PUERTO RICO
STATE GUARD

DIRECTIVE

PRSG-G2 PRSGD 23-200
DISTRIBUTION: A 15 October 2023

OPERATIONS SECURITY (OPSEC)

References: See Enclosure A.

1. PURPOSE: Operations Security (OPSEC) is crucial to ensuring the protection of sensitive information and ensuring the success of military operations. This policy establishes guidelines and procedures for the protection of operational and tactical information throughout all phases of military operations and the primary objective of this policy is to protect information relevant to military operations, prevent unauthorized disclosure, and minimize vulnerability to internal and external threats.

2. AUTHORITY: Puerto Rico Military Code Century XXI, Law Number 88 of August 8 of 2023.

3. APPLICABILITY AND SCOPE: This directive applies to all active members of the Puerto Rico State Guard Command, including Commissioned Officers, Warrant Officers, Non-Commissioned Officers, Airman's, and Enlisted personnel.

4. DEFINITIONS: Sensitive data is defined as: All the information that is important to an individual (Guard's member) or organization (Puerto Rico State Guard Command), such as personal data, emails, official organizational documents, photos, images, videos, etc.

5. DIRECTIVE/POLICY:

a. Article 4.02 of the Puerto Rico Military Code Century XXI, Law 88 of August 8 of 2023 authorizes the Adjutant General of Puerto Rico to promulgate rules and regulations, not inconsistent with the provisions of this Chapter, with respect to age, enlistment, organization, administration, equipment, sustainment, training, and discipline requirements of said forces; Said rules and regulations must be in accordance with the laws of Puerto Rico applicable to the Military Forces of Puerto Rico.

b. PRSGI Instruction 350-1, This instruction/policy directly supports any instruction established in the Regulations of the Puerto Rico State Guard Command regarding the Mandatory Annual Trainings (MAT), which will include the Operations Security (OPSEC) as a Mandatory Training Courses:

c. Guidelines for Protecting Information.

1. Information Classification: All information must be appropriately classified according to its sensitivity level and handled in accordance with security regulations.

2. Controlled Disclosure: Relevant information should only be shared with authorized individuals on a need-to-know basis.

3. Communication Protection: Secure and encrypted communication systems should be used to prevent interception and manipulation of messages.

4. Online Activity Monitoring: Military personnel must refrain from sharing sensitive information, including but not limited to photographs, videos, or any information related to training, field training, official meetings, assembly, military orders, or any official or unofficial documents on online platforms and social networks. While the Puerto Rico State Guard Command is a government agency, its members are not public figures to be recorded and exposed on social media. For their safety, this policy recommends that all Guard's members keep their social profiles private whenever possible.

5. Electronic Devices Management: Electronic devices, including mobile phones and computers, must be protected with strong passwords and data encryption.

6. Secure Information Disposal: All printed and electronic information must be securely disposed of when no longer needed.

d. Awareness and Training: Regular awareness and training programs led by PRSG G2 and STRATCOM will be conducted to educate personnel about OPSEC best practices and the latest security threats. An online OPSEC course will be provided as part of Mandatory Annual Training (MAT), and all Guard's members must annually complete and certify it. This directive will complement Instruction 350-1 of July 2023, Military Annual Training.

e. Evaluation and Continuous Improvement: Periodic assessments of OPSEC measures' effectiveness will be conducted, and adjustments will be made as necessary to address emerging threats.

f. Compliance and Penalties: Failure to comply with OPSEC directive will result in disciplinary actions, which may include administrative and legal sanctions, and even expulsion from the Puerto Rico State Guard Command based on the severity of the violation.

5. RESPONSIBILITIES:

a. Commanders: Responsible for identifying critical information and appointing an OPSEC NCO from S2 Section (MACOM, Battalion and Squadron Level) to coordinate information protection activities.

b. PRSG G2: Must develop and implement training programs, assess vulnerabilities, and establish measures to mitigate operational security risks.

c. Military and civilian personnel: All Guard's members must be familiar with OPSEC practices and comply with established guidelines to protect sensitive information.

d. Operational security is the responsibility of every Guard's member in the military forces. By following these guidelines and practicing constant vigilance, we can protect our sensitive information and ensure the success of our military operations.

6. INFORMATION REQUIREMENT: NA

7. RELEASABILITY: Unlimited.

8. EFFECTIVE DATE; This directive will expire 2 years from the effective date of publication unless sooner rescinded or superseded.

9. POINT OF CONTACT: The point of contact of this directive/policy is the PRSG G2, Intelligence Officer of the Puerto Rico State Guard Command at (787)-731-3633 Ext.1464.

Enclosure1: Reference

EDRICK RAMIREZ GONZALEZ
Brigadier General, PRSG
Commanding General

References:

1. Military Code of Puerto Rico, Law Number 88 of August 8 of 2023.

2. Commander's Legal Handbook Pub 27-8.

3. PRSG Regulation 600-10, Personnel and Administrative Procedures, April 1 of 2023.

4. PRSG Instruction 350-1, Mandatory Annual Training, July 2023.

5. PRSG Instruction 24-300, Social Media policy, June 2022.