



**ITU Centre of Excellence Network for Africa
National Computer Board / Computer Emergency Response Team of
Mauritius**

Training course outline

| | |
|-----------------------|---|
| Title | Implementation of UN Cyber Norms with a focus on the protection of Critical Infrastructure and Incident Response Teams |
| Modality | Online |
| Dates | 26 – 28 October 2022 |
| Duration | 3 days |
| Registration deadline | 21 October 2022 |
| Training fees | No charge |
| Description | <p>Global digital growth is continuing to fundamentally transform the lives of people, businesses and institutions, bringing people out of poverty, increasing wider prosperity, welfare and enabling new ways for governments and citizens to engage with each other. It is also creating a more connected world and supporting globalisation with greater access to free markets, democratic systems, prosperity and innovation.</p> <p>But as we become more reliant on cyberspace, malicious cyber activity has grown in intensity, complexity and severity over recent years, with rising incidents of cybercrime targeting critical national infrastructure, democratic institutions, business and media. There is too much at risk to allow cyberspace to become a lawless world and there is a need to setup rules and procedures to understand how international law applies to state behaviour in cyberspace just as it does to activities in other domains.</p> <p>The approved norms as part of the UN framework of responsible state behaviour in cyberspace, is a way to help develop those rules which will guide states to protect their ICT infrastructure better and engage with the others to combat cybercrime effectively in a form which is known as cyber diplomacy.</p> |
| Code | 22OI100018AFR-E |



1.LEARNING OBJECTIVES

The main objective of this training course is to allow participants to acquire essential knowledge to implement UN Norms. The focus will be specially on technical norms which applies to CERTS/CSIRTs or any other national team entrusted with the responsibility of protecting their cyberspace.

2. LEARNING OUTCOMES

This three-day instructor-led course will introduce you to the essential knowledge you need to acquire in order to implement the UN Norms such as 13 (f) (g) (h) (i) (j) &(k). Participants will also learn about the understanding of cybersecurity issues on the diplomatic agenda as well as its impact on geopolitics and digital technologies.

3.TARGET POPULATION

The target audience for this course is as follows:

- Current and future CSIRT/CIRT/CERT managers and team members
- C-level managers such as CIOs, CSOs, CROs, CISOs
- Cybersecurity professionals such as information security analysts, security engineers, incident handlers, amongst others
- Cyber Ambassadors and Diplomats

4.ENTRY REQUIREMENTS

Foundational understanding of cybersecurity and cyber diplomacy.

5.TUTORS/INSTRUCTORS

| Name of tutor(s)/instructor(s) | Contact details |
|--------------------------------|--|
| Kaleem Usmani | kusmani@cert.govmu.org |
| Selvana Naiken Gopalla | sgopalla@cert.govmu.org |
| Jennita Appanah | jappanah@cert.govmu.org |
| Manish Lobin | mlobin@cert.govmu.org |

6.TRAINING COURSE CONTENTS

Topics to be covered in this course are as follows:

- Introduction to UN Cyber Norms
 - Understanding of responsible state behaviour in cyberspace?
 - UN norms process (UN cyber groups)



- Purposes of the norms as reflected in the UNGGE Report 2021
- Importance of norms in international affairs
- Technical perspectives of the norms

- Implementation of UN Cyber Norms
 - Pre-requisites for technical norms implementation
 - Framework for norms implementation
 - Assessment process
 - Step by step process of Norms implementation
 - Role of the government in the implementation process and its importance
 - Practical guidance on the implementation of Norms 13 (f)(g)(h) (i) (j) &(k)
 - Institutions involved and tools used for the Norms implementation

7. TRAINING COURSE SCHEDULE

| Week / Session | Topic | Exercises and interactions |
|---|---|---|
| Day 1 26 October 2022 11am – 2pm (Geneva Time) | Introduction to UN Cyber Norms | Presentations Discussion Group work Case studies |
| Day 2 27 October 2022 11am – 2pm (Geneva Time) | Implementation of UN Cyber Norms- Part I | Presentations Discussion Group work Case studies |
| Day 3 28 October 2022 11am – 2pm (Geneva Time) | Implementation of UN Cyber Norms- Part II | Presentations Discussion Group work Case studies |

8. METHODOLOGY (Didactic approach)

The training will be carried out online through the ITU Academy Platform. It will include presentations, discussion, group work, case studies and an exam.

9. EVALUATION AND GRADING

An exam will be conducted at the end of the course. Participants are required to get 60% of the marks in order to pass the exam. It is also to be noted that Presentations, Discussions, Group works, and Case studies will not be graded.



10. TRAINING COURSE COORDINATION

| | |
|--|---|
| Course coordinator: Name: Manish Lobin Email address: mlobin@cert.govmu.org | ITU coordinator: Name: Email address: |
|--|---|