Republika e Kosovës
Republika Kosova-Republic of Kosovo
Qeveria-Vlada-Government

REGULATION (GRK) - No. 22/2023

ON THE DUTIES AND RESPONSIBILITIES OF THE STATE CYBER SECURITY TRAINING CENTER[1]

[1] Regulation (GRK) – No. 22/2023 on the Duties and Responsibilities of the State Cyber Security Training Center, has been approved in the 178th Meeting of the Government of the Republic of Kosovo, with the Decistion No. 15/178, dated 13.12.2023.

Government of the Republic of Kosovo

In support of Article 93 (4) of the Constitution of the Republic of Kosovo, in accordance with Article 21 paragraph (3) of Law No. 08L-173 on Cyber Security, (OG, No. 4/27.02.2023), Article 8 paragraph (4) subparagraph (4.5) of Law No. 08/L-117 on the Government of the Republic of Kosovo (OG, No. 34/18 November 2022), as well as Article 19 paragraph (6.2) of the Rules and Procedures Regulations of the Government of the Republic of Kosovo No. 09/2011, (OG, No. 15/12.09 2011),

Issues:

REGULATION (GRK) - NO. 22/2023 ON THE DUTIES AND RESPONSIBILITIES OF THE STATE CYBER SECURITY TRAINING CENTER

Article 1
Purpose

This regulation defines the duties and responsibilities of the State Training Center for Cyber Security.

Article 2
Scope

This Regulation is implemented by the MoD/ KSF and applies to other RKS institutions, identified as audience participants in trainings as well as operators of essential services and providers of digital services.

Article 3
Definitions

1. The expressions used in this Regulation have the following meaning:

1.1. **STCSC -** State Training Center for Cyber Security;

1.2. **Cyber Range** – is a cyber-attack simulation lab or environment used to conduct exercises, training and testing of security policies and procedures helping institutions improve their response to cyber-attack.

1.3. **Exercises in the field of cyber security** – are simulated activities to test the response and resilience of institutions to cyber-attacks, which serve to identify weaknesses and improve security measures in the IT system.

2. Expressions, terms and other abbreviations used in this Regulation have the same meaning as in the relevant legislation in force.

Article 4
Organizational Structure

1. The organizational structure of the STCSC consists but is not limited to:

1.1. Leadership staff ;

1.2. The coaching staff;

1.3. Support staff.

2. The internal organization and settlements of job positions is made in accordance with the applicable legislation of the MoD and the KSF, as well as other legislation in force.

Article 5

Duties and responsibilities of the STCSC

1. Designs and implements training programs in the field of cyber security.

2. In cooperation with Cyber Security Agency (next CSA), it determines the needs for training and exercises in the field of cyber security.

1. Draws up the work plan and the training program for the period of one year, based on the needs determined by paragraph 2 of this article.

2. Coordinates with state institutions, operators of essential services and providers of digital services for participation in trainings.

3. Assists state institutions, operators of essential services and digital service providers to develop suitable scenarios for their cyber operations.

4. Prepares training materials and auxiliary materials for the trainings and exercises held at STCSC.
5. Provides access to online training platforms hosted in this Center for all participating audiences.

6. Cooperates with academic institutions at the country level for the implementation of planned annual trainings.

7. Operates and maintains Cyber Range.

8. Keeps evidence for the realization of trainings.

9. Makes the after-action analysis for all trainings and exercises held at the STCSC.

10. Provides evidence of participation in training and exercises in the STCSC for all participants.

11. Cooperates with partners and allies to fulfil the centre's mission.

Article 6
Target Audience

1. STCSC offers training programs in the field of cyber security for public officials as in the following:

1.1 Civil servants employed in RKS institutions;

1.2 Public servants employed in RKS institutions;

1.3 for administrative and supporting employees who are employed in the RoK Institutions;

1.4. for employees of the Cabinet employed by the RoK Institutions due to needs and requests;

1.5. For employees of essential services and providers of digital services.

2. STCSC in cooperation with CSA organizes exercises in the field of cyber security for:

2.1. Civil servants employed in RoK institutions;

2.2. Public servants employed in RKS institutions;

2.3 for administrative and supporting employees who are employed in the RoK Institutions;

2.4. for employees of the Cabinet employed by the RoK Institutions due to needs and requests;

2.5.For employees of essential services and providers of digital services.

