



# CYBERWELLNESS PROFILE THE NETHERLANDS



## BACKGROUND

**Total Population:** 16 714 000

(data source: [United Nations Statistics Division](#), December 2012)

**Internet users, percentage of population:** 93.9564%

(data source: [ITU Statistics](#), 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:

- Electronic Signature Law      - Decision on Electronic Signatures      - [Data Protection Act](#).

### 1.2 TECHNICAL MEASURES

#### 1.2.1 CIRT

Until the [National Cyber Security Centre](#) was set up, [GOVCERT.NL](#) was the government organization dedicated to cyber security and incident response. The tasks and employees of [GOVCERT.NL](#) have all been transferred to the Center. This has ensured that the [NCSC](#) has had a sound foundation from the beginning. Therefore [NCSC](#) is the nationally recognized CIRT.

#### 1.2.2 STANDARDS

There is no information on any internationally recognized standards used in The Netherlands. However, [The Netherlands' iStrategy](#) will make generic frameworks, services and products available to all Central Government organizations.

#### 1.2.3 CERTIFICATION

The Netherlands 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

The Netherlands has adopted [The National Cyber Security Strategy \(NCSS\)](#), [National Cyber Security Strategy 2](#) and [The Defense Cyber Strategy](#) as its national cybersecurity strategies.

#### 1.3.2 ROADMAP FOR GOVERNANCE

The Netherlands has a nationally recognized governance roadmap for cybersecurity: [2014-2016 Action Programme Annex 1 to the NCSS 2](#).

#### 1.3.3 RESPONSIBLE AGENCY

The following are the officially recognized agencies responsible for implementing the national cybersecurity strategy, policy and roadmap:

- [National Coordinator for Security and Counterterrorism \(NCTV\)](#)

- [NCSC](#).

### 1.3.4 NATIONAL BENCHMARKING

The Netherlands has officially recognized the [Cybersecurity Assessment Netherlands \(CSBN\)](#) as the body responsible for the national benchmarking exercises or referential used to measure cybersecurity development.

## 1.4 CAPACITY BUILDING

### 1.4.1 STANDARDISATION DEVELOPMENT

The [NCSC](#) is the officially recognized national agency responsible for research and development (R&D) programs/projects for cybersecurity standards and best practices and guidelines to be applied in either the private or the public sector. It fulfils this function by collecting [knowledge and expertise](#) in the field of cybersecurity from all sectors of society, both practical knowledge and data from scientific research. The government, businesses and universities are able to pool their knowledge in the Center.

### 1.4.2 MANPOWER DEVELOPMENT

[NCSC](#)'s [Expertise & Advice and Sharing knowledge](#) is recognized as the national program for raising awareness and promoting cybersecurity especially educational programs among the public and private sectors.

### 1.4.3 PROFESSIONAL CERTIFICATION

There is no record of how many professionals are certified under internationally recognized certification programs in cybersecurity.

### 1.4.4 AGENCY CERTIFICATION

[NCSC](#) is the certified government and public sector agency certified under internationally recognized standards in cybersecurity.

## 1.5 COOPERATION

### 1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, the Netherlands has officially recognized partnerships with the following organizations:

- [EGC](#)

- [CSIRT](#).

### 1.5.2 INTRA-AGENCY COOPERATION

Various agencies are able to share cybersecurity assets in The Netherlands through the High-Tech Crime Unit of the [Dutch Police Services Agency \(KLPD\)](#) and through the [NCSC](#).

### 1.5.3 PUBLIC SECTOR PARTNERSHIP

The Netherlands has an officially recognized national [program](#) for sharing cybersecurity assets within the public and private sector.

### 1.5.4 INTERNATIONAL COOPERATION

The [NCSC](#) is a member of the following:

- [FIRST](#)

- [TERENA](#)

- [ENISA](#)

- [EGC](#).

The Netherlands is involved in [international cooperation](#) with many other agencies.

## 2. CHILD ONLINE PROTECTION

### 2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instrument:

- [Article 240b](#) of the Criminal Code.

## 2.2 UN CONVENTION AND PROTOCOL

The Netherlands has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the [Convention on the Rights of the Child](#).

The Netherlands 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

The Government Computer Emergency Response Team of the Netherlands ([GOVCERT.NL](#)), merged with the [NCSC](#), provides information on internet safety. The [DigiAware](#) Program, supported by the Ministry of Economic Affairs, Agriculture and Innovation, provides information about internet safety.

## 2.4 REPORTING MECHANISM

Online illegal content can be reported in the website of [Meldpunt](#).

---

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 22<sup>th</sup> January 2015