BACKGROUND

Total Population: 9 847 000

Internet users, percentage of population: 51.50%
(data source: ITU Statistics, December 2012)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION
Specific legislation pertaining to cybercrime is mandated through the following legal instrument:
- Criminal Code art. 298-304

1.1.2 REGULATION AND COMPLIANCE
Serbia does not have any specific legislation and regulation regarding cybersecurity and compliance requirements.

1.2 TECHNICAL MEASURES

1.2.1 CIRT
ITU conducted a CIRT readiness assessment for Serbia in 2010. Serbia has not yet established and legally mandated a national CERT. However the following institutions’ tasks are connected to CERT functions.
- Administrative Agency for Joint Service of Government Authorities performs the tasks of managing security risks in information-communication systems of public administration bodies, protecting the public administration network and data, cooperation and coordination related to information security.
- The Academic Network of the Republic of Serbia (AMRES) is a public institution that performs the CERT activities for the educational and scientific-research institutions in the Republic of Serbia.

1.2.2 STANDARDS
Serbia does not have any officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION
Serbia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY
Serbia does not have any officially recognized national cybersecurity strategy. However Serbia adopted a development strategy for Information Society in the Republic of Serbia by 2020 which has six priorities for development. One of the strategy priorities is Information Security, which will have to be developed by improving legal and institutional framework, critical infrastructure protection, fight against cybercrime and scientific, research and development work.
1.3.2 ROADMAP FOR GOVERNANCE
The Action plan (2013-2014) determines activities for the cybersecurity improvement in Serbia. The competent institution for proposing strategic and action plan documents in the area of information society is Ministry of Trade, Tourism and Telecommunications.

1.3.3 RESPONSIBLE AGENCY
The Ministry of Trade, Tourism and Telecommunications is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING
Serbia does not have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT
Serbia does not yet have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT
Serbia does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION
The Academic Network of the Republic of Serbia (AMRES) team members are certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION
The Academic Network of the Republic of Serbia (AMRES) is the official certified government and public sector agency certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION
Serbia does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.

1.5.2 INTRA-AGENCY COOPERATION
Serbia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP
Serbia does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

1.5.4 INTERNATIONAL COOPERATION
Serbia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Serbia participated in the second conference of South-Eastern Europe National Security Authorities (SEENSA) and the Serbian NSA participated on the third conference about information security and cybernetic defence “ISCD 2013” in Hungary.
2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY
Specific legislation on child protection has been enacted through the following instruments:
- Article 185 of the Criminal Code.
- Articles 54 and 55 of the Law on Amendments and Additions to the Criminal Code, n. 72/09.

2.2 UN CONVENTION AND PROTOCOL
Serbia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.
Serbia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT
Serbia does not have any officially recognized agency that offers institutional support on child online protection.

2.4 REPORTING MECHANISM
The Safer Internet Hotline “Net Patrol” provides an online form to report illegal content.

-----------------------------------------------------------------------------------------------------------------------------

DISCLAIMER: Please refer to http://www.itu.int/en/Pages/copyright.aspx
More information is available on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
Last updated on 27th November 2014