الهيئة العامة للصناعات العسكرية
General Authority for Military Industries

Data Management & Security Policy for Military Industries

As approved by General Authority for Military Industries Board Decision No. (C/W/49) dated Jumada al-Thani 18, 1444 AH corresponding to January 11, 2023 AD

Contents

Introduction

Launched in 2016 to unleash the potential of economic sectors and promote economic development in the Kingdom of Saudi Arabia, the Saudi Vision 2020 included among one key objective, namely to localize no less than 50% of spending on military equipment by 2030. This objective is further bolstered by Council of Ministers' decision to establish the General Authority for Military Industries (GAMI), with a view to realizing the Kingdom's ambition towards strengthening its national military industries and localizing the military industries making it a main powerhouse of the national economy. In so doing, GAMI has become the regulator of military industries sector in the Kingdom, which is responsible for its regulation, development and monitoring of its performance.

GAMI's role is central in supporting the military industries sector, and instrumental in creating job opportunities for Saudi nationals, enhancing non-oil revenues, and raising its direct contribution to the gross domestic product, thus enhancing the Kingdom's independence and military and security readiness, by building a local military and security industries sector.

The data produced, received, or processed by the military industries ecosystem are valuable national assets and an economic resource that support innovation, stimulate economic transformations and enhance competitiveness, given the sensitive and confidential nature of that data that is generated, processed, or circulated within the military industries ecosystem. To ensure a safe and reliable environment, GAMI has developed this "Data Security and Management Policy for the Military Industries Sector" in accordance with best organizational and operational practices to lay out rules and restrictions related to data classification, protection, sharing and circulation.

The purpose of this policy is to provide the facilities working in military industries with guidelines to ensure their compliance with the Kingdom's laws and regulations related to data security and management, as this policy is without prejudice to regulatory requirements of any of the other laws and regulations, but it rather seeks to facilitate and enhance compliance within military industries sector, and is considered complementary to the laws and regulations 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 Management & Security Policy for Military Industries Sector
Military Industries Sector	The military industries suppliers, main contractors, subcontractors
Facility	An entity that operates in any of the military activities supervised or licensed by GAMI.
Licensee	A legal person who is licensed to practice any of the activities subject to the control and supervision of GAMI.
Third Party	An external party that contracts with a military industries entity to, and be authorized to, carry out specific work, including but not limited to suppliers, contractors, and business partners, whether permanent or temporary, regardless of their work locations.
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 stored digitally as data, including, but not limited to, personal, technical or general data. Printed documents and reports are also classified as data according to the purpose of this policy.
Data Management	The development, implementation and supervision of the plans, policies, programs and practices to enable the entities to govern data and enhance its value as a valuable asset.
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 control 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 and manage 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 Classification and Confidentiality Restrictions

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 of relevant government agencies, including the National Cybersecurity Authority (NCA), the Saudi Authority for Data and Artificial Intelligence (SDAIA), National Data Management Office (NDMO), and the National Center for Archives and Records.

Article 5: Principles of Data Classification and Confidentiality Restrictions

Principle 1: Confidentiality by Default

Military Industries Data shall be "strictly confidential" unless its nature or sensitivity requires a lower level of classification and protection.

Principle 2: Necessity and Proportionality

Data shall be classified, in terms of confidentiality, to levels according to its nature, sensitivity, and impact taking into account to balance between its value and classification of confidentiality.

Principle 3: Timely Classification

Data shall be classified upon creation or upon being received from another entity and classification exercise should be time-bound.

Principle 4: Highest Level of Protection

If information includes an integrated set of data with different classification levels, the highest classification level shall be applied to the aggregated data.

Principle 5: Segregation of Duties

Duties of participants in the classification process shall not overlap in terms of classifying data, approving a classification decision, granting authorization for access or usage of data, accessing data, protecting data, or disposal of data – in a way that does not lead to overlapping specialization.

Principle 6: Need to Know

Access and use of data shall be provided only on a need-to-know basis and for the least number of persons possible.

Article 6: Classification Levels for Data and Documents

1. Classification of Digital Data:

The table below shows the main data classification levels in terms of confidentiality, in accordance with the impact levels. It also shows some indicative examples for each level based on the national policies issued by NDMO.

Classification	Impact Levels	Description
Top Secret "TS"	High	Data shall be classified as "Top Secret", if unauthorized access to or disclosure of such data or its content adversely and exceptionally affects in a way that is difficult to resolve: – National interest including violations of conventions and treaties, adverse damage to reputation of the country, diplomatic relations and political affiliations, operational efficiency of security or military operations, national economy, national infrastructure and Government functions, and/or – KSA organizations functionality causing damage to the national interest, and/or – Individual health and safety at massive scale and privacy of Protected Individual personnel, and/or – Catastrophic damage to the environment or natural resources
Secret "S"	Medium	Data shall be classified as "Secret", if unauthorized access to or disclosure of such data or its content adversely affects: - National interest such as damage to reputation of the country, diplomatic relations, operational efficiency of security or military operations, national economy, national infrastructure, Government functions, and/or - Financial loss of KSA organizations that leads to bankruptcy or inability of organizations to perform their duties or major loss of competitive abilities or combination thereof, and/or - Causes significant harm or injury impacting life of individuals - Causes long-term damage to the environment or natural resources, and / or - investigation of major cases such as terrorism funding
Confidential "C"	Low	Data shall be classified as "Confidential" data, if unauthorized access to or disclosure of such data or its content causes: - Limited adverse impact on government entities' operations, economic operations in the Kingdom or business of any person, and/or - Limited damage to any entity's assets and limited loss to its financial and competitive status, and/or - Limited damage in the short-term to the environment or natural resources.