Article 7
Training and exercise programs

1. STCSC offers training and exercises in the field of cyber security, as follows:

1.1. Specialized training in the field of cyber security such as:

1.1.1. Training for awareness of risks in the field of cyber security;

1.1.2. Technical training on the use of specific tools, technologies and techniques to defend against cyber-attacks;

1.1.3. Training for certification programs according to international standards in the field of cyber security;

1.1.4. Personalized training that is tailored to the specific needs of an institution.

1.1.5. Trainings to share best practices with partners and allies through exchange of expertise.

1.2. Exercises in the field of cyber security at Cyber Range:

1.2.1 To practice the skills and theoretical knowledge of officials from RKS institutions as well as operators of essential services and providers of digital services;

1.2.2. To practice the interaction of RoK institutions, essential service operators and digital service providers.

1.2.3. To organize and participate with domestic, regional, and international partners to simulate cyber security challenges through joint exercises.

Article 8
Training Programs and Curricula

1. STCSC in cooperation with CSA designs training programs and curricula for all personnel engaged in the field of cyber security.

2. Based on the training programs and curricula as well as the needs and requirements of the institutions, STCSC draws up the annual plan for the implementation of trainings.

3. The training program and curricula in the field of cyber security are reviewed and updated annually.

4. The review, introduction or removal of any specific training can be done outside the time of the review of the Training Program by decision of the Minister of Defence according to the needs and requests of the users from the institutions that are the participating audience of the STCSC trainings.

Article 9
Responsibilities of the audience participating in trainings and exercises at STCSC

1. All participants in specialized trainings and exercises in the field of cyber security at STCSC must have basic knowledge in the field of cyber security in advance.

2. The relevant institutions themselves are responsible for basic training in the field of cyber security for their personnel engaged in cyber security.

3. All participants in the trainings and exercises at STCSC must be subject to the internal security rules of the Ministry of Interior and the KSF for entry/exit and daily staying within the premises of this Center.

Article 10
Forms of training

1. Depending on the type of training program, the trainings will be conducted in the following forms:

1.1. Physical presence training for training programs that participants must physically attend the designated training;

1.2. Trainings with physical presence in different locations that will be conducted by mobile teams of the STCSC trainers, for the needs of the audience participating in the STCSC trainings;

1.3. Training with online presence for training programs that participants must attend the specified training, from wherever they have access to the Internet at a specified time online ;

1.4. Online training for programs that allow participants to learn at their own pace and from anywhere they have Internet access.

Article 11
Trainers at STCSC

1. The following types of trainers are engaged in STCSC, such as:

1.1. Permanent trainers in STCSC who are positioned in STCSC, as trainers in the field of cyber security;

1.2. Internal trainers made up of civilian and military personnel within the MoD and KSF, including members of the reserve component of the KSF, as well as public officials from other institutions as needed.

1.3. External trainers are experts in fields outside the institutions of the state administration who can be engaged by MoD/KSF as trainers in the relevant fields.

1.4. International trainers are trainers who are not citizens of Kosovo and they can be engaged as needed to hold training sessions MoD/KSF.

Article 12
Engagement of trainers at STCSC

1. The permanent trainers of STCSC are selected based on an open competitive process in accordance with the relevant legislation in force.

2. Internal trainers of STCSC are selected on the basis of an open competitive process in accordance with the relevant legislation in force and their commitment is made for the implementation of the training program to provide professional experiences and skills for the staff.

3. External trainers are engaged when there is a lack of internal trainers for certain trainings, and their engagement is done in accordance with provision of "*Agreement for special Services"* based on Law on Public Officials.

4. International trainers are engaged when certain trainings cannot be provided by internal and external trainers, and their engagement is done according to Bilateral Cooperation Agreement or contracting way of them based on legal criteria.

Article 13
Entry into force

This regulation enters into force seven (7) days after being signed by the Prime Minister and published in the Official Gazette of the Republic of Kosovo

Albin Kurti

Prime Minister of the Republic of Kosovo

05 January 2024.