months?

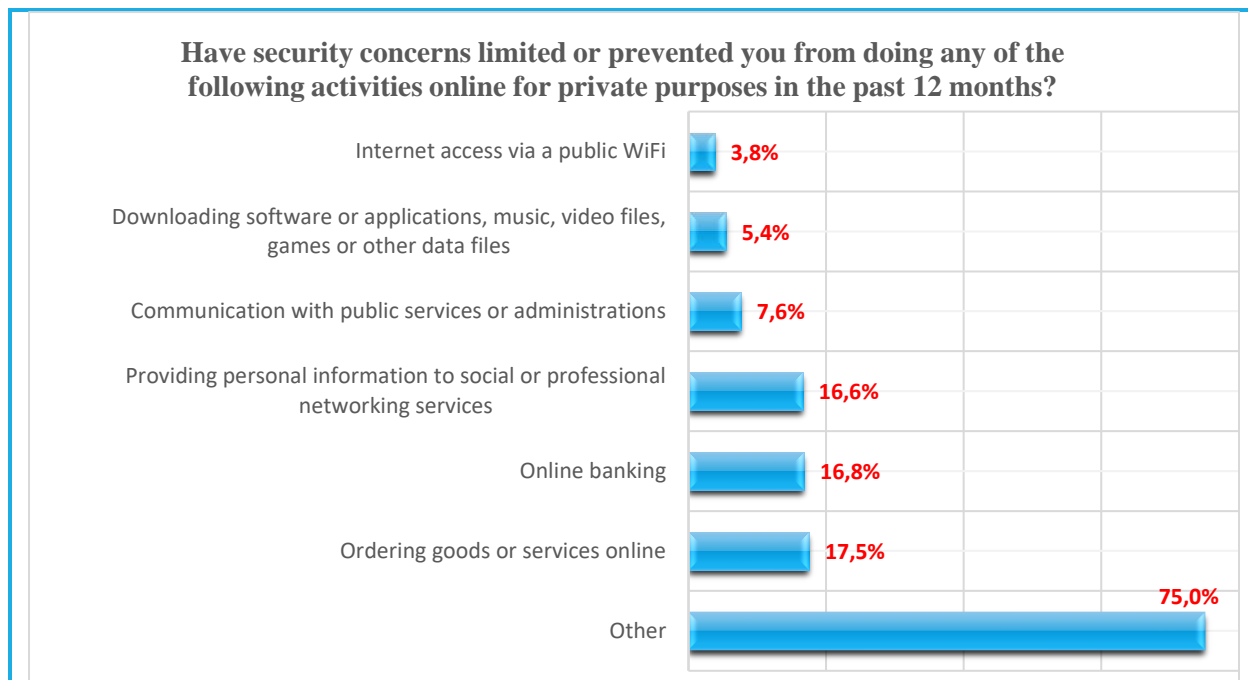


Have you experienced financial loss in the past 12 months resulting from identity theft, receiving fraudulent messages or being redirected to fake websites?



Do you make backup copies of you files on any external storage device or online (cloud services) for private purposes?





An analysis of survey results reveals that very few persons have experienced security-related issues online and, among those who did, the most common cases involved receiving fraudulent messages (8.1%) and being redirected to fake websites. Among the victims of identity theft, those who received fraudulent messages and those who were redirected to fake websites, 6.5% stated they had suffered financial loss as a result.

Furthermore, due to security concerns, 17.5% of respondents did not order goods or services online, 16.8% did not use online banking, and 16.6% did not provide personal information to social or professional networks.

As regards creating backup copies of files, 56.9% of respondents do not make backup copies, while 42.3% make backup copies, either automatically or manually.

Judging by the data presented above, it would appear that there is a strong case for raising citizens' awareness of information security. Namely, raising awareness of the risks and the ways to protect oneself online is essential to improve knowledge and promote the use of ICT, electronic services, online banking, e-commerce etc. In addition, a conclusion that can be drawn is that there is a clear correlation between digital competences and information security, corroborating the need to raise awareness and knowledge of these matters.

Information security of children – Information security of children in the Republic of Serbia was originally regulated by the Decree on Safety and Protection of Children when Using Information and Communication Technologies (hereinafter referred to as the “Decree”), while amendments and supplements to the Law on Information Security expanded its application to include also this subject matter.

The Law and the Decree set forth measures for the online safety and protection of children, which are implemented through the activities of the National Contact Centre for Online Safety for Children (hereinafter referred to as the “National Contact Centre”).

The National Contact Centre plays a key role primarily in the prevention and raising of awareness and knowledge of the advantages and risks of using the Internet and ways of using the Internet safely. Preventive measures for the online safety and protection of children are implemented through education and provision of information to children, parents and teachers by the National Contact Centre, as well as jointly with the competent authorities and institutions, schools, the media, civil and private sectors, academia, prominent individuals in modern art and creative industries and other stakeholders.

As of 31 December 2020, educators at the National Contact Centre held 394 presentations in primary schools for children and parents, which were attended by 14,667 pupils and 5,074 parents, and 12 education workshops in secondary schools for first- and second-year pupils. Since October 2020, they have also held 5 webinars/trainings for teachers, which were attended by 190 teachers.

A highly effective way of raising awareness of the risks involved in using the internet has been proven to be the media campaign implemented continually by the Ministry of Trade, Tourism and Telecommunications in collaboration with the public broadcasting service, which brings the subject matter of security closer to children, as well as their parents, in a way that is both entertaining and instructive.

Apart from prevention, the National Contact Centre is also the central point for reporting online security threats, which are then forwarded, depending on the type of threat to the child's rights and interests, to one of the relevant institutions: the Ministry of the Interior, the Office of the Special Prosecutor for Cybercrime, the Ministry of Education, Science and Technological Development, social work centres and medical centres.

As of December 2020, the total number of communications registered at the National Contact Centre since its formation via phone calls, e-mail, online reporting on the site and social networks is 20,050.

In 2016, the Ministry of Trade, Tourism and Telecommunications launched the school campaign "IT Caravan", which promotes the benefits of using the Internet and new technologies in education and warns against threats arising from their incorrect and unsupervised use. The "IT Caravan" was launched as part of the information society development platform entitled "Smart and Safe". The campaign has been implemented for three consecutive years and has comprised lectures, presentations, plays and competitions for fifth- and sixth-year pupils from 83 primary schools from all Serbian cities. It also featured programming and robotics workshops, with educational materials such as brochures and leaflets containing information and warnings against online threats distributed to pupils. More than 13,000 pupils participated in the programmes directly, while live online broadcasts were watched in 2018 by pupils from 800 schools, plus another 1,135 pupils competing in the pre-selection quiz in 2019. The campaign also included lectures for parents and, in addition to the events held at schools and cultural and sports centres, in technology hubs and at the Petnica Research Station, there were also promotional actions in city squares and in other communal areas.

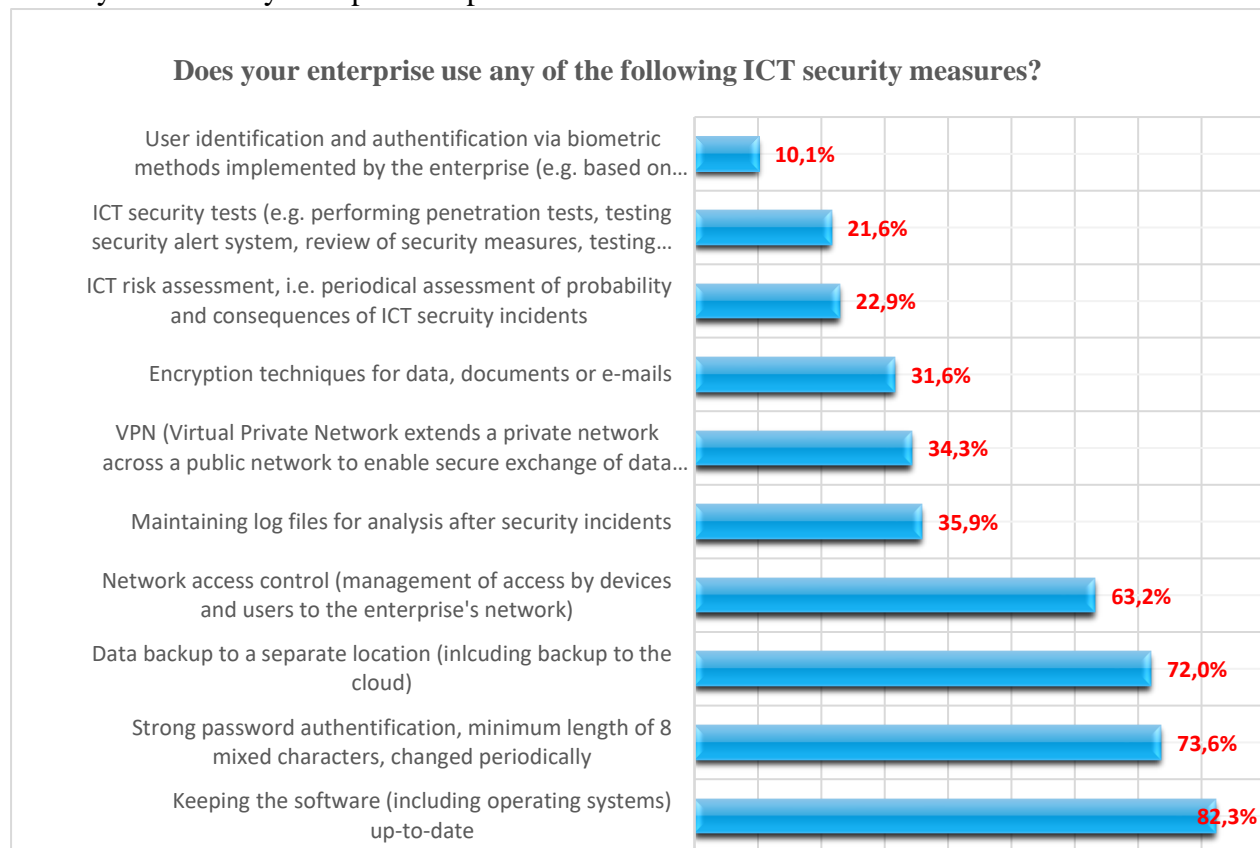
The comprehensive approach to the issue of information security of children taken in the Republic of Serbia, including the regulation of this area by laws and regulations, the establishment of preventive action mechanisms and identification of key stakeholders in this area, has proven itself as highly satisfactory, although it should be noted that further improvement in this area will

require additional capacity building of the National Contact Centre staff, improved cooperation between relevant institutions and provision of training to the staff of those institutions.

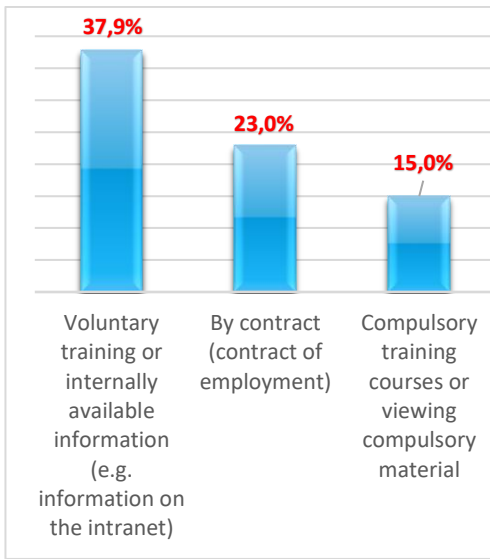
1.6.2 Information security of businesses

As regards information security of businesses, it should be noted that this group includes the so-called ICT systems of special importance, which are required under the Law on Information Security to implement security measures to maintain the information security of their systems at an appropriate level and reduce the risk of incidents, as well as those that are not subject to that Law, which means that the issue of information security is to them an issue of their awareness of the significance and importance of information security, especially in terms of consequences that may arise.

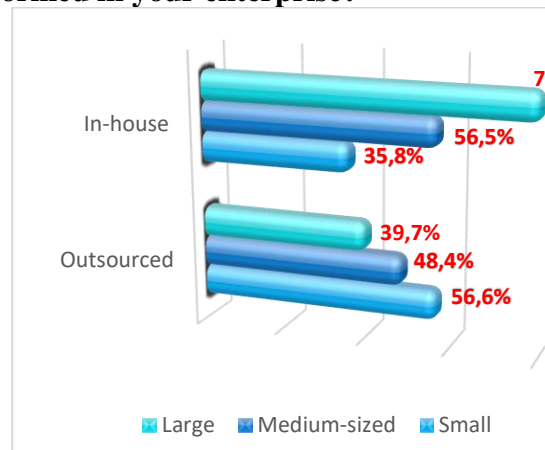
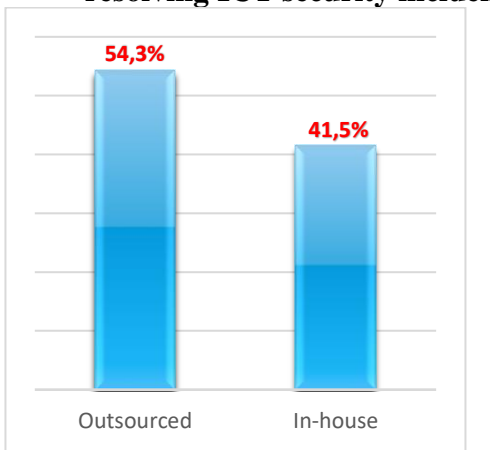
The “ICT Security” module in the SORS survey pertains to the application of certain security measures by enterprises to protect from incidents.



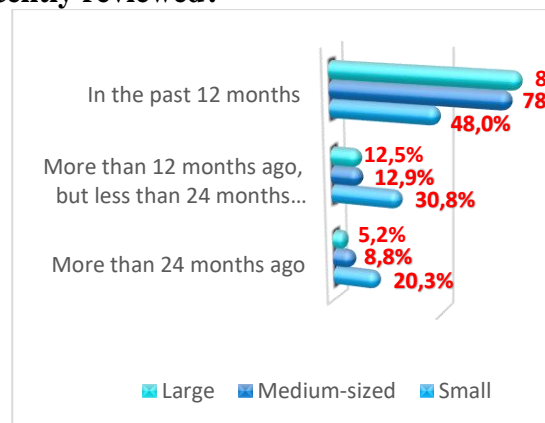
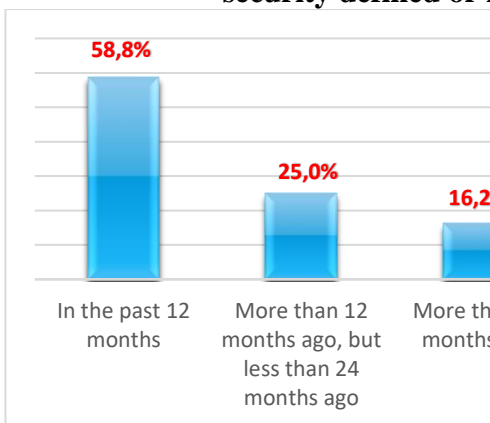
Does your enterprise make employees aware of their obligations in ICT security related issues in the following ways?

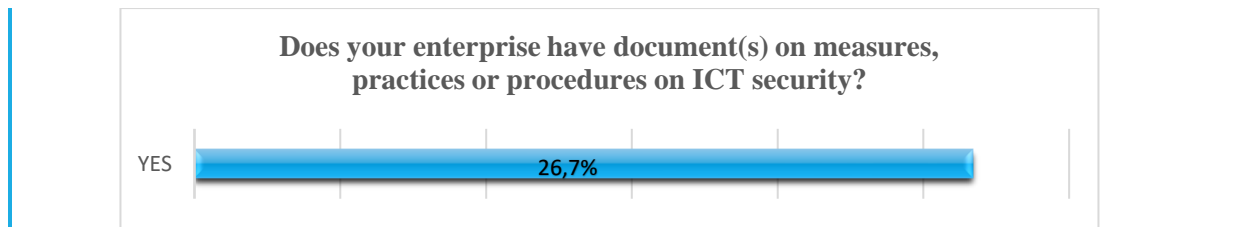


How are ICT security-related activities (security testing, ICT training on security, resolving ICT security incidents) performed in your enterprise?



