الهيئة العامة للصناعات العسكرية
General Authority for Military Industries

Data Security Policy for Military Industries Sector

Approved pursuant Board of Directors Resolution No. (G/T/49) dated 18/06/1444AH, corresponding to 11/01/2023AD, and amended pursuant to Executive Committee Resolution No. (TH/5/30), dated 23/04/1448 AH, corresponding to 04/10/2026AD

Disclaimer: The English version is a translation of the original Arabic text for information purposes only. In case of discrepancy, the Arabic original shall prevail.

الهيئة العامة للصناعات العسكرية
General Authority for Military Industries

Contents

Introduction 3

Chapter I: General Provisions 4

Chapter II: Data Protection 5

Chapter III: Data Dissemination Restrictions Based on Confidentiality Level 6

Chapter IV: Violation of Policy 7

Chapter V: Final Provisions 7

Introduction

The data produced, received, or processed by the Military Industries Sector ecosystem constitute valuable national assets and an economic resource that fosters innovation, supports economic transformation, enhances competitive capabilities. Given that the nature of such data — generated, processed, or circulated within the Military Industries ecosystem — is characterized by confidentiality and sensitivity, and in order to ensure a secure and trustworthy environment, the Authority has developed the "Data Security Policy for the Military Industries Sector" in accordance with best regulatory and operational practices, which govern the identification, protection, and sharing of data, as well as restrictions on its circulation.

The purpose of this Policy is to provide Facilities operating in the Military Industries Sector with guiding principles to ensure their compliance with the Kingdom's regulations and rules pertaining to data security. This Policy does not nullify or supersede the regulatory requirements of any other regulations or rules; rather, it seeks to facilitate and enhance compliance capabilities within the military industries sector, and shall be deemed complementary to the regulations and rules issued by other relevant authorities.

Chapter I: General Provisions

Article 1: Definitions

The following terms, wherever mentioned herein, shall have the meanings assigned thereto unless the context otherwise requires:

Term	Definition
Government/ KSA	The Kingdom of Saudi Arabia.
GAMI	The General Authority for Military Industries.
Policy	This Data Security Policy for Military Industries Sector.
Facility	An entity that operates in any of the military activities supervised or licensed by GAMI.
Licensee	A legal person licensed to engage in any of the activities subject to the regulation and supervision of GAMI.
Third Party	Any external entity contracted by an entity within the Military Industries Sector ecosystem to perform certain works and duly authorized to do so, including, without limitation, suppliers, contractors, and business partners, whether engaged on a permanent or temporary basis, regardless of their place of work.
Military and Security Agencies	The Ministry of Defense, Ministry of Interior, Ministry of National Guard, Presidency of Royal Guard, Presidency of State Security, and General intelligence Presidency.
Documents & Archives	The records containing information related to the work and interests of the state, whether these records contain information resulting from the state agencies' work or otherwise, as long as they need to maintained for reference or for their value.
DATA	The information or records that are created, collected, processed, stored, transmitted or exchanged, whether digital or physical, structured or unstructured, and that require protection against cybersecurity threats and risks.
Data Security	A set of systems, processes, techniques and technical solutions to protect data from unauthorized access, modification or deletion in cooperation with the competent authority, namely the National Cybersecurity Authority.
Physical Security	The security measures designed to prevent unauthorized access to the facilities, equipment, and resources of a facility, and to protect individuals and property against harm or damage such as (espionage, theft, or terrorist attacks). The physical security involves the use of multiple layers of integrated systems, including CCTV surveillance systems, security guards, security gates locks, access controls systems, and many other technologies.
Security Breach	Disclosure of, or unauthorized access to, information, or violating the cybersecurity policy of an entity through disclosure, unauthorized access, leakage, alteration, changing, sabotage or unauthorized use of sensitive data, whether intentionally or unintentionally. This includes encryption keys and other critical cybersecurity standards.
Encryption	Rules and means for storing and transferring data and information in certain formats in order to hide their content, prevent unauthorized access and minimal tampering to enable the authorized users only to access and process them.
Cybersecurity	Protecting networks, information technology systems, operational technology systems, their components including the hardware and software, the services they provide, and the data they contain, from any unauthorized access, disruption, alteration, use, or exploitation. Cybersecurity concept also includes information security, cybersecurity, digital security, etc...

Article 2: Statement of Purpose

This policy aims to protect all data received, produced, or processed by military industries facilities, regardless of its source, form or nature.

Article 3: Scope of Policy

This Policy applies to all military industries facilities that carry out any of activities supervised or licensed by GAMI. This document does not apply to the military and security agencies.

Chapter II: Data Protection

Article 4: Requirements of Competent Government Agencies

Military industries facilities shall comply with laws, regulations, and policies related to protection, management, and governance of data issued by the relevant government authorities.

Article 5: Responsibilities of Facilities Related to Data Protection

- Facilities shall prepare and implement data protection policies and procedures in accordance with this Policy and all laws and regulations related to data protection in the Kingdom.
- Facilities shall implement current and future legislative controls issued by NCA, which include the following:
  1) Essential Cybersecurity Controls.
  2) Critical Systems Cybersecurity Controls.
  3) Data Cybersecurity Controls.
  4) Social Media Accounts Cybersecurity Controls.
  5) Cloud Cybersecurity Controls.
  6) Telework Cybersecurity Controls.
  7) Operational Technology Cybersecurity Controls.
  8) Cybersecurity Controls for Private Sector Entities Other Than Critical Infrastructure Entities.

  When processing Personal Data, the Establishment shall comply with the Personal Data Protection Law and its Implementing Regulations, as well as the Personal Data Protection Policy for the Military Industries Sector. In the event of any conflict, the provisions of the Law and its Implementing Regulations shall prevail.

