

RULES ON INFORMATION SECURITY

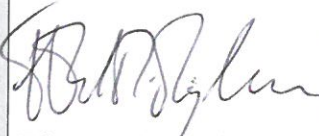
Approval Authority:	 Director-General	Date Approved:	17 January 2019
Effective Date	Date of Approval	Responsible Office:	Technology Services Unit (TSU)

Table of Contents

1. Background and Purpose3

2. Definitions.....3

3. Scope3

4. Security Standards.....4

5. Obligations for Users.....4

6. Governance4

7. Implementation5

8. Compliance**Error! Bookmark not defined.**

1. Background and Purpose

1.1 Collection, production, processing and dissemination of information is important to the mission of the GGGI and is an asset of significant value to GGGI. Information needs to be protected from threats that could potentially disrupt the mission of the organization and the proper administration of GGGI.

1.2 These Rules on Information Security (the Rules) are establishing a framework for GGGI's efforts to protect against threats against GGGI's information, as defined below, whether internal or external, deliberate or accidental, and minimize the impact of security incidents and complements the Rules on Protection of Personal Data. The Rules also seek to ensure the maintenance of:

- *Confidentiality*, information is accessible only to authorized users;
- *Integrity*, safeguarding of accuracy and completeness of information and processing methods; and
- *Availability*, ensuring authorized users have access to information/assets.

2. Definitions

The following definitions apply for the purpose of these Rules:

“Information” means all written information or data kept in electronic form by GGGI;

“Information System” means a tool for processing Information;

“Information Asset” means information assets, including online and offline IT systems, networks, databases, communication systems, conferencing systems, managed or hosted services, applications and any other information independently of its format;

“Security Threat” means a threat which may compromise the confidentiality, integrity and availability of Information; and

“Users” means all staff members, as well as to any consultants, contractors secondees or other individuals accessing and/or using GGGI Information Asset.

3. Scope

3.1 These Rules shall apply to all Users accessing and/or using any GGGI Information Asset for any purpose.

4. Security Standards

4.1 In order to protect GGGI's Information Asset's from Security Threats, GGGI shall:

- a) ensure security of the physical perimeter of information processing facilities, to prevent unauthorised access, damage and interference to information;
- b) comply with international standards and best practices relating to IT security and endeavour to comply with the principles established in ISO 27001 or similar standards;
- c) ensure that security is an integral component of the lifecycle of Information Systems and that appropriate security related considerations and measures are taken in all phases of the lifecycle, including but not limited to procurement, design, commissioning, implementation, maintenance and disposal of Information Systems.

4.2 GGGI shall ensure that an information security incident management process is implemented to respond to Security Threats. Security incidents shall be managed in a manner that allows timely and accurate identification and containment of as well as remediation of security incidents.

4.3 GGGI shall ensure that business continuity plans are developed, maintained and tested.

5. Obligations for Users

5.1 All Users accessing GGGI Information Assets shall:

- a) ensure the correct and secure operation of Information Systems used by GGGI; and
- b) take all appropriate measures in accordance with GGGI rules, guidelines and instructions, including GGGI's Code of Conduct, to protect the confidentiality, integrity and availability of those Information Assets and ensure that such assets are used only for the intended purposes.

5.2 GGGI shall promote awareness of individual roles and responsibilities as well as relevant guidelines and instructions in the context of information security among Users.

6. ICT Governance

6.1 The Information and Communication Technology (ICT) Executive Committee (ICT Executive Committee), comprising of the Director-General (DG), Head of Operations Enabling Division (Head of OED) and Head of Technology Services Unit (Head of TSU), or such other members as the DG determines, shall be the governing body which makes strategic decisions regarding ICT policies and infrastructure in GGGI and ensure monitoring of the effectiveness of GGGI's ICT infrastructure.

6.2 The ICT Executive Committee shall consider information security in all deliberations and ensure that all decisions are in compliance with these Rules.

7. Implementation

7.1 The content of these Rules and any related guidelines shall be communicated to Users through training, instructions and during the onboarding process for new Users.

7.2 The Head of TSU shall be responsible for the implementation of these Rules and provide leadership in the area of information security and coordinate the work on ICT security throughout the organization.

7.3 Supervisors shall, in consultation with the Head of TSU, ensure that all Users that are accessing, planning, developing or deploying new or existing Information Assets for GGGI are informed of and committed to comply with relevant GGGI information security policies.

7.4 All Users are responsible for the security of the Information Assets and Information Systems to which they have been granted access to and are accountable for security to the extent of their individual work responsibilities in GGGI.

7.5 The implementation of these Rules shall be supported by specific guidelines as appropriate, to address certain target areas within GGGI.