When were your enterprise's document(s) on measures, practices or procedures on ICT security defined or most recently reviewed?





An analysis of data on whether enterprises employ any security measures reveals that a large percentage of companies employ measures relating to software maintenance (82.3%), strong password authentication (73.6%) and data backup to a remote site (72.0%). On the other hand, very few enterprises use biometric methods for user identification (10.1%), run ICT security tests (21.6%) and conduct assessments of ICT risk and consequences of ICT security incidents (22.9%). It is also noticeable that, in terms of enterprise size (small with 10-49 employees, medium-sized with 50-249 employees and large with 200 or more employees), ICT security measures are most commonly employed by large enterprises, while the share of small enterprises that do so is the lowest. This is probably due to the fact that large companies have greater technological and human resources capacities and are mostly categorised as ICT systems of special importance, which is why they have a duty to apply security measures in accordance with the law.

As regards making employees aware of ICT security issues, only 15.0% of enterprises require compulsory courses or compulsory view of material for employees, while 37.9% provide voluntary trainings or internally available information. The survey results indicate that 23.0% learn of ICT security issues through contract. Once again, in terms of enterprises size, most large enterprises provide compulsory and voluntary trainings, while most medium-sized enterprises make their employees aware of ICT security issues through their contract.

ICT system security activities are outsourced at 54.3% of all respondents, although it should be noted that, out of that percentage, small companies tend to outsource these activities more commonly than others, while outsourcing is the least common among small enterprises, which is understandable given that small, as well as medium-sized enterprises usually do not have employees hired specifically to ICT posts.

From the survey results it is evident that there is significant room for improving information security for small businesses. It is necessary in particular to focus the measures on small and medium-sized enterprises, especially with regard to staff capacity building and raising awareness of the fact that information security must be an indispensable part of everyone's business, regardless of the size of their enterprise or their industrial activity, to ensure incident prevention and protection.

1.6.3 Information security of ICT systems of special importance

Legislative framework – The Law on Information Security in the Republic of Serbia was first passed in 2016 in accordance with the then Draft Network and Information Security Directive, hereinafter referred to as the “NIS Directive”). The Law defines the term “information security” as a set of measures enabling the protection of data managed in an ICT system from unauthorised access and protecting the integrity, availability, authenticity and indisputability of such data so the system could operate as intended, when intended and under the control of authorised officers.

Thus, the Law regulates the information security of those information systems that have been recognised as ICT systems of special importance and must therefore be appropriately protected, which implies the employment of technical, organisational and human resources-related measures, as well as compliance with other statutory obligations regarding incident reporting, submission of statistical data, regular ICT system audits etc..

The Law, and also the accompanying secondary legislation passed the same year, regulates the following areas:

- Defining ICT systems of special importance;
- Defining security measures applicable to ICT systems of special importance;
- Establishment of the Information Security Coordination Body;
- Establishment of the National CERT, the CERT's of public authorities and the CERTs of independent ICT system operators;
- Defining of a list of incidents posing significant threats to information security and mandatory incident reporting,
- Establishment of the information security directorate,
- Cryptosecurity and protection from compromising electromagnetic radiation performed, and
- A possibility of establishing and recording special CERTs.

Application of the Law and secondary legislation – Given that the field of information security was first regulated by the law passed in 2016 and the accompanying secondary legislation, its application will require an extended period of time and has not yet been fully achieved.

Although application of the Law began immediately after its passing, it was found that legislative amendments and supplements would have to be made to ensure compliance with the NIS Directive which had been adopted in the meantime, as well as to improve some of the existing solutions with a view to more effective implementation of the Law in practice.

The amendments and supplements to the Law on Information Security adopted in October 2019 introduce novelties concerning the following:

- The National CERT, its powers and required capacities;
- Involvement of the National Bank of Serbia in the work of the Information Security Coordination Body;
- Establishment of the Record of Operators of ICT Systems of Special Importance;
- Introduction of the duty to submit statistical data on incidents occurring in the ICT systems of special importance on an annual basis;
- Cooperation of CERTs in the Republic of Serbia;
- Protection of children in the use of information and communication technologies;
- Classification of incidents and responses by the competent authorities depending on the threat level of each incident.

Challenges for information security – Regarding ICT systems and their protection, certain challenges still remain, including:

- 1) Application of security measures by ICT systems of special importance;
- 2) Capacities of the National CERT, the CERT's of public authorities and the CERTs of independent ICT system operators;
- 3) Capacities of the information security inspectorate;

- 4) Incidents posing significant threats to information security;
- 5) Public-private partnership;
- 6) International cooperation.

1) Application of security measures by ICT systems of special importance

The Law specifies which ICT systems are considered to be ICT systems of special importance, namely those system which, if severely compromised, could have consequences both for the functioning of the organisations that manage them and for the rights and interests of citizens and businesses, as well as for national and public safety.

ICT systems of special importance, in particular those operated by public authorities, face issues in the employment of security measures for various reasons, including:

- Lack of staff;
- Lack of staff with appropriate levels of knowledge;
- High employee turnover;
- Inadequate equipment;
- Insufficient management awareness of the importance of information security.

The same challenges are also faced by the ICT systems of special importance falling within the group of ICT systems performing activities of general interest that are mainly owned by the private sector (finance, energy, telecommunications etc.); however, the risks they face are certainly far less severe, as the risks of incidents in these systems can have consequences both in financial terms and in terms of inability to provide services to a large portion of the population, which is why the level of awareness in the case of these systems is much higher and they also enjoy greater management support in the application of security measures.

The World Bank report also states that “up-to-date technical security controls are deployed in all sectors of Serbia, although the level of implementation can vary depending on the sector or size of the establishment.” It is noted that in the public sector it is common practice to apply controls such as automatic software patching and anti-virus updating, firewall management, offsite storage of backups and physical security controls, as well as some limited use of intrusion detection systems. It is also noted that the networks are monitored for unapproved devices and workstations are secured so that users are unable to install unapproved software. “A similar environment exists in the private sector, although the variation in deployment is much greater. Financial, telecommunications and larger institutions deploy a much broader range of controls and exhibit a much deeper knowledge not only of the importance of these controls, but also have the skills and financial resources to deploy them. It was noted that mid-sized, and some smaller, enterprises outsource their ICT operations, and therefore depend on their provider to ensure the security of the environment.”

2) Capacities of the National CERT, the CERT’s of public authorities and the CERTs of independent ICT system operators

The National CERT was established in 2017 and its capacities have since been increased in terms of staffing level, equipment and premises. This is witnessed by the fact that the National

CERT has become a full member of FIRST (Forum of Incident Response and Security Teams), as the world's largest organisation in this field, with 520 members from 95 countries, aiming to connect the CERT teams worldwide and establish information exchange channels. In addition, the National CERT is also accredited on the Trusted Introducer list of CERTs from all over the world.

Investment in the capacities of the National CERT is still needed and it is expected that the newly-adopted provisions of the Law on Information Security pertaining to the capacity of the National CERT will drive further improvement of its operations.

In addition, it is paramount to build the capacities of the public authority CERT tasked with incident protection in the ICT systems of public authorities. A significant number of public authorities are considered to have ICT systems of special importance and are included in the Single e-Government Information and Communication Network and, in this context, it is crucial to establish information exchange mechanisms with the public authority CERT, as well as to improve its incident response capacities.

Independent ICT system operators are required under the Law to form a CERT to manage incidents in their systems. Recently, the CERT of the Ministry of the Interior achieved significant results in terms of international cooperation, becoming a full member of FIRST (Forum of Incident Response and Security Teams) and receiving accreditation on the Trusted Introducer list of CERTs worldwide. Since not all ICT system operators have formed their CERTs, it is necessary to provide optimum conditions and support their formation, including through support to the teams that have already been formed, such as the CERT of the Ministry of the Interior.

Since the Law provides that the National CERT, the CERT's of public authorities and the CERTs of independent ICT system operators are to maintain continual cooperation, this cooperation mechanism needs to be implemented to enable sharing of experiences and knowledge, as well responding to certain incidents. This includes in particular incidents of national importance, which is why it is necessary to establish cooperation protocols, designate contact persons, develop incident response procedures at all levels and hold regular exercises in this segment.

3) Capacities of the information security inspectorate

The Law on Information Security provides that the information security inspectorate shall be tasked with inspecting the application of the Law and the activities of operators of ICT systems of special importance. The Ministry of Trade, Tourism and Telecommunications hired an information security inspector in 2018; however, inspection activities did not begin until 2019. As of December 2020, 34 inspections have been inspected in total.

Given the number of ICT systems of special importance, it is clear that a single inspector is not sufficient to conduct the inspections, which is why it is impossible to verify whether the number of ICT systems compliant with the Law and the statutory security measures has increased.

4) Incidents posing significant threats to information security

The operators of ICT systems of special importance are required to report any ICT system incidents that can have significant impact in terms of information security breaches. These are effectively incidents that may cause disruptions in operations or in the provision of services or that

may affect a large number of services, a large number of users or a substantial part of the territory or that may affect public safety etc.

However, although incident reporting applies only to incidents that significantly breach information security, very few incidents have been reported in recent years.

One of the reasons for the low number of reported incidents is the fact that ICT systems of special importance avoid reporting incidents for fear that their reputation may be harmed, or do not know where incidents should be reported, or manage to recover from the incidents without assistance and thus decide not to report them at all.

To ensure proper incident reporting, it is necessary to first make the ICT systems of special importance aware of the importance of incident reporting, while also establishing trust between the ICT systems of special importance and the competent institutions, so the ICT systems of special importance could be certain that the incident data which they submit will not harm their operations.

5) Public-private partnership

Public-private partnership in the field of information security in Serbia exists in the form of an informal group which refers to itself as the Petnica Group. Namely, in mid-2015, the OSCE Mission to Serbia, the DiploFoundation and the Geneva Centre for Security Sector Governance (DCAF) established a strategic partnership with the Petnica Research Station and held a coordination meeting attended by key public and private stakeholders in the field of cybersecurity. The so-called “Petnica Group” emerged from this meeting and developed, through several stages, into an informal multi-stakeholder group on public-private cooperation, comprised of key national public and private sector stakeholders in the field of cybersecurity, academia and the civil society. From its very start, the Group focused on strengthening cooperation between public and private sectors and developing appropriate policies and strategic frameworks in the field of cybersecurity in the Republic of Serbia⁷.

As regards public-private partnership, the key challenge is finding an appropriate cooperation mechanism, which will link all relevant stakeholders, while enabling operational functioning. Namely, while the Petnica Group operated successfully in the past, its future functioning required a mechanism that would formalise this cooperation and include in it certain actors that have hitherto been excluded, but would make the group operational, as opposed to its largely advisory role in the past, and enable information exchange. The existing form of cooperation within the Petnica Group did not enable the execution of projects that required finance, which limited its performance and rendered it insufficiently operational. For these reasons, in 2020 the Petnica Group transformed itself into the Cybersecurity Network Foundation, and it is expected that, as a registered foundation, it will have access to funding for project implementation in the field of information security.

⁷ Vodič kroz informacionu bezbednost u Republici Srbiji 2.0 (A Guide to Information Security in the Republic of Serbia 2.0);

<https://www.osce.org/sr/mission-to-serbia/404258>

6) International cooperation

Institutions of the Republic of Serbia have had an active role in international activities in the field of information security, whether through bilateral cooperation or cooperation within the framework of international organisations, including the United Nations, the Organisation for Security and Cooperation in Europe, the International Telecommunication Union, the Global Forum on Cyber Expertise, the Geneva Centre for Security Sector Governance etc.

The Republic of Serbia has served a full term on the UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UN GGE) in its composition for 2016-2017. The Republic of Serbia has been a member of the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG) since its establishment in 2018 and actively participates in the Group's activities.

Since 2019, the Republic of Serbia has been a member of the Global Forum on Cyber Expertise (GFCE). In addition to the country's active role through membership in the above bodies, the Ministry of Foreign Affairs as one of the authorities responsible for performing activities in the context of development of international cooperation on information security matters, plans and holds bilateral contacts to promote and improve cooperation with other countries in this field and examines all initiatives relevant for information security at national and global levels. In this context, Serbia has also recognised the importance of the French initiative "Paris Call for Trust and Security in Cyberspace", which we have supported and in whose working groups we intend to actively participate (at present we are only a member of the first working group).

Serbia actively participates in the work of the Informal Working Group on cyber security formed under OSCE Decision No. 1039 and has designated its political and technical focal point for cooperation in case of cross-border incidents in accordance with Confidence Building Measure No. 8. The efforts made and the progress achieved in the field of cybersecurity have contributed to Serbia's acceptance, upon consultations with management of the Informal Working Group and the competent national institutions, of sponsorship of Confidence Building Measure No. 9, which concerns the development of a list of national terminology and definitions of terms in the field of information security. As a result of this activity, Serbia has developed a platform with more than 1000 terms and definitions taken from the legislation of Member States.

the Ministry of Trade, Tourism and Telecommunications, the Ministry of the Interior and the National CERT take part in implementation of the Geneva Centre for Security Sector Governance project "Improvement of Cybersecurity Governance in the Western Balkans", launched in July 2018, which aims to contribute to a more efficient and more responsible governance of cybersecurity in the Western Balkans and improve regional cooperation in this field.

The Ministry of Defence continually takes part in international military exercises aimed at establishing and developing information security and cyber defence. An example of such cooperation is the international cyberspace exercise "Cyber Tesla", which is implemented in cooperation with the public and private sectors of the Republic of Serbia with powers in the field of information security and with members of the National Guard of Ohio.

In 2019, the United Nations Office for Project Services (UNOPS), the Ministry of Trade, Tourism and Telecommunications of the Republic of Serbia, the Regulatory Agency for Electronic,

Communications and Postal Services (RATEL) and the Norwegian Ministry of Foreign Affairs, represented by the Embassy of the Kingdom of Norway in Belgrade, signed the Memorandum of Understanding on cooperation and strengthening of information security in the Republic of Serbia. The project is being implemented in 2020 and 2021 and encompasses support to the strategic and regulatory frameworks in the field of information security and development of recommendations for Serbia's critical information infrastructure and purchase and installation of a platform for information security exercises at RATEL.

2. CHANGE ACHIEVED BY THE STRATEGY

2.1 VISION AND DESIRED CHANGE

The use of information and communication technologies has become indispensable for all - citizens, public administration and businesses – and largely affects both our daily lives and the economy and the overall business environment. In this context, it is necessary to adapt to the changes stemming from the use of ICT and focus on harnessing it to achieve maximum benefits. With this Strategy we aim to achieve the following:

1. A digitalised public administration capable of efficiently and transparently providing services to citizens and businesses.
2. Improved digital skills of all citizens, who are able to freely use ICT both in their daily lives and in communication with public administration.
3. A transformation of the economy through digitalisation and support for the employment of information technologies towards modernising business operations across all industries.
4. An information security environment with a sufficient level of awareness of both risks and advantages of new technologies for citizens, public administration and businesses.