Article 6: Facilities' Responsibilities Regarding Data Protection in Relation to Physical Security

1. Facilities shall ensure that all their physical facilities in which classified data is generated, processed, or circulated have security and safety factors.
2. Facilities shall determine all their internal facilities in which classified data is generated, processed, or circulated, and a security classification is assigned thereto which commensurate with degrees of data classification.
3. Facilities, when necessary to upgrade the physical security plan for their facilities and distribute it into zones, shall mark each zone with a color that distinguishes it, as each zone shall have appropriate access restrictions according to its classification. Classification of zones shall be as follows:

1) **Public and Reception Zone (Green Zone):** Access is subject to limited restrictions, and

the zone is subject to general monitoring. Unclassified information is handled in this zone.

2) **General Office Zone (Yellow Zone):** Access is limited, entry is recorded, and visitors permitted to enter this zone are escorted. The zone is subject to general monitoring, and information classified as "Restricted" is handled in this zone.
3) **Secure Zone (Orange Zone):** Access is very limited, entry is recorded, and visitors whose work requires entry into this zone are escorted. The zone is subject to monitoring and direct supervision, and information classified as "Secret" or lower is handled in this zone.
4) **Restricted Access Zone (Red Zone):** Access is subject to strict restrictions and is limited to authorized persons only. Entry is recorded, and each person entering this zone must obtain a special entry permit. The zone is subject to monitoring and direct supervision, and information classified as "Top Secret" is handled in this zone.

4. Facilities shall control who is entitled to enter their facilities in accordance with security standards determined by the competent authorities, including, but not limited to; access control mechanisms and detection and tracking systems.
5. Facilities shall use appropriate security measures such as encryption and isolate development and testing environment from the secure operating environment.
6. Facilities shall store and process data 'Within the geographical borders of the Kingdom to ensure preservation of national sovereignty for this data, and it may not be processed outside the Kingdom except after obtaining GAMI's approval.
7. Facilities shall document the policy and procedures for data disposal. Destruction of data shall be in a safe manner that prevents its loss, usage, or unauthorized access, including operational and archived data and backups, in accordance 'With NCA instructions.
8. Facilities shall include provisions of the data retention and disposal policies in contracts in the event that these tasks are assigned to any third party.
9. Facilities shall verify identity of individuals before granting them access to data in accordance with controls of this Policy, and controls of relevant authorities in the Kingdom (NCA).
10. Facilities are not allowed to share information with any third party except after obtaining official approval of data owner, provided that this information does not contain confidential and sensitive data that may affect national security, in accordance with specified purposes and relevant regulations and policies in the Kingdom, provided that the third party is provided with privacy policy and procedures followed and shall be included in contracts and agreements.
11. Facilities shall prepare awareness programs for their employees to enhance culture of data protection and raise level of their awareness.

Chapter III: Data Dissemination Restrictions Based on Confidentiality Level

Article 7: Classified Data and Documents Restrictions

1. Specific phrases are used as restrictions for circulating or controlling access to data commensurate with its sensitivity and who can access and view such data.
2. Circulation restriction shall be specified in a wording equivalent to degree of "Top Secret" and "Secret" classification, such as: "Open by Hand, "Limited Circulation", "Non-circulatable", or "Copy (…) of (…)".
3. when necessary, only Saudis may be authorized to access or view data; in which case circulation restriction is used for "SAUDI EYES ONLY".
4. Circulation restriction rests with data creator or processor of (Data Owner).
5. Circulation restriction shall be suitable for the purpose for which it is used.
6. The following table is an illustration of data and documents restriction:

Restriction	Description
To be opened by Designee Only	It determines the person (by his position) who can access information, as none else shall have access unless the situation requires otherwise, provided that is under his responsibility and supervision.
Limited Dissemination	It allows data to be circulated within a narrow scope as necessary, such as circulation within a specific department, division, or workgroup only.
No Dissemination	It prevents data circulation with third parties, as data shall only be available to those authorized only.
Copy No. (…) of (…).	It determines total number of copies allowed to be distributed, provided that each copy shall have a serial number and shall be handed over a protected document receipt for those authorized to view only.
Saudi Eyes Only	when necessary, only Saudis may be authorized to access or view data.

Chapter IV: Violation of Policy

Article 8: Reporting Data Security Violations in Military Industries Sector

Facilities operating in the sector shall implement the following provisions in the event of detecting breaches related to data security, namely:

1. Inform GAMI and relevant authorities immediately of any data security breaches as soon as they are detected.
2. Prepare a report that includes all information related to security breach and assess its initial impact.
3. Keep a record of "security breaches", which is subject to GAMI inspection in accordance with regulations and procedures.
4. GAMI may audit licensees' incident records to ensure compliance with this Policy.

Article 9: Violations and Administrative Penalties

In case of violation of this Policy by any facility, GAMI may apply the appropriate administrative penalties according to type, nature and severity of violation:

Administrative warning to the violating facility, including details of the violation, the action to be taken by the facility, and the grace period granted by GAMI for making good such violation.

1. Suspension of the license for the period GAMI deems appropriate, renewable for other periods if the facility fails to rectify the violation.
2. Disqualification from future military tenders and procurements.
3. Cancellation of license.

Chapter V: Final Provisions

Article 10:

1. The Authority may interpret, review, and update this Policy as needed and submit any proposed updates to the competent approving authority.
2. Matters not specifically addressed in this policy shall be governed by the Authority's Statute, regulations, and approved decisions.
3. without prejudice to the regulatory requirements stipulated in other laws and regulations, this Policy shall be binding on Facilities and aims to facilitate and enhance compliance within the sector.
4. This Policy shall enter into force on the date of its publication.