[Ref: CL-19/47](https://www.itu.int/md/S19-SG-CIR-0047/en) - **Participation in the process for developing guidelines for utilization of the Global Cybersecurity Agenda**

**Contribution submitted by Cameroon**

**CAMEROON CYBER WELLNESS PROFILE**

**BACKGROUND**

**POPULATION TOTAL (26 000 000)
Internet users, Percentage of population : 45 percent.**

1. **CYBERSECURITY**

**1.1 LEGAL MEASURES**

**1.1.1 CRIMINAL LEGISLATION**

The following are implemented in Cameroon :

- THE CAMEROON PENAL CODE; Law No 2016/007 of 12 July 2016 relating to the Penal Code: https://www.prc.cm

**https://www.antic.cm**

-Law n°2010/012 of 21 December 2010 relating to Cybersecurity and Cybercriminality in Cameroon.

-Law n°2015/006 of 20 April 2015 modifying and complementing provisions for Law n° 2010/013 Governing Electronic Communications in Cameroon.

-Law n°2010/013 of 21 December 2010 Governing Electronic Communications in Cameroon.

-Law n°2010/002 of 21 December 2010 Governing Electronic Commerce in Cameroon.

-Law n°2011/012 of 6 May 2011, on the Protection of Consumers in Cameroon.

**1.1.2 REGULATION AND COMPLIANCE (**[**https://www.antic.cm**](https://www.antic.cm)**): The following texts and decrees ensure regulation and compliance.They include:**

1-Decree N°2012/1318/PM Laying down Conditions and Modalities for Granting Authorizations to Carry Electronic Certification Activities.

2-Decree N° 2012/309 of 26 June 2012 Laying down Modalities for Managing the Special Funds for Electronic Security Activities.

3-Decree N° 2012/308 of 26 June 2012 Laying down Modalities for Managing the Special Funds for Telecommunications.

**1.2 TECHNICAL AND PROCEDURAL MEASURES**

**1.2.1 TECHNICAL MEASURES**

a) Security Toolkit

The security toolkit consist of:

Microsoft Security Essential x64, x86, Antivirus and 360 security (mobile);

Ciphering (encryption 25 MB);

Firewall (Comodo internet security 21 MB);

USB key protection;

Parental Control: K9 Webprotection 3MB, Control kid 4 MB; Q studio 2MB;

Qustodio (Android) 20MB. Malware detection (Malwarebyte Antimalmware 22MB);

Network Monitoring PRTG Network monitor 180 MB. Proxy (Proxi switch standard 6MB); Recover (Recovery of erased data);

Detection of Microsoft windows vulnerability (Microsoft baseline security analyser 2MB)

(Software programs and applications that serve as anti-virus,

**b) Security Alerts: SECURITY BULLETINS**

Security alerts are published in the site: <https://www.antic.cm/index.php/fr/cybersecurete/alerts.html>,

<https://www.antic.cm/index.php/en/>

https://www.antic.cm/indix.php/fr.

**c) Security Best Practices: 10 COMMANDMENTS OF INTERNET SECURITY;**

1) Use quality passwards

2) Have an operating system and updated software (browser, antivirus, desktop, personal firewall). Etc.

3) Do regular updates;

4) Deactivate active X and Javascript component.

5) Don’t be in a haste to click on links.

6) Never use an administrative account to navigate.

7) Control the dissemination of personal information.

8) Never leave jokes.

9) Be careful.

10) Be careful while opening attachments to Email (they often have malicious codes). 11) Other security best practices.

**1.2.2 CIRT**

Cameroon has a Government CIRT which is being managed by **the National Agency for Computer and Communication Technologies (ANTIC).**

**1.2.3 STANDARDS**

Some national standard have been developed by ANTIC: https:www.antic.cm, which can be implemented at global level.

**1.2.4 CERTIFICATION**

Electronic certification is carried out by the **National Agency for Computer and Communications Technologies** **(ANTIC**) under the supervision of the **Ministry of Posts and Telecommunications (MINPOSTEL)**. Cameroon has a Public Key Infrastructure which is being managed by **ANTIC** since October 2012.

**1.2.5 SECURITY AUDITS**

Security audits are carried out by authorized security auditors yearly in both government and private institutions under the control of ANTIC and supervision of MINPOSTEL.

**1.3 ORGANIZATIONAL STRUCTURES**

 **1.3.1 POLICIES**

Cameroon has an official Cybersecurity Policy and a Cybersecurity Strategy yet to be officially approved since December 2018.

* + 1. **INSTITUTIONS**

Presidential Decree N°2012/180 of 10 April 2012 Organizing the functioning of ANTIC, states the missions of ANTIC conforming to Sections 90, paragraph 2 of Law N°2015/006 Governing Electronic Communications in Cameroon. These missions are related to:

-Security Audit;

-Security Monitoring (Intelligence);

-Electronic Certification;

-Internet Regulation.

ANTIC works in collaboration with other state institutions such as: the **Judicial Police** and the **Ministry of Justice.**

**1.3.3 SOC (Security Operations Center)**

Within the framework of the cybersecurity policy and cybersecurity strategy, Cameroon officially intends to construct a national SOC (Security Operations Center) by 2020 to coordinate all national CIRTs and to cooperate with regional and international SOCs and CIRTS.

The Terms of Reference is ready meanwhile funding is still being expected.

**1.4 CAPACITY BUILDING**

Cameroon regularly organizes forum on cybersecurity, fight against cybercriminality and cyber terrorism as: from **24th to 27th February 2015** in collaboration with the CTO, ITU, INTERPOL, AfricaCERT, IMPACT private companies, Universities and NGOs.

 Another forum on cybersecurity, fight against cybercriminalty and cyberterrorism is scheduled this year 2020.

 Also, the National Advanced School of Post and Telecommunications (NASPT) has designed a Master’s Program in Cybersecurity.

 A cybersecurity laboratory has been installed in **The National Advanced School of Engineering (Ecole Normal Superieur Politechnique), at the University of Yaoundé I.**

 Cameroon also organizes:

-Training seminars on cybersecurity;

-Training on Personal Data Protection;

-Training seminar on risk assessment of CII, and Identification of Critical Information Infrastructure, and CIIP.

**1.5 INTERNATIONAL CO-OPERATION**

Cameroon sometimes organizes and also participate in regional and international seminars, conferences, forums and summits in cybersecurity with stake holders such as: ITU, CTO, IMPACT, INTERPOL, AfricaCERT, NGOs and private companies.