3. OBJECTIVES OF THE STRATEGY

3.1 OVERARCHING OBJECTIVE OF THE STRATEGY

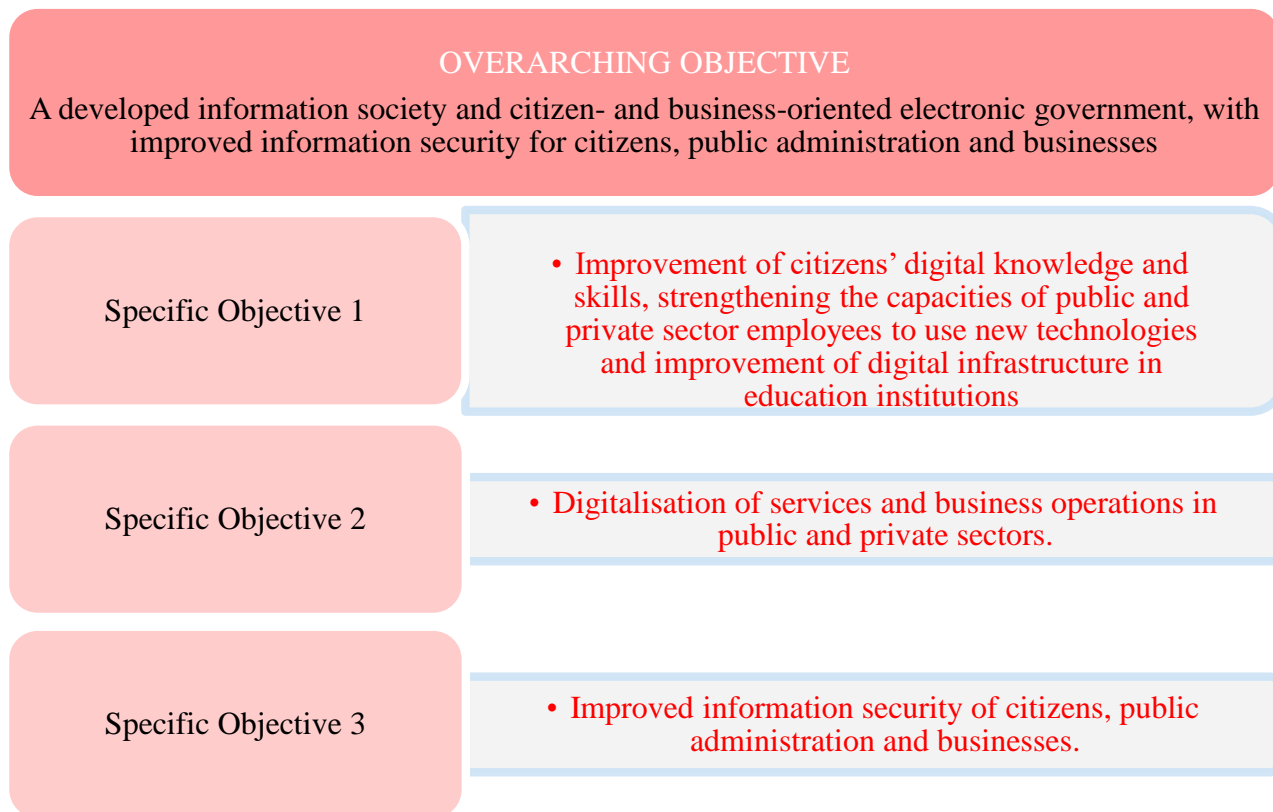
The fields of information society and information security are comprehensive and are applied in almost all fields and activities on which development of an economy and a society are based, and which at the same time relate to citizens, the public administration and businesses of a country.

The use of information systems in operations of the public administration and businesses is unavoidable, and it is necessary to protect devices, networks, data and also organisations and individuals in order to ensure appropriate security level for such systems.

The Overarching Objective of the Strategy is a developed information society and citizen- and business-oriented electronic government, with improved information security for citizens, public administration and businesses.

The Overarching Objective of the Strategy will be achieved through the following Specific Objectives:

- **Specific Objective 1:** Improvement of citizens’ digital knowledge and skills, strengthening the capacities of public and private sector employees to use new technologies and improvement of digital infrastructure in education institutions.
- **Specific Objective 2:** Digitalisation of services and business operations in public and private sectors.
- **Specific Objective 3:** Improved information security of citizens, public administration and businesses.



OVERARCHING OBJECTIVE	A developed information society and citizen- and business-oriented electronic government, with improved information security for citizens, public administration and businesses			
Indicators at the level of SPECIFIC OBJECTIVES	Baseline value in 2020	Target value in 2026	Verification source	
Specific Objective 1	Computer literate persons	34.2%	46%	Statistical Yearbook of the Republic of Serbia (SORS)

	Use of the Internet	Households	80.1%	90%	Usage of ICT Report (SORS)
		Individuals	78.4%	88%	
Specific Objective 2	<i>eGovernment EU benchmark</i>		43.75%	65%	<i>eGovernment Benchmark Report</i>
	Percentage of businesses that sold products and services on the Internet		27.9%	30.3%	Usage of ICT Report (SORS)
	Total exports of computer and information services		EUR 1,342 million	EUR 1,690 million	Balance of payments (NBS)
Specific Objective 3	Global information security index		58	30	Telecommunication Union report <i>Global Cybersecurity Index - ITU</i>

3.2. SPECIFIC OBJECTIVES AND MEASURES OF THE STRATEGY

Specific Objectives		Measures	
SO 1	Improvement of citizens' digital knowledge and skills, strengthening capacities of public and private sector employees to use new technologies and improvement of digital infrastructure in education institutions	Measure 1.1	Improvement of digital knowledge, skills and capacities of citizens and employees through trainings aimed at increased usage of ICT.
		Measure 1.2	Promotion of useful, creative and secure usage of information technologies through organisation of educational and media campaigns and prize competitions.
		Measure 1.3	Improvement and promotion of the work of the National Contact Centre for Child Safety on the Internet.
		Measure 1.4	Improvement of the digital infrastructure in educational institutions.
SO 2	Digitalisation of services and business operations in public and private sectors	Measure 2.1	Development of the information society
		Measure 2.2	Support to entry in foreign markets
		Measure 2.3	Digital transformation of MSMEs
		Measure 2.4	Development of e-business
		Measure 2.5	Strengthening capacities for usage of ICT in cultural institutions with the aim of developing and improving the IS and the basis for development of entrepreneurship in

			culture / creative industries (gaming, applications, multimedia guides...)
SO 3	Improved information security of citizens, public administration and businesses	Measure 3.1	Awareness rising and improvement of knowledge of information security for citizens, public servants and businesses.
		Measure 3.2	Strengthening capacities of the ICT systems of particular importance for application of safeguards.
		Measure 3.3	Strengthening capacities of the National CERT, govCERT and CERT of independent ICT operators.
		Measure 3.4	Strengthening capacities of the information security inspectorate.
		Measure 3.5	Promoting public-private partnership in the field of information security.
		Measure 3.6	Improvement of regional and international cooperation.

SPECIFIC OBJECTIVE 1

Improvement of citizens' digital knowledge and skills, strengthening capacities of public and private sector employees to use new technologies and improvement of digital infrastructure in education institutions

An important precondition for development of the information society and eGovernment is improvement of digital knowledge and skills of all citizens, strengthening the capacities of both public and private sector employees for the use of new technologies and improvement of the digital infrastructure in education institutions.

Development of digital skills is defined by the Strategy of Digital Skills Development in the Republic of Serbia for the period 2020-2024 (hereinafter referred to as the "Strategy of Digital Skills Development"), and is implemented through Specific Objectives, including:

- 1) Improvement of digital competencies in the education system,
- 2) Improvement of basic and advanced digital skills for all citizens,
- 3) Development of digital skills in accordance with the needs of the labour market, and
- 4) Lifelong learning for ICT experts

To achieve the objectives regarding development of digital skills it is, thus, necessary to start from the education system and ensure conditions for learning and acquiring digital competencies in the education system and to improve curricula and syllabuses accordingly for the purpose of acquiring digital competencies in pre-university education.

It is also necessary to accredit digital skills development programmes for citizens, particularly taking into account vulnerable categories such as the elderly, persons with disabilities, poor citizens and persons in rural areas, with continual citizens' awareness-rising of the need to adopt digital skills.

Digital skills are necessary for the majority of jobs and it is necessary to develop employees' digital skills, including employees in the public administration, and to recognise digital skills linked with specific features of each job.

Due to dynamic development of the ICT sector, it is necessary to keep up with the needs of this sector and the entire economy in terms of necessary digital skills, and also to continually work on the improvement of ICT experts and promotion of lifelong learning.

The aim of implementation of Specific Objectives and measures of the Strategy of Digital Skills Development is to improve the system which ensures higher citizens' digital skills through development of computational thinking, provision of skills necessary for everyday life and development of a successful career in the digital economy and ensuring conditions for further improvement of knowledge and skills of ICT experts.

Since the above Strategy includes the period from 2020 to 2024, upon expiry of that period a new programme will be passed, which will define objectives and measures in the field of digital skills development until 2026. Until a new programme is passed, measures set under the Strategy and additional measures indicated and set within this Specific Objective will be implemented.

Specific Objective 1		Improvement of citizens' digital knowledge and skills, strengthening capacities of public and private sector employees to use new technologies and improvement of digital infrastructure in education institutions		
Indicator		Baseline value in 2020	Target value in 2026	Verification source
Computer literate persons		34.2%	46%	Statistical Yearbook of the Republic of Serbia (SORS)
Use of the Internet	Households	80.1%	90%	Usage of ICT Report (SORS)
	Individuals	78.4%	88%	

Measures for Implementation of Specific Objective 1

In addition to measures specified under the Strategy of Digital Skills Development, other measures aimed at improvement of digital knowledge and skills and strengthening of skills will also be implemented within the framework of this Strategy.

Specific Objective 1. "Improvement of citizens' digital knowledge and skills, strengthening the capacities of public and private sector employees to use new technologies and improvement of digital infrastructure in education institutions" is implemented through measures, including:

- **Measure 1.1:** Improvement of digital knowledge, skills and capacities of citizens and employees through trainings aimed at increased usage of ICT.
- **Measure 1.2:** Promotion of useful, creative and secure usage of information technologies through organisation of educational and media campaigns and prize competitions.
- **Measure 1.3:** Improvement and promotion of the work of the National Contact Centre for Child Safety on the Internet.
- **Measure 1.4:** Improvement of the digital infrastructure in educational institutions.

Measure 1.1.

Improvement of digital knowledge, skills and capacities of citizens and employees through trainings aimed at increased usage of ICT

One of preconditions for popularisation and increased use of ICT in citizens' everyday life and communication with the public sector is education aimed at improvement of digital knowledge, skills and capacities of citizens and employees. In addition to formal education where digital competencies are acquired, it is necessary to increase the level of digital knowledge through trainings and support programmes, particularly for citizens in vulnerable categories and public servants.

Measure 1.1. is implemented through the following key activities:

- **Activity 1.1.1:** Support programmes for associations through award of funds for implementation of programmes in the field of development of the information society
- **Activity 1.1.2:** Trainings aimed at improving teachers' competencies in the field of information and communication technologies
- **Activity 1.1.3:** Development and implementation of trainings aimed at improving digital competencies of employees in the public administration
- **Activity 1.1.4:** Popularisation and promotion of the use of ICT through the Serbian-Korean Information Access Centre

Measure 1.1. Informational and educational measure	Improvement of digital knowledge, skills and capacities of citizens and employees through trainings aimed at increased usage of ICT		
Implementing agency	Ministry of Trade, Tourism and Telecommunications Ministry of Education, Science and Technological Development Ministry of Public Administration and Local Self-Government National Academy for Public Administration		
Indicator	Baseline value in 2019	Target value in 2026	Verification source
1.1.1 Number of approved support programmes	41	50	MTTT
1.1.2 Number of trained teachers	34,500	45,000	MTTT MESTD
1.1.3 Number of trained employees	1.543	3.500	MTTT
1.1.4 Number of trainings held at the Serbian-Korean Information Access Centre	400	350	MPALSG

Measure 1.2.

Promotion of useful, creative and secure usage of information technologies through organisation of educational and media campaigns and prize competitions

To increase the use of information technology, it is necessary to continually raise awareness of the importance and usefulness of the use of ICT, which must be implemented together with

education on safe use of ICT, through campaigns intended for special categories of individuals (children, parents, teachers, girls).

Measure 1.2. is implemented through the following key activities:

- **Activity 1.2.1:** IT Caravan – an educational campaign for promotion of useful, creative and secure usage of information technologies
- **Activity 1.2.2:** Popularisation and promotion of the use of ICT in classes through a prize competitor titled “Digital Class”
- **Activity 1.2.3:** Promotional campaign “Smart and Safe” (the Girls in ICT Day, the Safer Internet Day, the European Programming Hour, the Information Society Day...)

Measure 1.2. Informational and educational measure	Promotion of useful, creative and secure usage of information technologies through organisation of educational and media campaigns and prize competitions.		
Implementing agency	Ministry of Trade, Tourism and Telecommunications		
Indicator	Baseline value in 2019	Target value in 2026	Verification source
1.2.1 Number of children who attended educational debates	2,000	3,000	MTTT
1.2.2 Number of works published in the electronic compendium “Digital Class”	1,835	3,000	MTTT
1.2.3 Number of events held	6	10	MTTT

Measure 1.3.
Improvement and promotion of the work of the National Contact Centre for Child Safety on the Internet

With the aim of continuing prevention and awareness-rising and improvement of knowledge of advantages and risks of the use of the Internet and safe use of the Internet, it is necessary to continue strengthening the capacities of the National Contact Centre for Child Safety on the Internet, particularly employees in institutions which apply regulations providing for child safety on the Internet, and also continual provision of information to and education of children, parents and teachers in this field.

Measure 1.3. is implemented through the following key activities:

- **Activity 1.3.1:** Trainings aimed at strengthening the capacities of employees in institutions of the system for the purpose of applying of the Regulation on Safety and Protection of Children in the Use of Information and Communication Technologies
- **Activity 1.3.2:** Provision of information to and education of children, parents and teachers in child safety on the Internet through organisation of trainings in schools

Measure 1.3. Informational and educational measure	Improvement and promotion of the work of the National Contact Centre for Child Safety on the Internet		
Implementing agency	Ministry of Trade, Tourism and Telecommunications		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
1.3.1 Number of trained employees	626	900	MTTT
1.3.2 Number of informed children, parents and teachers	20,000	23,000	MTTT

Measure 1.4
Improvement of the digital infrastructure in educational institutions

As regards digital infrastructure, the Ministry of Trade, Tourism and Telecommunications successfully completed the first stage of the “Connected Schools” project, through which free of charge, reliable and secure access to the Internet and to the Academic Network of the Republic of Serbia (AMRES) and Pan-European Academic Network (GEANT) and the content and services they offer was provided to the majority of approximately 1,700 central school facilities in Serbia. The second stage of the “Connected Schools” project which will be implemented in the period from 2019 to 2021 will include comprehensive improvement of the information and communication infrastructure in all primary and secondary schools in Serbia.

Also, in addition to the needs of primary and secondary schools, it is necessary to work quickly on understanding and providing the necessary digital infrastructure and services that would be purposefully used for the needs of higher education and scientific research activities. Regular cycles of infrastructure improvement are not enough to neutralize the existing digital divide for developed European countries. Given that these needs require significant financial resources, a proactive approach is needed to provide them, which would contribute not only to preserving the value of previous investments, but also to preventing the creation of new technological differences between the Republic of Serbia and developed European countries in relations to national research and education networks. The importance of rapid action lies in the fact that by the end of 2021 in the Republic of Serbia a GEANT hub will be formed with a capacity of several terabytes per second with AMRES access link of 100 gigabytes per second, making the Republic of Serbia an important point on the map. In order to take full advantage of this opportunity, it is necessary to work intensively not only on further development of the computer network, but also on the implementation of high-tech solutions in the field of cloud infrastructure and high-performance data processing (so-called supercomputing) as soon as possible.

Measure 1.4. is implemented through the following key activities:

- **Activity 1.4.1:** Continuation of connection of all central primary and secondary school facilities, cultural institutions and public libraries in Serbia to the AMRES network
- **Activity 1.4.2:** Development of the information and communication infrastructure in primary and secondary schools within the “Connected Schools” project.

Measure 1.4. Subsidy	Improvement of the digital infrastructure in educational institutions		
Implementing agency	Ministry of Trade, Tourism and Telecommunications AMRES		
Partner	Ministry of Education, Science and Technological Development		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
1.4.1 Number of schools, cultural institutions and public libraries connected to the AMRES network	1,938	3,500	AMRES
1.4.2 Number of schools to which wireless communication infrastructure was provided	900	1,830	MTTT

Analysis of Effects of Measures for Implementation of Specific Objective 1

The analysis of the impact on the society – Implementation of the above measures contributes to the society by contributing to the improvement of digital knowledge and skills of citizens, employees and unemployed persons and by training them to adjust to new conditions resulting from unavoidable use of new technologies in everyday life, at work or in communication with the public administration. Training the majority of the population to use ICT ensures shift from classic to e-business and faster acting of the public administration and other electronic service providers. On the other hand, development of the digital infrastructure, particularly in educational institutions, will ensure reliable and safe internet access in all teaching and administrative rooms and for all participants in the education system, which will largely affect the quality of work and the possibility for unobstructed work in the digital environment.

