BACKGROUND

Total Population: 5,593,000

Internet users, percentage of population: 94.6297%
(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION
Specific legislation on cybercrime has been enacted through the following instrument:
- Penal Code.

1.1.2 REGULATION AND COMPLIANCE
Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:
- Ecommerce Act
- Law on Electronic Signatures
- Act on Processing of Personal Data
- Law on Electronic Communications Networks and Services
- Act on Processing of Personal Data by the Operation of the Government.

1.2 TECHNICAL MEASURES

1.2.1 CIRT
Denmark has an officially recognized national CIRT known as GovCERT.DK. There is an ISP customer base CIRT known as CSIRT.DK and an educational and research CIRT known as DKCERT.

1.2.2 STANDARDS
Denmark does not have any officially approved national cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION
Denmark is a member of the CCRA which provides officially approved national cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY
Danish cyber strategy is defensive and focused on protecting military computer systems from exploitation or disruption, without an explicit focus on developing offensive or response mechanisms. Denmark is preparing a new cyber security strategy.

1.3.2 ROADMAP FOR GOVERNANCE
Denmark does not currently have any national governance roadmap for cybersecurity.
1.3.3 RESPONSIBLE AGENCY
The GovCERT.DK and the Center for Cyber Security are the officially recognized institutions responsible for implementing a national cybersecurity strategy, policy and roadmap.

1.3.4 NATIONAL BENCHMARKING
In Denmark the Center for Cyber Security produces an officially recognized national benchmarking report used to measure cybersecurity development. The Danish Defense Intelligence Service also makes an annual intelligence assessment of conditions abroad affecting Danish security, referring to the appropriate risk assessment.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT
Center for Cyber Security’s publications include guides, forms and templates that are relevant to authorities and the telecommunications industry. This is the officially recognized national or sector-specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT
Computer Security is a new DTU programme which will benefit public and private sectors alike. The programme comprises—among other things—a special competence course in cyber security, which the Danish Defense Intelligence Service’s Cyber Security Center, Copenhagen Finance IT Region (CFIR) and IBM have helped to realize.

1.4.3 PROFESSIONAL CERTIFICATION
There is no information on the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity for Denmark.

1.4.4 AGENCY CERTIFICATION
There is no information of any government and public sector agencies that are certified under internationally recognized standards in cybersecurity in Denmark.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION
Center for Cyber Security collaborates with private and public stakeholders at home and abroad to facilitate sharing of cybersecurity assets across borders, working with various CIRTS of different countries and intelligence agencies amongst others. Also participates in: - EU - NATO.

1.5.2 INTRA-AGENCY COOPERATION
Center for Cyber Security establishes a contact with representatives of relevant ministries and authorities to dialogue on the identification of critical ICT infrastructure and to ensure coordination of cyber security in Denmark. There is also in place an MoU between the members of the ISP Security Forum, DK-CERT and GovCERT to combat botnets.

1.5.3 PUBLIC SECTOR PARTNERSHIP
Center for Cyber Security has established a forum for cooperation with public and private owners and providers of ICT infrastructure. The Forum will contribute to the dialogue on security of critical ICT infrastructure and support this work.
1.5.4 INTERNATIONAL COOPERATION
To facilitate sharing of cybersecurity assets across borders or with other nation states, Denmark has officially recognized partnerships with the following organizations: -DKCERT is a member of:
- FIRST - EU - NATO - ENISA.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION
Specific legislation on child online protection has been enacted through the following instrument:
-S235 of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL
Denmark has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Denmark 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
There is no information on the institutional support in for online child protection in Denmark.

2.4 REPORTING MECHANISM
Child pornography on the internet can be reported by a form filled in the National Police (*) website. Save the Children Denmark also provides a space to report child abuse images on the internet.

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

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 January 2015