Public "P"	None	Data shall be classified as "Public", if unauthorized access to or disclosure of such data or its content has no impact on: - National Interest, or - Organizations, or - Individuals, or - Environment.

2. **Classification of Data and Documents:**
Facilities operating in the sector shall apply a classification of confidentiality degrees of documents and archives to all their transactions with military and security agencies, as follows:

Classification	Description
Top Secret Documents and Archives	Documents and archives whose knowledge of data by third parties may jeopardize the state-security, such as military plans and weapons quantities, types, and locations. These documents shall usually be viewed during their prohibition period only by senior officials concerned with such documents, or courts concerned with examining state security cases and to the extent necessary to adjudicate these cases.
Secret Documents and Archives	Documents and archives whose disclosure of data may harm public or private interests, such as documents related to administrative, industrial, or trade secrets. Such documents are usually viewed during their prohibition period only by specialists.
Confidential Documents and Archives	Documents and archives that are related to individual matters or issues, whose disclosure or access may have negative impacts on social life of groups or individuals, such as documents of investigation and judgments related to individual matters. These documents are usually viewed only by specialists.

Article 7: Data Classification Controls:

Based on levels of data classification in terms of its confidentiality, facilities operating in the military industries sector shall:

1. Determine and implement appropriate data protection controls to ensure safe handling, processing, sharing, and disposal of data.
2. In the event of non-classification of data upon its generation or receipt in accordance with approved classification standards, this data shall be treated as Top Secret until it is properly classified.

Facilities operating in the military industries sector may use controls described below when classifying data, including the following:

- **Watermark:**
It applies to hard and soft documents, including e-mails, according to each level of classification.
- **Data Access:**
It allows access to data based on principles of "Minimum Privilege" and "Need-to-Know".
- **Data Usage:**
It restricts Top-Secret Data, including for example, to specific locations, whether physical such as offices or virtual, using devices or special applications.

- **Data Storage:**
  It observes data classified as "Top Secret", "Secret", or "Confidential", as well as mobile devices that process or store such data.
- **Data Sharing:**
  Entities shall determine the appropriate physical and digital means for secure data sharing, in order to ensure reduction of potential risks and application of data sharing systems.
- **Data Retention:**
  A time schedule is prepared that determines retention period of all data. This retention period is determined as set out by relevant commercial, contractual, regulatory, and legal requirements.
- **Disposal of Data:**
  - All data is securely disposed and in accordance with data retention schedule.
  - Data classified as "Top Secret" or "Secret" and electronically controlled is disposed using the latest electronic media disposal methods.
  - All hard documents are disposed by Micro-cut paper shredders.
  - A detailed log is prepared for all disposed data.
- **Data Archiving:**
  - Data is archived in secure storage locations.
  - Archived data is backed up.
  - The archived data that has been classified as "Top Secret" and "Secret" is protected using the latest encryption methods approved by NCA.
  - A detailed list of users authorized to access archived data is prepared and documented.

Article 8: Obligations of Facilities Related to Data Classification and Confidentiality Restrictions

1. All facilities operating in the military industries sector shall specify all data they possess in accordance with provisions of this Policy.
2. Facilities operating in the military industries sector shall appoint a data classification official who is responsible for classification process and specification of all data.
3. Facilities operating in the military industries sector shall assign an individual to be responsible for carrying out obligations assigned thereto, as well as be responsible for carrying out the functional obligations related to data classification process and conditions for data protection.
4. Facilities operating in the military industries sector shall follow necessary measures to assess the potential impact of data disclosure or unauthorized access, modification and/or destruction of data.

Article 9: 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 restrictions:

Restriction	Description

Open 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 (-) 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 III: Data Protection

Article 10: 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:
  a) Essential Cybersecurity Controls.
  b) Critical Systems Cybersecurity Controls.
  c) Data Cybersecurity Controls
  d) Social Media Accounts Cybersecurity Controls
  e) Cloud Cybersecurity Controls.
  f) Telework Cybersecurity Controls.
  g) Operational Technology Cybersecurity Controls.
- Facilities shall ensure that all their physical facilities in which classified data is generated, processed, or circulated have security and safety factors.
- 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.
- 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:
  a. **Public and Reception Zone (Green Zone):** Limited restrictions and subject to public monitoring, in which unclassified information is handled.
  b. **General Office Zone (Yellow Zone):** Limited access, where visitors are logged in and escorted to this zone, and subject to public monitoring and direct supervision, in which information classified as "Prohibited" is handled.
  c. **Secure Zone (Orange Zone):** Very limited access, where visitors are logged in and escorted to this zone as required by work, and subject to public monitoring and direct supervision, in which information classified as "Secret" or less is handled.
  d. **Restricted Zone (Red Zone):** High restricted access, only for those authorized, where individuals with private clearance and have access to this zone are logged in, and subject to

public monitoring and direct supervision, in which information classified as "Top Secret" is handled.

- 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.
- Facilities shall use appropriate security measures such as encryption and isolate development and testing environment from the secure operating environment.
- 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.
- 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.
- 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.
- 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).
- 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.
- Facilities shall prepare awareness programs for their employees to enhance culture of data protection and raise level of their awareness.

Article 11: 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:

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

Chapter IV: Violation of Policy

Article 12: 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, including for example:

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

Chapter V: Final Provisions

Article 13:

1. GAMI may interpret, review and update this document when needed, and to submit the update proposal to GAMI's Board of Directors.
2. For matters not covered herein, the laws, regulations and the like issued by GAMI or the relevant legislative authorities in the Kingdom shall apply.
3. Without prejudice to the regulatory requirements contained in other laws and regulations, this Policy is binding and all parties and individuals working in the sector shall work to facilitate and enhance compliance herewith within the sector.
4. This Policy shall enter into force as from its date of approval and publication.