The analysis of management capacities – Implementation of the measures requires further improvement of administrative and technical capacities at the Ministry of Trade, Tourism and Telecommunications, the Ministry of Education, Science and Technological Development and the Ministry of Public Administration and Local Self-Government, to ensure that educational programmes intended for improvement of digital knowledge and competencies are at the appropriate level and that they meet the needs in this field, as well as to ensure unobstructed implementation of digitalisation of the infrastructure in educational institutions.

The analysis of economic effects – Implementation of the measures contributes to improvement of productivity of the workforce in the Republic of Serbia and to ensuring adjustment to changes in the society and business operations conditioned by the use of new technologies in all segments of the society.

The risk analysis – Improvement of digital knowledge and skills is implemented through educational and promotional activities carried out by employees in competent institutions and the main risk for their implementation are capabilities of such human resources. To prevent the risk, it is necessary to plan activities which will support continual advancement of employees, particularly if upgrading of their knowledge is required for the use of new technologies and transfer of new knowledge to target groups included in the Specific Objective 1.

SPECIFIC OBJECTIVE 2

Digitalisation of services and business operations in public and private sectors

To ensure the shift from classic to e-commerce, it is necessary to digitalize the entire society, i.e. both public and private sector, through digitalisation of services and business operations. The importance of digitalisation of all segments of the society was best seen during the COVID-19 pandemic, due to which those parts of the society that did not previously shift to electronic operations suffered and are still suffering consequences, while on the other hand digitalisation and electronic operations proved to be able to fully or partially replace traditional manners of work or schooling.

As regards the public administration, the generally accepted principle of public administration development in modern systems is development of the efficient government, as the citizens' service, through introduction of electronic services, which is defined in the eGovernment Development Programme in the Republic of Serbia for the period from 2020 to 2022, and is implemented through Specific Objectives, including:

- 1) Development of infrastructure in eGovernment and provision of interoperability
- 2) Improvement of legal certainty in the use of eGovernment
- 3) Increasing availability of eGovernment for citizens and businesses through improvement of customer services
- 4) Opening data in public administration.

In addition to the above, digitalisation and provision of public administration electronic services are planned under a number of strategic enactments relating to e-judiciary, e-education, e-health, e-culture, e-business, e-commerce, e-tourism, e-construction and e-agriculture.

Overview of fields, activities and strategic documents

Field	Activities	Strategic document
e-Judiciary	Improvement of the ICT system through significant investment in infrastructure and improvement of software and improvement of human resources; Ensuring unified acting in the entire judicial system in terms of entering and exchange of data in the ICT system, which also implies training in this field for all users of the ICT system; Continual improvement of data exchange between authorities within the judicial system and with other state authorities; Improvement of the usage of the existing capacities, through improvement of the efficiency of case management and ensuring a possibility of real monitoring of the duration of judicial proceedings; Development of an internal prosecutorial practice database, availability of the database in all prosecutor's offices and linking with the database of the Judicial Academy (e-Academy) and the case law database;	Judicial Development Strategy

Field	Activities	Strategic document
	<p>Creating the normative framework and undertaking other measures with the aim of improving ICT security;</p> <p>Further improvement of the transparency of work of judicial authorities and judicial professions using ICT tools;</p> <p>Further expanding of possibilities for electronic institution and conducting of judicial proceedings for lawyers and citizens using the eCourt app or through other commercial software on the market using the Application Programming Interface technology, in compliance with the statutory standards;</p> <p>Further opening of judicial data appropriate for publishing on the national open data portal in compliance with positive legislation on personal data protection.</p>	
e-Education	<p>Development and application of the Single Education Information System (SEIS)</p> <p>Improvement of the infrastructure of educational institutions for information and communication technologies (ICT)</p> <p>Improvement of digital capacities of institutions in pre-university education</p> <p>Improvement of digital competencies of employees in education</p> <p>Implementation and promotion of innovative pedagogical approaches which imply integration of ICT in the teaching and learning process</p> <p>Introduction of the system for continual monitoring of digital education development</p> <p>Development of pupils' digital competence</p> <p>Establishing the digital environment for development of open education resources, digital services and supporting teaching and learning material</p>	Strategy for the Development of Education and Science
e-Health	<p>Electronic medical records – medical records which enable exchange of all medical data in connection with patients vertically within the health network and provide physicians insight in all patient's medical documentation</p> <p>e-POS – the system for electronic reporting of death within which data are submitted to registrars for registration with the register of deaths and to the Institute for Public Health “Batut” and the Statistical Office of the Republic of Serbia.</p> <p>e-Sick leave</p> <p>Extending e-prescriptions to medical technical aids</p> <p>Platform for consultations between physicians and patients by phone</p>	

Field	Activities	Strategic document
e-Culture	<p>Normative enactments in the field of digitalisation which provide for duties and competences of cultural institutions and participants in the digitalisation process include:</p> <ul style="list-style-type: none"> - The Regulation on Single Technical and Technological Requirements and Procedures for Keeping and Protection of Archiving Material and Documentary Material which will define procedures for e-archiving and permanent keeping of electronic documents, formation of the e-archive and adjustment of the archive material digitalisation process and the existing Single Software Solution in Archives (ARHIS) with e-archive. - The aim of the Guidelines for Digitalisation of the Cultural Heritage of the Republic of Serbia is to define technical standards and metadata for uniform and interoperable implementation of the cultural heritage digitalisation process in the Republic of Serbia. Adoption and implementation of the Guidelines will ensure uniformity in the work in conservation institutions in the digitalisation process. - Passing of the Instrument on Security of ICT Systems in Cultural Institutions is planned, which would include all safeguards set under the Law on Information Security. The model should be adjusted in accordance with specific features and the actual situation in the security system should be defined and the current situation should be adjusted to recommendations and standards set under the Law and regulations. 	<p>Government's Resolution 05 number: 6-213/2021-1 Strategic Priorities of Culture Development in the Republic of Serbia from 2021 to 2025</p>
	<p>Introduction and development of new services on the artificial intelligence platform used for data sets available at Single Software Solutions databases in the field of culture;</p>	
	<p>Networking of the existing and development and upgrading of single software solutions intended for museums, archives, libraries and institutes for protection of cultural monuments;</p>	
	<p>Strengthening capacities of cultural institutions in the digitalisation process through procurement of modern technical equipment and hiring people on digitalisation tasks.</p>	
e-Business	Bringing the legal framework in compliance with the regulation providing for e-government and e-business	eGovernment Development Programme

Field	Activities	Strategic document
	Improvement of the legal framework and the practice of the use of eSignature and eSeal within the public administration	
	Development of e-Business	Information Society and Information Security Development Strategy
e-Commerce	Eliminating offer and demand obstacles in the e-commerce market	Program for the Development of E-Commerce
	Strengthening infrastructure in e-commerce;	
	Improvement of the legislative and institutional frameworks in the field of e-commerce	
e-Tourism	Introduction of the central information system in the field of hospitality and tourism (e-Tourist)	Tourism Development Strategy
e-Construction	Continual activities on maintenance of the Central Register of Energy Passports (CREP) - a database on energy passports, energy efficiency engineers and authorised organisations.	
	Introduction of the single system of spatial planning indicators in accordance with the ESPON system;	
	Introduction and development of the information system on the spatial situation for the purpose of preparation of annual reports on achievement of the continual activity on maintenance of the Central Register of Energy Passports (CREP)	
	Development and improvement of the Central Records of Unified Procedures system (system for e-building permits)	
e-Agriculture	Development of all types of analytical and information systems for support to agriculture, including missing parts of agricultural statistics, public reporting and forecasting service systems, market information, registers etc.	Strategy for Agriculture and Rural Development
	Digitalisation of subsidies award to farmers using the IACS system (Directorate for Agrarian Payments)	IACS system introduction project
	Upgrading the existing information system for development and implementation of the Annual Programme for Protection, Cultivation and Use of Agricultural Land by all local self-government units (Directorate for Agricultural Land)	
	Implementation of the SCAP project (content security protocol)	
e-Mining and	Further development of the web application GeolISS of the information system through defining of public, commercial or unlimited Internet access	
	Development of new functionalities of the CISGIR information system	
e- Energy	Continual annual improvements of the CROPP Register	

Field	Activities	Strategic document
	Development of new functionalities of the SEMIS and ISEM information systems	
	Development of new functionalities of the IMIS information system	

It is also necessary to develop the use of ICT in the private sector, mainly with the aim of improving and digitalising business operations, and this was recognised in many fields and, accordingly, in various strategic documents of the Republic of Serbia, including:

- The Smart Specialisation Strategy in the Republic of Serbia for the period from 2020 to 2027;
- The Industrial Policy Development Strategy from 2021 to 2030;
- The Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period from 2020 to 2025;

The Smart Specialisation Strategy in the Republic of Serbia for the period from 2020 to 2027 recognised two priority fields in the ICT sector, including:

- 1) Development of tailored software, and
- 2) Development of own products

The importance of developing customised software and the development of own products is witnessed by the fact that those are new solutions which include application of big data and business analytics, cloud computing, the Internet of Things, installed systems, artificial intelligence and blockchain technology. Solutions which should be developed in the field of information and communication technologies to improve the work of state authorities and passing of strategic decisions are crucial. In the field of information and communication technologies, the entrepreneurial discovery process highlighted a need for providing the state-of-the-art technologies to capacities for education of human resources and forming additional innovation and research business parks for ICT companies and starts-ups.

The implementation of the above priorities is expected to result in establishing the Republic of Serbia as a source of sophisticated high technology products and services for the global market.

The Industrial Policy Development Strategy in the Republic of Serbia from 2021 to 2030 defined the Specific Objective “Improvement of Digitalisation of Industrial Production Business Models” and through implementation of planned measures aims to achieve digitally transformed industry of the Republic of Serbia which, together with other measures under the Industrial Policy Development Strategy, strongly supports economic growth and improves the quality of life of its citizens.

A Specific Objective of the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period from 2020 to 2025 titled “Development of Economy Based on Artificial Intelligence” includes implementation of measures aimed at successful adjustment of the economy to new business models and new market expectations with marked development of economic operators whose business operations are based on application of artificial intelligence.

It can be concluded that development of the ICT sector in accordance with the existing strategic documents is based on several pillars, including:

- 1) Development of companies and products in the field of information technologies;

- 2) Digitalisation of business operations in all economic activities using ICT;
- 3) Development of economy based on the use of artificial intelligence;
- 4) Development of digital skills for the needs of the labour market and strengthening the human resource potential of ICT experts.

Specific Objective 2	Digitalisation of services and business operations in public and private sectors		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
<i>eGovernment EU benchmark</i>	43.75%	65%	<i>eGovernment Benchmark Report</i>
Percentage of companies which sold products and services on the Internet	27.9%	30.3%	Usage of ICT Report (SORS)
Total export of computer and information services	EUR 1,342 million	EUR 1,900 million	Balance of payments (NBS)

Measures for Implementation of Specific Objective 2

In addition to measures implemented through sectoral and inter-sectoral public policy documents, other measures will also be implemented aimed at digitalisation of services and business operations within this Strategy.

Specific Objective 2 “Digitalisation of services and business operations in public and private sectors “ is implemented through measures, including:

- **Measure 2.1:** Development of the information society
- **Measure 2.2:** Support to entry in foreign markets
- **Measure 2.3:** Digital transformation of MSMEs
- **Measure 2.4:** Development of e-business
- **Measure 2.5:** Strengthening capacities for usage of ICT in cultural institutions with the aim of developing and improving the IS and the basis for development of entrepreneurship in culture / creative industries (gaming, applications, multimedia guides...)

Measure 2.1.

Development of the information society

Taking into account that the concept of the information society is comprehensive and relates to various segments, it is necessary to continually cooperate with all relevant actors through organisation of expert and other meetings, domestic or international, to keep up with new trends and exchange experts’ opinions on topics in the field of the information society.

One of the topics which is becoming increasingly relevant relates to data, or more specifically to data management. Many countries are starting to recognise the importance of data and their value in the economic sense, and, for example, Hungary founded the National Data

Management Agency to address this issue systematically. Thus, in order to keep up with the world, it is necessary not only to recognise Serbia’s approach in this field, i.e. to assess the needs, possibilities and risks for various data management models in our country; instead, it is also necessary to identify data of relevance for increasing transparency and citizens’ trust in services based on new technological solutions.

Measure 2.1. is implemented through the following key activities:

- **Activity 2.1.1:** Organisation of expert and other meetings in the field of information society within the Internet Governance Forum (IGF)
- **Activity 2.1.2:** Needs assessment for introduction of the data management system in the Republic of Serbia
- **Activity 2.1.3:** Analysis of readiness and needs of businesses for application of new technologies in business operations

Measure 2.1. Subsidy	Support to development of innovation		
Implementing agency	Ministry of Trade, Tourism and Telecommunications Serbian National Internet Domain Registry Foundation Chambers of Commerce		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
2.1.1 Number of meetings held	0	2	MTTT RNIDS
2.1.2 Analysis developed	0	1	MTTT
2.1.3 Analysis developed	0	1	Chambers of Commerce

Measure 2.2.
Support to entry in foreign markets

The domestic ICT sector undoubtedly has a large potential, but it is important that domestic economic operators are also presented in foreign markets and to ensure the increase of export of their products and services on those markets.

The Centre for Organisation of Fairs, Performances and Events of the Chamber of Commerce and Industry of Serbia organizes international fairs in foreign countries, which are always used as an instrument of business and development policy and constitute the specific framework for promotional, expert and commercial meetings of economic operators in Serbia.

With the aim of promoting and internationalising business operations of economic operators, the Chamber of Commerce and Industry of Serbia, in cooperation with the Development Agency of Serbia and other partners, organizes joint exhibitions of domestic companies in international fairs abroad.

One of the manners to promote the ICT sector is organisation of joint bodies for bilateral cooperation, which constitute a mechanism for promotion of export of Serbian products and services, including IT products and services.

Measure 2.2. is implemented through the following key activities:

- **Activity 2.2.1:** Support to economic operators for entry in foreign countries
- **Activity 2.2.2:** Organisation of meetings of joint bodies for bilateral economic cooperation (committees, commissions, working groups, business councils) in the field of IT with the aim of promoting export of domestic IT products and services
- **Activity 2.2.3:** Support to economic operators for participation in business delegations

Measure 2.2. Subsidy	Support to entry in foreign markets		
Implementing agency	MTTT		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
2.2.1 Number of events organised in foreign countries	6	12	CCIS RAS
2.2.2 Number of organised meetings of joint bodies for bilateral economic cooperation in the field of IT	10	15	MTTT
2.2.3 Number of events organised in Serbia	12	20	CCIS

Measure 2.3.
Digital transformation of MSMEs

To ensure the existing economic operators can develop and remain competitive in the market, it is necessary for them to continually develop and keep up with development of information technologies and recognise the importance of the use of new technologies in their business operations.

The Chamber of Commerce and Industry of Serbia founded the Centre for Digital Transformation (CDT) – a national hub of innovative practices targeted primarily towards micro, small and medium-sized enterprises.

The Centre for Digital Transformation ensures efficient and transparent digital transformation of the Serbian economy – through educations, counselling and creation of strategic partnerships with technology providers, on the one hand, and companies which would apply these solutions in their business operations, on the other hand.

The CDT has so far implemented three programmes aimed at enabling companies in the SME sector in Serbia and Republic of Srpska to improve their business operations according to the available digital trends (“Digital Transformation Support Programme for MSMEs-2019-2020”) and also to efficiently respond to new challenges in business operations caused by the COVID-19 pandemic. (*SPEED 1.0* and *SPEED 2.0*)

One of the conditions for development of innovation of small and medium-sized enterprises in the field of ICT is access to sources of financing necessary for research and development which will eventually result in development of products with a potential for placement on the global market. Financial support for development of innovation of small and medium-sized enterprises in

Serbia is available through the Innovation Fund, which is, as a national organisation, specialised for provision of support to innovation activity and management of financial funds for stimulation of innovation development.

