

TEMPLATE FOR SUBMISSION OF CONTRIBUTIONS



2020 Regional Development Forum for Africa (RDF-AFR)

*Digital transformation to accelerate achievement of the SDGs
– Digital development, partnerships and funding*

6-7 October 2020, 12:00 – 15:00 CAR (Virtual meeting)

with preparatory break-out sessions on 5 October 2020 (12:00 – 13:30 CAT time)

CONTRIBUTION BY BOCRA, Botswana

TITLE: Cybersecurity initiatives

EXPECTED DURATION OF PRESENTATION: [5 minutes]

CONTACT: Emmanuel Thekiso, Thekiso@BOCRA.ORG.BW, +267 73111260

❖ **Africa Regional Initiatives:** [Select the Regional Initiative(s) relevant for your contribution]

[No] AFR Regional initiative 1 – Building digital economies and fostering innovation in Africa

[No] AFR Regional initiative 2 – Promotion of emerging broadband technologies

[Yes] AFR Regional initiative 3 – Building trust and security in the use of telecommunications/
information and communication technology

[No] AFR Regional initiative 4 – Strengthening human and institutional capacity building

[No] AFR Regional initiative 5 – Management and monitoring of the radio-frequency spectrum
and transition to digital broadcasting

❖ **Related ITU development thematic:** [Select the thematic area(s) relevant for your
contribution]

[Yes/No] Networks and digital infrastructure

[Yes/No] Cybersecurity

[Yes/No] Emergency telecommunications

[Yes/No] Environment

[Yes/No] Digital policy and regulation

[Yes/No] Capacity development

[Yes/No] Digital services and applications

[Yes/No] Digital inclusion

[Yes/No] Digital innovation ecosystems

[Yes/No] Statistics and data for evidence-based decision making

❖ **Year(s) of implementation:** [Select the year(s) for which your action/project/initiative is
relevant]

[Yes/No] 2018	[Yes/No] 2019	[Yes] 2020	[Yes] 2021	[Yes/No] Others

TEMPLATE FOR SUBMISSION OF CONTRIBUTIONS

- ❖ **COVID-19 response related initiative:** [Please indicate if your action/project/initiative is relevant for COVID-19 response]

[Yes/No] **COVID-19 response related initiative**

Botswana Communications Regulatory Authority (BOCRA) regulates the communications sector in Botswana, comprising telecommunications, internet and ICTs, radio communications, broadcasting, postal services and related matters. Steps taken to help during the coronavirus pandemic include:

- As the COVID-19 Pandemic cases increases in Botswana and in other countries, BOCRA encouraged many companies to allow employees to work from home to curb the spread of the disease and to follow procedures as laid down by the Government on COVID-19 pandemic. BOCRA encouraged companies to create more secure platforms like virtual private network (VPN) or a secure home network with strong end-to-end encryption to facilitate working from home.
- Encouraging the use of online platforms to access BOCRA services, such as payment and licensing.
- Issuing a public notice, which warned the public of the need to be vigilant and not to spread fake news and misinformation. It also warned of sites containing misleading health information related to COVID-19, and encouraged the public to report any suspected content to the police.

Background [max 300 words]

The Ministry of Transport and Communications (MTC) developed the National Cybersecurity Strategy in collaboration with all the relevant stakeholders from the Private Sector, relevant Ministries, Regulator, and Academia. The Commonwealth Telecommunications Organisation (CTO) assisted in the development of the National Cyber Security Strategy with funding from the Foreign & Commonwealth Office (FCO) of the Government of United Kingdom of Great Britain. In addition, the project team that developed National Cyber Security Strategy benefited from inputs and comments from the State Department of the United States of America (USA), through the technical consultant from MITRE and Carnegie Melon University.

The National Cybersecurity Strategy clarifies the roles of the various stakeholders and outlines various action plan to be carried out to ensure that the country is cybersecurity secure. The Strategy recommends the establishment of Computer Incidence Response Team (CIRT) as a matter of urgency due to rising and complexity of cybersecurity threats and attacks. To ensure a secure cyberspace for Botswana, MTC requested BOCRA to establish a Communications Sector CIRT (either Herein referred to interchangeably as COMM-CIRT or the CIRT) to ensure that the communication sector, both private and public, are secure. The COMM-CIRT also acts as cybersecurity focal point. COMM-CIRT will assume National cybersecurity responsibilities in the interim, while awaiting the establishment of National CIRT (BWCIRT). The COMM-CIRT have been developed with the assistance of the International Telecommunications Union. Cyber for Development (Cyber4Dev), a European Union based program under the Cyber4Dev Program assisted in capacity building of the CIRT team.



TEMPLATE FOR SUBMISSION OF CONTRIBUTIONS

Proposal [max 400 words]

In national cybersecurity strategy framework, BOCRA will draft a national child online protection strategy. partners and funding are still to be determined.

Child online Protection (COP) project aims at protecting children and other vulnerable groups against cyber threats. The project involves creating an outreach program for specific target groups mainly Children, determine the role of governments and international organizations in cybersecurity and child online protection; Develop national cybersecurity strategies; Policy and regulatory framework for child online protection; Organizational and technical tools for child online protection; Capacity building in the field of cybersecurity and child online protection; Child online should have a well-defined communication plan, cybersecurity Protection Guidelines and proper information sharing mechanism.

Child Online Protection involves engagement of all stakeholders nationwide either through campaigns, conferences and workshop incorporating schools, colleges, vulnerable groups, disseminate information on the correct and safe use of the internet, and reduce illegal and harmful content on the Internet, to combat online harassment, as well as to inform children, parents and guardians about the risks of the online environment and the possibilities of avoiding them.

The project aims to include parents as they are the ones supposed to protect children online and, in most cases, they are not aware of how their children are exposed online and do not apply protective measures. This project will assist Botswana to conduct Child online Protection with national assessments and propose action plans, educational materials, software, to strengthen the child online protection environment and infrastructure and to learn from best practises adopted by other countries.

PLEASE SUBMIT THE CONTRIBUTION BY 15 SEPTEMBER TO ITU-RO-AFRICA@ITU.INT