Programmes of the Innovation Fund are intended for small and medium-sized enterprises, specifically those at early stages of development and at growth stages, as well as for cooperation with research and development organisations. In addition, by awarding innovation vouchers, the Innovation Fund supports small and medium-sized enterprises in using technical services of research and development organisations.

Measure 2.3. is implemented through the following key activities:

- **Activity 2.3.1:** Digital transformation support programme for MSMEs
- **Activity 2.3.2:** Support to small and medium-sized enterprises for development of innovation in the field of ICT

Measure 2.3. Informational and educational measure	Digital transformation of MSMEs		
Implementing agency	Ministry of Economy Chamber of Commerce and Industry of Serbia Centre for Digital Transformation		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
2.3.1 Number of economic operators that underwent the programme	100	1,000	CCIS/CDT
2.3.2 Number of financed projects by small and medium-sized enterprises in the field of ICT (cumulative)	99	550	Innovation Fund

Measure 2.4.
Development of e-business

The conditions for development of e-business were ensured when the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions and the Law on eGovernment entered into force; however, full implementation of the law requires promotion of institutes and mechanisms laid down by it. It is necessary to increase the use of qualified trust services, particularly qualified electronic certificates, and electronic identification schemes used in electronic services.

It should also be noted that unobstructed implementation of the digitalisation process requires significant financial investment in solutions which enable electronic services important for many segments of the society, including economic and production activities. It is necessary to develop modern telecommunication solutions which ensure connection between remote rural areas and remote production plants (factories, farms etc.), and thus enable development of Industry 4.0, i.e. development of precision agriculture.

Measure 2.4. is implemented through the following key activities:

- **Activity 2.4.1:** Promoting the use of qualified trust services
- **Activity 2.4.2:** Support to formation of the Conformity Assessment Body

- **Activity 2.4.3:** Promoting the use of electronic identification schemes
- **Activity 2.4.4:** Mutual recognition of qualified services between Serbia and the EU and countries in the region

Measure 2.4. Informational and educational measure	Development of e-business		
Implementing agency	Ministry of Trade, Tourism and Telecommunications		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
2.4.1 Number of issued qualified electronic certificates	614,422	800,000	MTTT
2.4.2 Accredited Conformity Assessment Body	0	2	Accreditation Body of Serbia
2.4.3 Number of registered electronic identification schemes	2	8	MTTT
2.4.4 Number of concluded international contracts	2	4	MTTT

Measure 2.5.
Strengthening capacities for usage of ICT in cultural institutions with the aim of developing and improving the IS and the basis for development of entrepreneurship in culture / creative industries (gaming, applications, multimedia guides...)

Strengthening capacities for the usage of ICT in cultural institutions requires provision of support to cultural institutions and projects of economic operators that cooperate with cultural institutions to increase interest in this field, which would contribute to development of new products and services.

Measure 2.5. is implemented through the following key activities:

- **Activity 2.5.1:** Award of funds within the programme to support development of entrepreneurship through financial support
- **Activity 2.5.2:** Award of funds within the programme to support cultural institutions through development programmes

Measure 2.5. Subsidy	Strengthening capacities for usage of ICT in cultural institutions		
Implementing agency	Ministry of Culture and Information		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
2.5.1 Number of projects to which funds were awarded	61	90	MCI
2.5.2 Number of institutions and other cultural entities that digitalised their archiving materials	19	50	Report of the digitalisation process coordinator

Analysis of Effects of Measures for Implementation of Specific Objective 2

The analysis of the impact on the society – The Specific Objective 2 and its measures have a significant impact on the society because they result in digitalisation of services and business operations, which relates both to the public administration providing services electronically and to digitalisation of business operations in the private sector, which leads to modernisation and improvement of operations. This ensures faster and more efficient business operations and cost reduction for operations of economic operators, public authorities and citizens, modernisation and efficient work of public authorities, easier and safer access to services of public authorities and other entities which are provided electronically, as well as access to more such services.

The analysis of management capacities – Implementation of these measures requires further improvement of administrative and expert capacities at the Ministry of Trade, Tourism and Telecommunications, the Chamber of Commerce and Industry of Serbia and the Innovation Fund, particularly in terms of grant award administration process, with the aim of promoting development of entrepreneurship and start-ups, the education process, counselling aimed at digitalisation of small and medium-sized enterprises and activities aimed at developing e-business, particularly qualified trust services.

The analysis of economic effects – Implementation of measures to achieve Specific Objective 2 contributes to reduction of costs of business operations, particularly in the private sector, because the number of electronically available services is increasing, thus reducing certain costs. Digitalisation enables operations to be carried out electronically, without the need to go to windows, to certain institutions and without physical contact, which saves material resources (costs of transport, paper etc.) and time required in classic business operations.

The risk analysis – Risks in implementation of these measures exist for the public administration and for the private sector, first in terms of awareness rising on the importance of digitalisation and its advantages and then in provision of necessary infrastructure for its implementation. It is thus necessary to mitigate risks through planned and gradual digitalisation, to ensure appropriate infrastructure, expertise of those who implement it, and also by continual awareness rising of its importance.

SPECIFIC OBJECTIVE 3

Improved information security of citizens, public administration and businesses

As new technologies develop, the risks they imply also increase and those risks exist for both citizens and public administration and for businesses. To minimise the risks, it is necessary to undertake steps for awareness rising and improvement of knowledge in this field in order to stimulate citizens to use new technologies and to ensure their use is secure and protected.

In addition, it is important to appropriately protect ICT systems, not only those covered by the protection under the Law on Information Security, but also those ICT systems that exist in businesses and are also exposed to attacks and the risk of jeopardising information security.

Appropriate implementation of measures and improvement of knowledge and awareness-rising in this field depend also on the capacities of competent institutions in this field, and it is

necessary to strengthen those capacities accordingly through training for employees, through more intensive inspection and through development of various forms of cooperation, both within the country and regional and international.

Priority areas of the Strategy for the Development of Information Security in the Republic of Serbia for the period from 2017 to 2020 *inter alia* include the fight against cybercrime and information security in Serbia. However, three new strategies were passed in 2019 which address these fields in more details, including:

- The Strategy for the Fight against Cybercrime for the period from 2019 to 2023;
- The Defence Strategy of the Republic of Serbia;
- The National Security Strategy of the Republic of Serbia.

The Strategy for the Fight against Cybercrime recognised through the Overarching Objective the need for better connecting of all entities covered by the Strategy in the fight against cybercrime through improvement of the legislative framework, capacities, prevention and improvement of national, international and regional cooperation.

The Strategy *inter alia* includes a Specific Objective which relates to improvement of organisational, human resource, technical and operational capacities of authorities responsible for the fight against cybercrime, through activities that include trainings for employees for acting in case of incidents and improvement of their digital competences.

Under the Defence Strategy of the Republic of Serbia, security of the Republic of Serbia and its citizens is also planned to be protected, *inter alia* through improvement of cyber security, and includes:

- Improvement of abilities and capacities for coordination of tasks directed at achieving cyber security and protection against security risks in information and communication systems,
- Formulation of a clear and coherent policy in order to increase resistance of information and communication systems to incidents,
- Introduction of a network of entities competent for the fight against cyber attacks and crime,
- Development of the general security culture for all citizens in order to raise awareness on the need to increase security of individuals and the society.

In addition, the National Security Strategy of the Republic of Serbia states that improvement of abilities and capacities of processing, transfer and protection of information and information and communication systems and defence against hybrid and information warfare techniques in information and cyber space will be continued in the field of cyber security.

In view of the foregoing, it can be concluded that Serbia has a comprehensive approach to the field of information security, which includes both information security of ICT systems of special importance and security of the Republic of Serbia, and security of citizens and businesses, which is particularly reflected through the fight against cybercrime.

Specific Objective 3	Improved information security of citizens, public administration and businesses		
Indicator	Baseline value in 2019	Target value in 2026	Verification source
Global information security index	58	30	International Telecommunication Union report <i>Global Cybersecurity Index - ITU</i>

Measures for Implementation of Specific Objective 3

Specific Objective 3 “Improved information security of citizens, public administration and businesses” is implemented through measures, including:

- **Measure 3.1:** Awareness rising and improvement of knowledge of information security for citizens, public servants and businesses.
- **Measure 3.2:** Strengthening capacities of the ICT systems of particular importance for application of safeguards.
- **Measure 3.3:** Measure 3.3: Strengthening capacities of the National CERT, govCERT and CERT of independent ICT system operators.
- **Measure 3.4:** Strengthening capacities of the information security inspectorate.
- **Measure 3.5:** Promoting public-private partnership in the field of information security.
- **Measure 3.6:** Improvement of regional and international cooperation.

Measure 3.1.

Awareness rising and improvement of knowledge of information security for citizens, public servants and businesses

As regards promotion of the topic of information security, findings of the World Bank report state that “in Serbia there appears to be some media coverage of cybersecurity topics, but only in an *ad hoc* manner and that there is very little presence of the issue of information security in the social media. As regards civil servants, cybersecurity awareness in Serbia can vary considerably, depending on the individual’s environment, but it should be noted many government employees are increasing their level of awareness, in part due to the growth of awareness training in the government. However, a cybersecurity mindset remains uneven across government entities.”

The report further states that “in the private sector the mindset depends on the industry and size of the company. The cybersecurity mindset is highest within the larger companies, particularly those with a more international presence, and most if not all the financial services and technology companies.”

The fact that a significant percentage of citizens who indicated lack of skills, or even the fact that they do not have Internet access, as a reason why they do not use public administration or e-commerce services, as well as that they did not take some activities on the Internet because they were worried about security, shows the importance of improvement of citizens’ digital competence, and also that in such process, focus should also be the segment of information security. It is

necessary to find the right balance between promoting the use of ICT on one hand and awareness rising and improvement of knowledge on the protection against possible risks, abuse or fraud.

Improving digital competences on one hand and awareness rising and improvement of knowledge on risks in the use of ICT on the other hand will ensure that a higher percentage of the population use digital services in various fields, which will consequently lead to higher digitalisation of the society and also to significant reduction of costs, both for the citizens and for businesses.

The advantages for businesses, particularly small and medium-sized enterprises, from implementation of safeguards for ICT systems are undoubtable, particularly having in mind consequences that enterprises may suffer in case of possible attacks, which in drastic circumstances may even lead to bankruptcy. It is necessary to raise awareness of risks for business operations of companies, and also to raise awareness and improve knowledge of the manners to minimize these risks. In addition to the obvious need for application of safeguards, awareness of continual strengthening of employees' capacities is also necessary. This does not include only employees working as ICT experts; instead, this includes all other employees who can, by their inappropriate acting, out of ignorance, contribute to exposure of the system to ICT risk and to occurrence incidents which can significantly jeopardise security of ICT systems and cause severe consequences.

Measure 3.1. is implemented through the following key activities:

- **Activity 3.1.1:** Organisation and coordination of awareness-raising media campaigns for citizens, public servants and small and medium-sized enterprises on the importance of information security, on risks and safeguards.
- **Activity 3.1.2:** Educations for citizens for awareness rising of information security.
- **Activity 3.1.3:** Development and implementation of compulsory continual training for public servants in information security.
- **Activity 3.1.4:** Trainings for small and medium-sized enterprises on the need and the manner of application of safeguards and the importance of continual strengthening of employees' capacities, in accordance with national and international standards.
- **Activity 3.1.5:** Development of guidelines on the basic level of safeguards for small and medium-sized enterprises
- **Activity 3.1.6:** Development, harmonisation and expansion of specialised information security courses and programmes on universities and other higher education institutions.
- **Activity 3.1.7:** Creating courses, seminars and lectures on the topic of information security for students in non-technical study programmes such as law, management etc.
- **Activity 3.1.8:** Setting up a platform for awareness-rising and improvement of knowledge on information security through interactive programmes (*Cybersecurity Awareness Platform*)

Measure 3.1. Informational and educational measure	Awareness rising and improvement of knowledge of information security for citizens, public servants and businesses		
Implementing agency	Ministry of Trade, Tourism and Telecommunications National CERT Ministry of Education, Science and Technological Development Ministry of Interior National Academy For Public Administration		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
3.1.1. Number of campaigns implemented	3	4	MTTT RATEL MoI CERT
3.1.2 Number of educational materials for citizens	0	5	RATEL
3.1.3 Number of educated civil servants introduced	40	350	MTTT NAPA MoI CERT
3.1.4 Number of trainings held for small and medium-sized enterprises	1	8	RATEL
3.1.5 Guidelines prepared for basic level safeguards for small and medium-sized enterprises	0	1	RATEL
3.1.6 Specialised courses and programmes developed			MESTD
3.1.7 Courses, seminars and lectures created			MESTD
3.1.8 Platform established	0	1	MTTT RATEL

Measure 3.2.
Improvement of cooperation and strengthening capacities of the ICT systems of particular importance for application of safeguards

ICT systems of particular importance, or the so-called critical information infrastructure, are identified by the Law as special and vital because their unobstructed functioning must be maintained, since any obstruction, downtime or destruction of these systems may have significant consequences when they cover a large number of users, a large part of the territory or public security. It is therefore necessary for ICT systems to apply safeguards which provide prevention of incidents, i.e. prevent incidents and reduce damage from incidents which jeopardise exercise of powers and performance of activities.

Preconditions for application of safeguards in ICT systems of particular importance include equipment, trained employees, awareness of the importance of application of measures and statutory procedures (security instrument) defining safeguards and responsibilities of employees and the management.

A major segment of development of this field is also cooperation between ICT systems of particular importance, in particular those who have similar structure, such as financial, energy and health systems, systems of public authorities etc.

One of important novelties introduced by amendments of the Law on Information Security is establishing of the Records of ICT Systems of Particular Importance. To fully implement the Law, it is necessary to establish cooperation between relevant institutions responsible for information security, MTTT, NCERT and govCERT one hand, and ICT of particular importance on the other hand. This cooperation is important for reporting of incidents which significantly jeopardize information security and which ICT must report, but which rarely occur in practice. It is necessary to inform ICT systems of particular importance through joint meetings on the importance of reporting the incidents, to explain reporting mechanisms and to create mutual trust which will result in mutual benefits.

The second novelty of the Law on Information Security relates to submission of all statistics on all incidents that occurred in one ICT system of particular importance. Thus, statistics do not include only data that significantly jeopardize information security and which must be reported; instead, it includes all incidents which occurred, so that comprehensive overview of the situation in this field would be obtained based on their analysis and that measures and activities could be defined for improvement.

Measure 3.2. is implemented through the following key activities:

- **Activity 3.2.1:** Trainings for employees in ICT systems of particular importance on application of safeguards and acting in case of an incident in an ICT system.
- **Activity 3.2.2:** Organisation of meetings of ICT systems of particular importance according to the sectors to which they belong with the aim of encouraging cooperation and promoting formation of special sectoral CERTs.
- **Activity 3.2.3:** Organisation of international and national meetings, round tables and conferences with the aim of raising awareness of the importance of information security.
- **Activity 3.2.4:** Determining manners and mechanisms for strengthening the capacities of ICT systems of particular importance to achieve the necessary level of compliance with information security requirements (common criteria) within management of all stages of the lifecycle of ICT systems or parts of the systems
- **Activity 3.2.5:** Preparation of brochures, recommendations and other materials with the aim of rising awareness of the importance of safeguards.
- **Activity 3.2.6:** Development of a platform for information exchange between the National CERT and ICT systems of particular importance with the aim of providing information on current risks and threats in the field of information security and promoting good practice examples.
- **Activity 3.2.7.** – Development of an overview of threats based on submitted statistics on incidents and reported incidents.
- **Activity 3.2.8.** – Harmonisation of legislation with EU regulations in the field of information security
- **Activity 3.2.9.** – Development of a self-evaluation form for ICT systems of particular importance

- **Activity 3.2.10.** – Development of a form to assess the level of development of information security in Serbia

Measure 3.2. Informational and educational measure	Improvement of cooperation and strengthening capacities of the ICT systems of particular importance for application of safeguards		
Implementing agency	Ministry of Trade, Tourism and Telecommunications National CERT Ministry of Interior National Academy for Public Administration		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
3.2.1 Number of trained employees in ICT systems of particular importance	120	350	MTTT RATEL NAPA
3.2.2 Number of sectoral meetings of ICT systems of particular importance	1	20	MTTT
3.2.3 Number of meetings, round tables and conferences held	15	40	MTTT RATEL MoI CERT NAPA
3.2.4 The manners and mechanisms for strengthening the capacities of ICT systems of particular importance established	0	1	MTTT
3.2.5 Materials (brochures, recommendations etc.) developed	119	80	RATEL MoI CERT
3.2.6 Platform developed for information exchange between the National CERT and ICT systems of particular importance	0	1	RATEL
3.2.7 The number of developed overviews of threats for the National CERT	1	8	RATEL
3.2.8 Regulations in the field of information security amended	0	2	MTTT
3.2.9 A self-evaluation form developed	0	1	MTTT
3.2.10 A form to assess the level of development of information security developed	0	1	MTTT

Measure 3.3.
Strengthening capacities of the National CERT, govCERT and CERT of independent ICT system operators

The role of the National CERT, govCERT and CERTs of independent ICT system operators is important from the aspect of cooperation, coordination and monitoring the situation with information security in the country.

It is particularly important for the National CERT to be able and has capacities to collect information on risks for security of ICT systems and to timely provide support, warns and give advice to ICT systems of particular importance and also the public.

It is also necessary to develop mechanism for cooperation and data exchange between ICT systems of public authorities within the Single Information and Communication Network of eGovernment and govCERT, because those systems have similar structure and the level of development and information exchange could therefore could contribute to their improvement.

From the aspect of national security, it is important for independent ICT system operators to have developed capacities and that they are able to defend both their systems and other independent ICT system operators affected by an incident.

Measure 3.3. is implemented through the following key activities:

- **Activity 3.3.1:** Training for employees in the National CERT with the aim of strengthening capacities for acting in case of incidents.
- **Activity 3.3.2:** Training for employees in govCERT and in independent ICT system operators.
- **Activity 3.3.3:** Establishing of CERT of independent ICT system operators.
- **Activity 3.3.4:** Development of guidelines for acting in case of high and very high risk incidents.
- **Activity 3.3.5:** Establishing a mechanism for information exchange and cooperation between individual CERTs and the National CERT.
- **Activity 3.3.6:** Establishing cooperation between the National CERT, the MTTT and the Emergency Management Team of the MoI (Emergency Management Sector) for the purpose of recognising a cooperation mechanism in case of high and very high risk incidents.
- **Activity 3.3.7:** Organisation of civil and military exercises
- **Activity 3.3.8:** Setting up of a system for detection of cyber threats

Measure 3.3. Informational and educational measure	Strengthening capacities of the National CERT, govCERT and CERT of independent ICT system operators		
Implementing agency	Ministry of Trade, Tourism and Telecommunications RATEL Office for IT and Electronic Government Ministry of Defense Ministry of Foreign Affairs Security Information Agency Military Security Agency Military Intelligence Agency		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
3.3.1 Number of trained employees in the NCERT	6	10	RATEL
3.3.2 Number of trained employees in govCERT and in independent ICT operators	35	55	MoD MFA SIA MSA

			MIA MoI ITE
3.3.3 Number of established CERTs of independent operators	2	4	MoD MFA MSA MIA
3.3.4 Guidelines developed	0	1	MTTT MoI
3.3.5 Mechanisms established for information exchange between NCERT and individual CERTs	0	1	RATEL
3.3.6 Cooperation established between the NCERT, the MTTT and the MoI (Emergency Management Sector)	0	1	MTTT RATEL MoI
3.3.7 Number of organised civil and military exercises	3	7	MoD MoI RATEL
3.3.8 A systems for detection of cyber threats established	0	1	RATEL

Measure 3.4.

Strengthening capacities of the information security inspectorate

In addition to promotion and provision of information on legislative provisions, the Law on Information Security is also implemented through inspection which implies control of application of safeguards and verification whether annual assessment of the security situation in ICT systems of particular importance was performed.

To increase the coverage of ICT systems of particular importance by inspection, it is necessary to strengthen the capacities of the inspection, namely, to hire new employees and to increase expert capacities of employed inspectors.

Measure 3.4. is implemented through the following key activities:

- **Activity 3.4.1:** Training for information security inspectors based on prepared needs assessments for trainings with the aim of strengthening capacities for implementation of the Law on Information Security
- **Activity 3.4.2:** Employment of information security inspectors.

Measure 3.4. Informational and educational measure	Strengthening capacities of the information security inspectorate		
Implementing agency	Ministry of Trade, Tourism and Telecommunications		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
3.4.1 Number of trainings attended by inspectors	7	12	MTTT
3.4.2 Number of employed inspectors	1	5	MTTT

Measure 3.5.

Promoting public-private partnership in the field of information security

Cooperation between the public and the private sectors is one of the key elements of information security of every country. Namely, limitations which exist on both sides in responses to challenges of information security impose the need to establish partnerships, particularly in case when incidents significantly jeopardise information security. In public-private partnership, finding the appropriate cooperation mechanism is not the only issue; instead, there is also the issue of creating trust between them that will contribute to strengthening of capacities and increasing the level of information security.

Measure 3.5. is implemented through the following key activities:

- **Activity 3.5.1:** Formation of an expert working group named Information Security Coordination Body.
- **Activity 3.5.2:** Organisation of meetings of the “Cyber Security Network” foundation with the aim of promoting public-private partnership.
- **Activity 3.5.3:** Concluding cooperation agreements between public authorities and private and non-governmental sectors with the aim of implementing projects in the field of information security.

Measure 3.5. Informational and educational measure	Promoting public-private partnership in the field of information security		
Implementing agency	Ministry of Trade, Tourism and Telecommunications		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
3.5.1 Expert working group formed	0	2	MTTT
3.5.2 Number of meetings held	1	Minimum 3 years	MTTT
3.5.3 Number of cooperation agreements concluded	0	4	Reports by relevant ministries

Measure 3.6.

Improvement of regional and international cooperation

Just as the field of information security requires cooperation between the public and the private sectors, it also requires both regional and international cooperation because all countries face risks and threats in this field which in some cases can also jeopardise national security.

International and regional cooperation mechanisms have been developed to a high extent through activities of various institutions and agencies (ITU, OSCE, DCAF..), as well as through various project activities and should be upgraded by concluding bilateral and multilateral agreements which would define joint objectives and activities for improvement of information security.

It is also important to continue the already initiated practice of organising international and civil exercises which efficiently strengthen the capacities of institutions and employees for response in case of incidents, with exchange of experiences and practical presentation of the manner of responding.

Measure 3.6. is implemented through the following key activities:

- **Activity 3.6.1:** Conclusion of bilateral and multilateral cooperation agreements in the field of information security.
- **Activity 3.6.2:** Participation of representatives of competent authorities in international forums and meetings dedicated to information security within the UN, OSCE, GFCE and other international organisations.
- **Activity 3.6.3:** Cooperation with EU institutions and organisations competent for the field of information security (FIRST, ENISA, EU CERT Network etc.)

Measure 3.6.	Improvement of regional and international cooperation		
Implementing agency	Ministry of Trade, Tourism and Telecommunications Ministry of Defence National CERT Ministry of the Interior Ministry of Foreign Affairs		
Indicator	Baseline value in 2020	Target value in 2026	Verification source
3.6.1 Number of concluded bilateral and multilateral agreements	0	3	MTTT
3.6.2 Number of attended international forums and meetings (UN, OSCE, GFCE etc.)	6	15	MTTT MoI MFA MoD RATEL ITE
3.6.3 Number of listed, accredited and certified CERTs on the Trusted Introducer List and the number of FIRST members or associate members	7	9	Trusted Introducer list FIRST report

Analysis of Effects of Measures for Implementation of Specific Objective 3

Analysis of the impact on the society – There is a very large spectrum of positive impacts on the society achieved through implementation of the measures within the Specific Objective 3. Having in mind the consequences which may occur for citizens and businesses due to inappropriate development of information security, such as identity theft, financial frauds, disabling the functioning of key institutions and ICT systems, it is clear that awareness rising and improvement of knowledge of the protection against risks, application of safeguards for ICT systems of particular importance and strengthening employees’ capacities significantly increase the level of information security and reduce risks. This comprehensively protects citizens, public administration and businesses.

Analysis of management capacities – In order to implement these measures, it is necessary to invest significantly in management capacities, particularly in those institutions that are responsible for information security in accordance with the law. Investment in capacities implies continual development of employees and improvement of their knowledge through various educational programmes, participation in conferences and exchange of experiences with other countries. The dynamic nature of this field means that staff adaptation to new challenges that are always present also has to be dynamic; however, these challenges are always new, which makes them even higher and more demanding for acting. Strengthening the capacities of public administration authorities will also be achieved through strengthening of the existing and establishing of new partnerships with the expert and academic sectors and civil society organisations.

Analysis of economic effects – On one hand, implementation of these measures increases the costs for the public and the private sectors, which must implement safeguards against potential incidents in their ICT systems, but, on the other hand, potential damage which can result from incidents fully justifies investment and is a kind of saving.

Risk analysis – Risks in implementation of the measures exist for education of employees, procurement of appropriate equipment, awareness of the importance of information security and its impact on all segments of life. In order to reduce risks, implementation of campaigns on the importance of this topic is necessary, as well as commitment of competent institutions to plan investment and systematically invest in employees, equipment and protection of their systems, and to continue development of cooperation between all relevant actors in this field, as an important mechanism which is particularly relevant when incidents occur which significantly jeopardise information security.

4. MECHANISM FOR IMPLEMENTATION OF STRATEGY AND REPORTING ON RESULTS OF IMPLEMENTATION

The Ministry of Trade, Tourism and Telecommunications is responsible for reporting on the implementation of this Strategy through monitoring of the implementation and coordination of public policies in cooperation with competent ministries. The report on implementation of the Strategy is prepared upon expiry of every third calendar year from the date of adoption of the Strategy, in accordance with deadlines laid down by the Law of Planning System. The competent ministries submit to the Ministry of Trade, Tourism and Telecommunications reports on implemented measures and achieved values of indicators, according to the following schedule:

Specific Objective	Competent ministry	Reporting schedule
Specific Objective 1	Ministry of Trade, Tourism and Telecommunications Ministry of Education, Science and Technological Development	November 2023 November 2026

Specific Objective 2	Ministry of Public Administration and Local Self-Government Ministry of Education, Science and Technological Development Ministry of Economy Ministry of Trade, Tourism and Telecommunications	November 2023 November 2026
Specific Objective 3	Ministry of Trade, Tourism and Telecommunications	November 2023 November 2026

Reporting on implementation of Action Plans is carried out annually, based on data submitted on request by other ministries and institutions to the Ministry of Trade, Tourism and Telecommunications, through the Single Information System for planning, monitoring of implementation, coordination of public policies and reporting, in accordance with the law.

5. CONSULTATIONS IMPLEMENTED WITH STAKEHOLDERS

The Working Group of the Ministry of Trade, Tourism and Telecommunications participated in the development of the Strategy, which consisted of the following institutions: the Ministry of Defence, the Ministry of Justice, the Ministry of the Interior, the Ministry of Finance, the Ministry of Education, Science and Technological Development, the Ministry of Health, the Ministry of Mining and Energy, the Ministry of Foreign Affairs, the Ministry of Culture, the Ministry of Agriculture, Forestry and Water Management, the Ministry of Construction, Transport and Infrastructure, the Security Information Agency, the Office for Information Technologies and eGovernment, the Office of the National Security Council and Classified Information Protection, the Regulatory Agency for Electronic Communications and Postal Services and the National Bank of Serbia.

A number of stakeholders were included in the process of consultation and public-private dialogue, such as economic operators and associations, educational and scientific institutions, expert organisations and civil society organisations. Namely, in accordance with Article 5 of the Law on Information Security, the Expert Working Group of the Information Security Coordination Body was formed, which consisted of experts in the field of information security, and which was tasked with submission of information on activities, needs and priorities of the private sector in the field of information security of relevance for development of the Strategy and preparation of proposals and recommendations for improvement of information security in the Republic of Serbia.

The public debate was held in the period from 23 April to 19 May 2021.

6. ASSESSMENT OF FINANCIAL RESOURCES NECESSARY FOR IMPLEMENTATION OF STRATEGY AND ANALYSIS OF FINANCIAL EFFECTS

Funds necessary for implementation of measures and activities planned under this Strategy, the implementation of which will contribute to achievement of the defined strategic objectives, will be provided from the budget of the Republic of Serbia according to the available balance, and where necessary, additional funds will be provided from donations, projects, international assistance and other sources. Nearly 6 billion dinars are planned for the realization of the Action Plan for the period from 2021 to 2023, and it is assumed that a similar amount will be allocated for the Action Plan for the period from 2024 to 2026.

7. ACTION PLAN FOR IMPLEMENTATION OF INFORMATION SOCIETY AND INFORMATION SECURITY DEVELOPMENT STRATEGY IN THE REPUBLIC OF SERBIA FOR THE PERIOD FROM 2021 TO 2023

The Action Plan for Implementation of the Information Society and Information Security Development Strategy in the Republic of Serbia for the period from 2021 to 2023 is enclosed to this Strategy and constitutes an integral part thereof.

8. FINAL PART

This Strategy shall be published on the Government's official website, on the eGovernment portal and on the official website of the Ministry of Trade, Tourism and Telecommunications, within seven working days of the date of adoption of the Strategy.

This Strategy shall be published in the *Official Gazette of the Republic of Serbia*.

05 No.: 021-7637/2021
Belgrade, 26. August 2021.

9. ACTION PLAN FOR IMPLEMENTATION OF THE INFORMATION SOCIETY AND INFORMATION SECURITY DEVELOPMENT STRATEGY IN THE REPUBLIC OF SERBIA FOR THE PERIOD FROM 2021 TO 2023

Action plan:	ACTION PLAN FOR IMPLEMENTATION OF THE INFORMATION SOCIETY AND INFORMATION SECURITY DEVELOPMENT STRATEGY IN THE REPUBLIC OF SERBIA FOR THE PERIOD FROM 2021 TO 2023
Authority proposing the Action Plan:	Ministry of Trade, Tourism and Telecommunications
Coordination and reporting:	Ministry of Trade, Tourism and Telecommunications

Overarching Objective 1:	A DEVELOPED INFORMATION SOCIETY AND CITIZEN- AND BUSINESS-ORIENTED ELECTRONIC GOVERNMENT, WITH IMPROVED INFORMATION SECURITY FOR CITIZENS, PUBLIC ADMINISTRATION AND BUSINESSES					
Institution responsible for monitoring and control of implementation:	Ministry of Trade, Tourism and Telecommunications					
Overarching Objective indicator (<i>effect indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in the last year of AP	The last year of validity of AP
Digital economy and society index	Percentage	<i>International Digital Economy and Society Index</i>	38	2018.	40	2023

Specific Objective 1:	IMPROVEMENT OF CITIZENS' DIGITAL KNOWLEDGE AND SKILLS, STRENGTHENING CAPACITIES OF PUBLIC AND PRIVATE SECTOR EMPLOYEES TO USE NEW TECHNOLOGIES AND IMPROVEMENT OF DIGITAL INFRASTRUCTURE IN EDUCATION INSTITUTIONS							
Institution responsible for coordination and reporting:	Ministry of Trade, Tourism and Telecommunications							
Specific Objective indicator (<i>outcome indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023	
Computer literate persons	Percentage	Statistical Yearbook of the Republic of Serbia (SORS)	34.2%	2020.	36%	38%	40%	
Use of the Internet	Households	Percentage	Usage of ICT Report (SORS)	80.1%	2020.	81%	83%	84%
	individuals	Percentage	Usage of ICT Report (SORS)	78.4%	2020.	80%	82%	83%

Measure 1.1:	Improvement of digital knowledge, skills and capacities of citizens and employees through trainings aimed at increased usage of ICT							
Institution responsible for implementation:	MTTT							
Implementation period:	2021 – 2023			Type of the measure:		Informational and educational		
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023	
1.1.1 Number of approved support programmes	Number	MTTT report	41	2019.	43	45	50	
1.1.2 Number of trained teachers	Number	MTTT/ MESTD reports	34,500	2019.	36,000	38,000	40,000	
1.1.3 Number of trained employees	Number	MTTT report	430	2019.	480	500	520	
		NAPA report	1,113	2020.	1,200	1,300	1,400	
1.1.4 Number of trainings held at the Serbian-Korean Information Access Centre	Number	MPALSG report	400	2019.	350	350	350	
Source of financing for the measure	Reference to programme budget		Total estimated funds in RSD					
			2021	2022	2023			
Revenue from the budget	MTTT Programme 0703 Function 460 PA 0006 EK 481		20,000,000		40,000,000		40,000,000	
	MTTT Programme 0703 Function 460 PA 0008 EK 424		/		12,000,000		6,000,000	
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023

1.1.1.	Support programmes for associations through award of funds for implementation of programmes in the field of development of the information society	MTTT		IV quarter 2023.	Budget of RS	MTTT Programme 0703 Function 460 PA 0006 EK 481	20,000,000	40,000,000	40,000,000
1.1.2.	Trainings aimed at improving teachers' competencies in the field of information and communication technologies	MESTD		IV quarter 2023.	Budget of RS (regular funding)	MESTD Programme 2005 Function 460 PA 0014			
			MTTT	IV quarter 2023.		MTTT Programme 0703 Function 460 PA 0008 EK 424		6,000,000	6,000,000
1.1.3	Development and implementation of trainings aimed at improving digital competencies of employees in the public administration	NAPA		IV quarter 2023.	Budget of RS (regular funding)	NAPA Programme 0615 PA 0001 EK 411			
			MTTT	IV quarter 2023.		MTTT Programme 0703 Function 460 PA 0008 EK 424		6,000,000	
1.1.4	Popularisation and promotion of the use of ICT through the Serbian-Korean Information Access Centre	MPALSG		IV quarter 2023.	Budget of RS (regular funding)	MESTD Programme 0613 Function 111 PA 005 EK 411			

Measure 1.2:	Promotion of useful, creative and secure usage of information technologies through organisation of educational and media campaigns and prize competitions							
Institution responsible for implementation:	MTTT							
Implementation period:	2021 – 2023			Type of the measure:		Informational and educational		
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023	
1.2.1 Number of children who attended educational debates	Number	MTTT report	2,000	2019.	2,200	2,400	2,600	
1.2.2 Number of works published in the electronic compendium “Digital Class”	Number	MTTT report	1,835	2019.	2,000	2,400	2,600	
1.2.3 Number of events held	Number	MTTT report	6	2019.	6	7	7	
Source of financing for the measure	Reference to programme budget		Total estimated funds in RSD					
			2021	2022	2022			
Revenue from the budget			100,000	100,000	100,000			
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021.	2022.	2023.
1.2.1. IT Caravan – an educational campaign for promotion of useful, creative and secure usage of information technologies	MTTT		III quarter 2023.	Budget of RS	MTTT Programme 0703 Function 460 PA 0008 EK 423	3,000,000	3,000,000	3,000,000
1.2.2. Popularisation and promotion of the use of ICT in classes through a prize competitor titled “Digital Class”	MTTT		IV quarter 2023.	Budget of RS	MTTT Programme 0703 Function 460 PA 0008 EK 423	3,000,000	3,000,000	3,000,000
1.2.3. Promotional campaign “Smart	MTTT		III quarter 2023.	Budget of RS	MTTT	1,000,000	2,000,000	2,000,000

and Safe” (the Girls in ICT Day, the Safer Internet Day, the European Programming Hour, the Information Society Day...)					Programme 0703 Function 460 PA 0008 EK 423			
---	--	--	--	--	---	--	--	--

Measure 1.3:		Improvement and promotion of the work of the National Contact Centre for Child Safety on the Internet							
Institution responsible for implementation:		MTTT							
Implementation period:		2021 – 2023			Type of the measure:		Informational and educational		
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023		
1.3.1 Number of trained employees	Number	MTTT report	626	2020.	680	720	740		
1.3.2 Number of informed children, parents and teachers	Number	MTTT report	20,000	2020.	20,500	21,000	22,000		
Source of financing for the measure		Reference to programme budget		Total estimated funds in RSD					
				2021	2022	2023			
Revenue from the budget		MTTT Programme 0703 Function 460 PA 0008 EK 423		100,000	100,000	100,00			
Activities:		Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget			
							Total estimated funds by sources in RSD		
							2021	2022	2023
1.3.1. Trainings aimed at strengthening the capacities of employees in institutions of the system for the purpose of applying		MTTT		IV quarter 2023.	Budget of RS	MTTT Programme 0703 Function 460 PA 0008 EK 423	100,000	100,000	100,00

	of the Regulation on Safety and Protection of Children in the Use of Information and Communication Technologies							
1.3.2	Provision of information to and education of children, parents and teachers in child safety on the Internet through organisation of trainings in schools	MTTT		IV quarter 2023.	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411		

Measure 1.4:	Improvement of the digital infrastructure in educational institutions						
Institution responsible for implementation:	MTTT						
Implementation period:	2021 – 2023			Type of the measure:		Subsidy	
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023
1.4.1 Number of central school facilities, cultural institutions and public libraries connected to the AMRES network	Number	AMRES report	1,938	2020.	2,000	2,500	3,000
1.4.2 Number of schools to which wireless communication infrastructure was provided	Number	MTTT report	900	2020.	1,200	1,500	1,830
Source of financing for the measure	Reference to programme budget		Total estimated funds in RSD				
			2021	2022	2023		
Revenue from the budget	MTTT Programme 0703 Function 460 PA 0003		135,000,000	150,000,000	150,000,000		

		EK 424						
		MTTT Programme 0703 Function 460 PA 5003 EK 512			2,090,000,000	/		/
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023
1.4.1. Continuation of connection of all central primary and secondary school facilities, cultural institutions and public libraries in Serbia to the AMRES network	AMRES		IV quarter 2023.		MTTT Programme 0703 Function 460 PA 0003 EK 424	135,000,000	150,000,000	150,000,000
1.4.2. Development of the information and communication infrastructure in primary and secondary schools within the “Connected Schools” project	MTTT	MESTD	IV quarter 2023.	Budget of RS	MTTT Programme 0703 Function 460 PA 5003 EK 512	2,090,000,000	/	/

Specific Objective 2:	DIGITALISATION OF SERVICES AND BUSINESS OPERATIONS IN PUBLIC AND PRIVATE SECTORS						
Institution responsible for coordination and reporting:	Ministry of Trade, Tourism and Telecommunications						
Specific Objective indicator (outcome indicator)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023
eGovernment EU benchmark	Percentage	eGovernment Benchmark Report	43.75%	2020.	45%	50%	61.75%

Percentage of businesses that sold products and services on the Internet	Percentage	Usage of ICT in Serbia Report (SORS)	27.9%	2020.	28.1%	28.3%	28.5%
Total export of computer and information services	EUR million	Balance of payments (NBS)	1,342	2020.	1,380	1,410	1,480

Measure 2.1:		Development of the information society							
Institution responsible for implementation:		MTTT							
Implementation period:		2021 – 2023			Type of the measure:		Subsidy		
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023		
2.1.1 Number of meetings held	Number	MTTT RNIDS reports	0	2020.	2	2	2		
2.1.2 Analysis developed	Yes/No	MTTT report	No	2020.	/	/	Yes		
2.1.3 Analysis developed	Yes/No	CCIS report	No	2020.	/	/	Yes		
Source of financing for the measure		Reference to programme budget		Total estimated funds in RSD					
				2021	2022	2023			
Revenue from the budget		MTTT Programme 0703 Function 460 PA 0008 EK 423		2,600,000	2,000,000	2,000,000			
Activities:		Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
							2021	2022	2023
2.1.1. Organisation of expert and other meetings in the field of information society within the		MTTT	RNIDS	IV quarter 2023.	Budget of RS	MTTT Programme 0703 Function 460 PA 0008 EK 423	2,000,000	2,000,000	2,000,000

Internet Governance Forum (IGF)								
2.1.2. Needs assessment for introduction of the data management system in the Republic of Serbia	MTTT		IV quarter 2023.	Budget of RS	MTTT Programme 0703 Function 460 PA 0008 EK 423	600,000	/	/
2.1.3 Analysis of readiness and needs of businesses for application of new technologies	CCIS		IV quarter 2023.	CCIS		/	/	350,000

Measure 2.2:	Support to entry in foreign markets						
Institution responsible for implementation:	CCIS						
Implementation period:	2021 – 2023			Type of the measure:		Subsidy	
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023
2.2.1 Number of events organised in foreign countries	Number	CCIS report RAS report	6	2020.	7	8	9
2.2.2 Organisation of meetings of joint bodies for bilateral economic cooperation (committees, commissions, working groups, business councils) in the field of IT with the aim of promoting export of domestic IT products and services	Number	MTTT report	10	2020.	10	11	12
2.2.3 Number of events organised in Serbia	Number	CCIS report	12	2020.	13	15	16
Source of financing for the measure	Reference to programme budget	Total estimated funds in RSD					
		2021	2022	2023			
Revenue from the budget	ME Programme 1510 PA0001	175,000,000	175,000,000	175,000,000			

EK 424								
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023
2.2.1. Support to economic operators for entry in foreign countries	CCIS		IV quarter 2023.	CCIS		/	2,500,000	2,500,000
		RAS ME		Budget of RS	Budget of RS	175,000,000	175,000,000	175,000,000
2.2.2. Organisation of meetings of joint bodies for bilateral economic cooperation (committees, commissions, working groups, business councils) in the field of IT with the aim of promoting export of domestic IT products and services	MTTT		IV quarter 2023.	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			
2.2.3. Support to economic operators for participation in business delegations	CCIS		IV quarter 2023.	CCIS				

Measure 2.3:	Digital transformation of MSMEs						
Institution responsible for implementation:	ME						
Implementation period:	2021 – 2023				Type of the measure:		Informational and educational
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023

2.3.1 Number of economic operators that underwent the programme		CCIS / CDT reports	100	2020.	150	200	250	
2.3.2 Number of financed projects by small and medium-sized enterprises in the field of ICT (cumulative)	Number	Innovation Fund report	99	2020.	170	260	340	
Source of financing for the measure	Reference to programme budget	Total estimated funds in RSD						
		2021	2022	2023				
Revenue from the budget	ME Programme 1509 Function 410 PA 4008 EK 423 and 454		136,500,000		155,000,000		165,000,000	
	MESTD Programme 0201 Function 140 PA 0005 EK 451		340,000,000		/		360,000,000	
Financial assistance from the EU	MESTD Programme 0201 Function 140 PA 4004 EK 424		246,250,000		619,863,000		619,863,000	
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023
2.3.1. Digital transformation support programme for MSMEs	CCIS	ME	IV quarter 2023.	Budget of RS	ME Programme 1509 Function 410 PA 4008 EK 423 and 454	136,500,000	155,000,000	165,000,000
2.3.2. Support to small and medium-sized enterprises for development of	Innovation Fund	MESTD	IV quarter 2023.	Budget of RS	MESTD Programme 0201 Function 140	340,000,000	/	360,000,000

innovation in the field of ICT					PA 0005 EK 451			
				Financial assistance from the EU	MESTD Programme 0201 Function 140 PA 4004 EK 424	246,250,000	619,863,000	619,863,000

Measure 2.4:		Development of e-business						
Institution responsible for implementation:		MTTT						
Implementation period:		2021 – 2023			Type of the measure:		Informational and educational	
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023	
2.4.1 Number of issued qualified electronic certificates	Number	MTTT report	614,422	2020.	680,000	700,000	720,000	
2.4.2 Accredited Conformity Assessment Body	Number	Report of the Accreditation body of Serbia	0	2020.	1	1	2	
2.4.3 Number of registered electronic identification schemes	Number	MTTT report	2	2020.	3	4	5	
2.4.4 Number of concluded international contracts	Number	MTTT report	2	2020.	3	3	3	
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023
2.4.1. Promoting the use of qualified trust services	MTTT		IV quarter 2023.	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			

2.4.2.	Support to formation of the Conformity Assessment Body	MTTT		IV quarter 2023.	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			
2.4.3.	Promoting the use of electronic identification schemes	MTTT		IV quarter 2023.	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			
2.4.4.	Mutual recognition of qualified services between Serbia and the EU and countries in the region	MTTT		IV quarter 2023.	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			

Measure 2.5:	Strengthening capacities for usage of ICT in cultural institutions with the aim of developing and improving the IS and the basis for development of entrepreneurship in culture / creative industries						
Institution responsible for implementation:	MCI						
Implementation period:	2021 – 2023			Type of the measure:		Subsidy	
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023
2.5.1 Number of projects to which funds were awarded	number	MCI report	61	2020.	70	80	85
2.5.2 Number of institutions and other cultural entities that digitalised their archiving materials	number	MCI report	19	2020.	25	30	35
Source of financing for the measure	Reference to programme budget		Total estimated funds in RSD				
			2021	2022	2023		
500,00Revenue from the budget	MCI Programme 1202 PA 0009		2,000,000	2,000,000	2,000,000		

	EK 463							
	MCI Programme 1203 PA 0008 EK 463			1,000,000		1,000,000		1,000,000
	MCI Programme 1202 PA 0014 EK 423			5,000,000		5,000,000		5,000,000
	MCI Programme 1203 PA 0009 EK 463			500,000		500,000		500,000
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023
2.5.1. Award of funds within the programme to support development of entrepreneurship through financial support	MCI		IV quarter 2023.	Budget of RS	MCI Programme 1202 PA 0009 EK 463	2,000,000	2,000,000	2,000,000
					MCI Programme 1203 PA 0008 EK 463	1,000,000	1,000,000	1,000,000
2.5.2. Award of funds within the programme to support cultural institutions through development programmes	MCI		IV quarter 2023.	Budget of RS	MCI Programme 1202 PA 0014 EK 423	5,000,000	5,000,000	5,000,000
					MCI Programme 1203 PA 0009 EK 463	500,000	500,000	500,000

Specific Objective 3:	IMPROVED INFORMATION SECURITY OF CITIZENS, PUBLIC ADMINISTRATION AND BUSINESSES						
Institution responsible for coordination and reporting:	Ministry of Trade, Tourism and Telecommunications						
Specific Objective indicator (<i>outcome indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023
Global information security index	Ranking on the list	International Telecommunication Union report <i>Global Cybersecurity Index - ITU</i>	58	2019.	45	43	40

Measure 3.1:	Awareness rising and improvement of knowledge of information security for citizens, public servants and businesses						
Institution responsible for implementation:	RATEL						
Implementation period:	2021 – 2023			Type of the measure:		Informational and educational	
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023
3.1.1 Number of campaigns implemented	Number	MTTT MoI report	3	2020.	3	3	3
3.1.2 Number of educational materials for citizens	Number	RATEL		2020.	1	2	3
3.1.3 Number of educated civil servants	Number	MTTT Report		2020.			
		NAPA Report	40	2020.	60	90	120
3.1.4 Number of trainings held for small and medium-sized enterprises	Number	MTTT report	1	2020.	1	2	2
3.1.5 Guidelines prepared for basic level safeguards for small and medium-sized enterprises	Number	RATEL report	No	2020.	/	Yes	/
3.1.6 Specialised courses and programmes developed	Number	MESTD report		2020.			
3.1.7 Courses, seminars and lectures created	Number	MESTD MoI CERT		2020.			

3.1.8 Platform established		MTTT report	No	2020.	0	Yes		
Source of financing for the measure	Reference to programme budget		Total estimated funds in RSD					
			2021	2022	2023			
Revenue from the budget	MoI Programme 1408 PA 0001 EK 423		/		300,000		300,000	
	MoI Programme 1408 PA 0001 EK 512		/		2,000,000		2,000,000	
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023
3.1.1. Organisation and coordination of awareness-raising media campaigns for citizens, public servants and small and medium-sized enterprises on the importance of information security, on risks and safeguards.	RATEL	MTTT	IV quarter 2023.	RATEL				
		MoI	IV quarter 2023.	Budget of RS	MoI Programme 1408 PA 0001 EK 423	/	300,000	300,000
3.1.2. Educations for citizens for awareness rising of information security	RATEL		IV quarter 2023.	RATEL				
3.1.3. Development and implementation of compulsory continual training for public servants in information	MTTT		IV quarter 2023.	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			

security when they are employed.		NAPA	IV quarter 2023.	Budget of RS (regular funding)	NAPA Programme 0615 PA 0001 EK 411			
		MoI	IV quarter 2023.	Budget of RS	MoI Programme 1408 PA 0001 EK 423	/	2,000,000	2,000,000
3.1.4. Trainings for small and medium-sized enterprises on the need and the manner of application of safeguards and the importance of continual strengthening of employees' capacities, in accordance with national and international standards.	RATEL	MoE CCIS	IV quarter 2023.	RATEL	MoI Programme 1408 PA 0001 EK 512			
3.1.5. Development of guidelines on the basic level of safeguards for small and medium-sized enterprises	MTTT		IV quarter 2022.	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			
3.1.6. Development, harmonisation and expansion of specialised information security courses and programmes on universities and other higher	MESTD		IV quarter 2023.	Budget of RS (regular funding)				

education institutions								
3.1.7. Creating courses, seminars and lectures on the topic of information security for students in non-technical study programmes such as law, management etc.	MESTD	MoI	IV quarter 2023.	Budget of RS (regular funding)				
3.1.8. Setting up a platform for awareness-rising and improvement of knowledge on information security through interactive programmes (Cybersecurity Awareness Platform)	RATEL	MTTT	IV quarter 2023.	RATEL	/	10,000,000	2,000,000	

Measure 3.2:	Improvement of cooperation and strengthening capacities of the ICT systems of particular importance for application of safeguards						
Institution responsible for implementation:	MTTT						
Implementation period:	2021 – 2023			Type of the measure:		Informational and educational	
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023
3.2.1 Number of trained employees in ICT systems of particular importance	Number	MTTT RATEL MoI CERT reports	120	2020.	150	170	200

3.2.2 Number of sectoral meetings of ICT systems of particular importance	Number	MTTT report	1	2020.	4	8	12	
3.2.3 Number of annual round tables/ conferences	Number	MTTT RATEL MoI CERT reports	15	2020.	17	20	25	
3.2.4 The manners and mechanisms for strengthening the capacities of ICT systems of particular importance established	Number	MTTT report	0	2020.	/	/	1	
3.2.5 Materials (brochures, recommendations etc.) developed	Number	RATEL MoI CERT reports	199	2020.	80	80	80	
3.2.6 Platform developed for information exchange between the National CERT and ICT systems of particular importance		RATEL report	No	2020.	/	Yes	/	
3.2.7 The number of overviews of threats for the National CERT	Number	RATEL report	1	2020.	2	2	2	
3.2.8 Regulations in the field of information security amended	Number	MTTT report	0	2020.	0	2	2	
3.2.9 A self-evaluation form developed	Number	MTTT report	0	2020.	0	1	1	
3.2.10 A form to assess the level of development of information security developed	Number	MTTT report	0	2020.	0	1	1	
Source of financing for the measure	Reference to programme budget		Total estimated funds in RSD					
			2021	2022	2023			
Revenue from the budget	MoI Programme 1408 PA 0001 EK 423		600,000	360,000	360,00			
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023

3.2.1.	Trainings for employees in ICT systems of particular importance on application of safeguards and acting in case of incidents in ICT systems	RATEL	NAPA MTTT	IV quarter 2023.	Budget of RS (regular funding)	NAPA Programme 0615 PA 0001 EK 411			
3.2.2.	Organisation of meetings of ICT systems of particular importance according to the sectors to which they belong with the aim of encouraging cooperation and promoting formation of special sectoral CERTs	MTTT		IV quarter 2023.	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			
3.2.3.	Organisation of international and national meetings, round tables and conferences with the aim of raising awareness of the importance of information security.	RATEL	MTTT MoI CERT NAPA		RATEL		/	1,000,000	1,500,000
3.2.4.	Determining manners and mechanisms for strengthening the capacities of ICT systems of particular importance to achieve the necessary level of compliance with	MTTT		IV quarter 2023.	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			

	information security requirements (common criteria) within management of all stages of the lifecycle of ICT systems or parts of the systems								
3.2.5.	Preparation of brochures, recommendations and other materials with the aim of rising awareness of the importance of application of safeguards	RATEL			RATEL				
			MoI	IV quarter 2023.	Budget of RS	MoI Programme 1408 PA 0001 EK 423	600,000	360,000	360,000
3.2.6.	Development of a platform for information exchange between the National CERT and ICT systems of particular importance with the aim of providing information on current risks and threats in the field of information security and promoting good practice examples	RATEL		IV quarter 2023	RATEL				
3.2.7.	Development of an overview of threats based on submitted statistics on incidents and reported incidents	RATEL		IV quarter 2023	RATEL				
3.2.8.	Harmonisation of legislation with EU	MTTT		IV quarter 2023	Budget of RS (regular funding)	MTTT			

regulations in the field of information security					Programme 0703 Function 460 PA 0008 EK 411			
3.2.9. Development of a self-evaluation form for ICT systems of particular importance	MTTT		IV quarter 2023	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			
3.2.10. Development of a form to assess the level of development of information security in Serbia	MTTT		IV quarter 2023	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			

Measure 3.3:	Strengthening capacities of the National CERT, govCERT and CERT of independent ICT system operators						
Institution responsible for implementation:	RATEL						
Implementation period:	2021 – 2023			Type of the measure:		Informational and educational	
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023
3.3.1 Number of trained employees in the NCERT	Number	RATEL report	6	2020.	6	7	8
3.3.2 Number of trained employees in govCERT and in independent ICT operators	Number	Reports of ITE and independent ICT operators	35	2020.	35	40	45
3.3.3 Number of established CERTs of independent operators	Number	MoD MFA MSA reports	2	2020.	2	2	3
		MIA report	0	2020.			1
3.3.4 Guidelines developed	Number	MTTT MoI CERT reports	0	2020.			Yes

3.3.5 Mechanisms established for information exchange	Number	RATEL report	No	2020.		Yes	
3.3.6 Cooperation established between the NCERT, the MTTT and the MoI (Emergency Management Sector)	Number	MTTT RATEL MoI reports	No	2020.	Yes		
3.3.7 Number of organised civil and military exercises	Number	MoD MoI RATEL reports	3	2020.	4	5	6
3.3.8 A systems for detection of cyber threats established	Number	RATEL report	No	2020.		Yes	
Source of financing for the measure	Reference to programme budget	Total estimated funds in RSD					
		2021	2022	2023			
Revenue from the budget	MoI Programme 1408 PA 0001 EK 423	2,352,000	2,400,000	2,400,000			
	MFA Programme 0301 PA 0003 EK 423	600,000	600,000	600,000			
	MoD Programme 1703 PA 0001 EK 423	5,556,180	/				
	SIA	1,000,000	2,000,000	2,000,000			
	MFA Programme 0301 PS 0003 EK 411	2,961,000	5,922,000	5,922,000			
	MFA Programme 0301 PS 0003 EK 412	493,000	986,000	986,000			
	MFA Programme 0301 PS 0003 EK 512	685,000	/	/			
	Activities:					Total estimated funds by sources in RSD	

	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	2021	2022	2023
3.3.1. Training for employees in the National CERT with the aim of strengthening capacities for acting in case of incidents	RATEL		IV quarter 2023	Budget of RS (regular funding)		2,000,000	2,000,000	2,000,000
3.3.2. Training for employees in govCERT and in independent operators.	Independent ICT operators	ITE	IV quarter 2023	Budget of RS (regular funding)	ITE Programme 0614 PA 0002 EK 411			
		MoI	IV quarter 2023	Budget of RS	MoI Programme 1408 PA 0001 EK 423	2,352,000	2,400,000	2,400,000
		MFA	IV quarter 2023	Budget of RS	MFA Programme 0301 PA 0003 EK 423	600,000	600,000	600,000
		MoD	IV quarter 2023	Budget of RS	MoD Programme 1703 PA 0001 EK 423	2,492,830	/	/
		SIA	IV quarter 2023	Budget of RS		1,000,000	2,000,000	2,000,000
		MSA	IV quarter 2023	Budget of RS (regular funding)				
		MIA	IV quarter 2023	Budget of RS (regular funding)				

3.3.3. Establishing of CERT of independent ICT system operators in Serbia	Independent ICT operators	MoD	IV quarter 2021	Budget of RS	MoD Programme 1703 PA 0001 EK 423	1,099,800	/	/
		MFA	IV quarter 2023	Budget of RS	MFA Programme 0301 PS 0003 EK 411	2,961,000	5,922,000	5,922,000
			IV quarter 2023	Budget of RS	MFA Programme 0301 PS 0003 EK 412	493,000	986,000	986,000
			IV quarter 2023	Budget of RS	MFA Programme 0301 PS 0003 EK 512	685,000	/	/
			MSA	IV quarter 2023	Budget of RS (regular funding)			
		MIA	IV quarter 2023	Budget of RS (regular funding)				
3.3.4. Development of guidelines for acting in case of high and very high risk incidents.	MTTT	MoI	IV quarter 2023	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			
3.3.5. Establishing a mechanism for information exchange and cooperation between individual CERTs and the National CERT	RATEL		IV quarter 2023	RATEL				

3.3.6.	Establishing cooperation between the National CERT, the MTTT and the Emergency Management Team of the MoI (Emergency Management Sector) for the purpose of recognising a cooperation mechanism in case of very high risk incidents	MTTT	MoI RATEL	IV quarter 2023	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			
3.3.7.	Organisation of civil and military exercises	MoD	MoI MTTT MFA	IV quarter 2023	Budget of RS	MoD Programme 1706 PA 0001 EK 423	2.026.550		
			RATEL		RATEL		200,000	300,000	500,000
3.3.8	Setting up of a system for detection of cyber threats	RATEL		IV quarter 2022	RATEL		4,000,000	400,000	4,000,000

Measure 3.4:	Strengthening capacities of the information security inspectorate						
Institution responsible for implementation:	MTTT						
Implementation period:	2021 – 2023			Type of the measure:		Informational and educational	
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023
3.4.1 Number of trainings attended by inspectors	Number	MTTT report	7	2020.	7	8	9
3.4.2 Number of employed inspectors	Number	MTTT report	1	2020.	1	2	3

Source of financing for the measure	Reference to programme budget		Total estimated funds in RSD					
			2021	2022	2023			
Revenue from the budget	MTTT Programme 0703 Function 460 PA 0008 EK 423		200,000	200,000	200,000			
	MTTT Programme 0703 Function 460 PA 0008 EK 411		420,000	840,000	840,000			
	MTTT Programme 0703 Function 460 PA 0008 EK 412		179,100	358,200	358,200			
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023
3.4.1. Training for information security inspectors based on prepared needs assessments for trainings with the aim of strengthening capacities for implementation of the Law on Information Security	MTTT		IV quarter 2023	Budget of RS	MTTT Programme 0703 Function 460 PA 0008 EK 423	200,000	200,000	200,000
3.4.2. Employment of information security inspectors	MTTT		IV quarter 2023	Budget of RS	MTTT Programme 0703 Function 460 PA 0008 EK 411	420,000	840,000	840,000

					MTTT Programme 0703 Function 460 PA 0008 EK 412	179,100	358,200	358,200
--	--	--	--	--	---	---------	---------	---------

Measure 3.5:		Promoting public-private partnership in the field of information security						
Institution responsible for implementation:		MTTT						
Implementation period:		2021 – 2023			Type of the measure:		Informational and educational	
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023	
3.5.1 Expert working group formed	Number	MTTT report	1	2020.	1	1	1	
3.5.2 Number of meetings of the “Cyber Security Network” foundation with the aim of promoting public-private partnership Number	Number	MTTT report	1	2020.	1	3	3	
3.5.3 Number of cooperation agreements concluded	Number	Reports of relevant ministries	0	2020.	1	2	3	
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023
3.5.1. Formation of an expert working group named Information Security Coordination Body.	MTTT		IV quarter 2023	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			
3.5.2. Organisation of meetings of the “Cyber Security	MTTT		IV quarter 2023	Budget of RS (regular funding)	MTTT Programme 0703			

Network” foundation					Function 460 PA 0008 EK 411			
3.5.3. Concluding cooperation agreements between public authorities and private and non-governmental sectors with the aim of implementing projects in the field of information security	MTTT		IV quarter 2023	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			

Measure 3.6:	Improvement of regional and international cooperation						
Institution responsible for implementation:	MTTT						
Implementation period:	2021 – 2023			Type of the measure:		Informational and educational	
Measure indicator (<i>result indicator</i>)	Measurement unit	Verification source	Baseline value	Base year	Target value in 2021	Target value in 2022	Target value in 2023
3.6.1 Number of concluded bilateral and multilateral agreements	Number	MTTT NCERT reports	0	2020.	1	2	3
3.6.2 Number of attended international forums and meetings (UN, OSCE, GFCE etc.)	Number	MTTT report	6	2020.	7	9	11
3.6.3 Number of listed, accredited and certified CERTs on the Trusted Introducer List and the number of FIRST members or associate members	Number	Trusted Introducer List Report FIRST report	7	2020.	7	8	9
Source of financing for the measure	Reference to programme budget		Total estimated funds in RSD				
			2021	2022	2023		
Revenue from the budget	MoI Programme 1408		700,000	700,000	700,000		

		PA 0002 EK 422						
Activities:	Authority implementing the activity	Authorities-partners in implementation of activities	Deadline for completion of activities	Source of financing	Reference to programme budget	Total estimated funds by sources in RSD		
						2021	2022	2023
3.6.1. Conclusion of bilateral and multilateral cooperation agreements in the field of information security	MTT	RATEL	IV quarter 2023	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			
3.6.2. Participation of representatives of competent authorities in international forums and meetings dedicated to information security within the UN, OSCE, GFCE and other international organisations.	RATEL	MTTT MoI MFA MoD RATEL ITE	IV quarter 2023	RATEL		1,000,000	2,000,000	2,500,000
		MoI	IV quarter 2023	Budget of RS	MoI Programme 1408 PA 0002 EK 422	700,000	700,000	700,000
3.6.3. Cooperation with EU institutions and organisations competent for the field of information security (FIRST, ENISA, EU CERT Network etc.)	MTTT	RATEL ITE MFA MoI CERT	IV quarter 2023	Budget of RS (regular funding)	MTTT Programme 0703 Function 460 PA 0008 EK 411			

ABBREVIATIONS

AMRES	Academic Network of the Republic of Serbia
SIA	Security Information Agency
MSA	Military Security Agency
MIA	Military Intelligence Agency
ICT	Information and communication technologies
ITE	Office for IT and Electronic Government
MPALSG	Ministry of Public Administration and Local Self-Government
MoD	Ministry of Defence
MoE	Ministry of Economy
MESTD	Ministry of Education, Science and Technological Development
MFA	Ministry of Foreign Affairs
MTTT	Ministry of Trade, Tourism and Telecommunications
MoI	Ministry of the Interior
MSMEs	Micro, small and medium-sized enterprises
NAPA	National Academy for Public Administration
NBS	National Bank of Serbia
NCERT	National Computer Emergency Response Team
CCIS	Chamber of Commerce and Industry of Serbia
RAS	Development Agency of Serbia
RNIDS	Register of the National Internet Domain of Serbia
RATEL	The Regulatory Agency for Electronic Communications and Postal Services
SORS	Statistical Office of the Republic of Serbia
FDI	Foreign direct investment
IF	Innovation Fund
govCERT	Government Computer Emergency Response Team
CDT	Centre for Digital Transformation