PROCESS OWNER IT Director	REV. LEVEL: REV. DATE:	04 7/5/2023	DOCUMENT NUMBER PR-MP06.01.01.01

1. OBJECTIVE/PURPOSE:

The Information Security Policy objectives are defined goals and targets that aim to protect the organization, including but not limited to the following:

- To ensure confidentiality, integrity, availability, authentication, authorization, and nonrepudiation of information technology systems to protect Dura-Shiloh and Customer intellectual property (IP), financials, and personal identifiable information (PII).
- To protect various systems and infrastructure from failure, unauthorized modification, and all other foreseeable disruptions.
- To ensure Employee personal data is kept confidential and secured from unauthorized access or use.
- To ensure Dura-Shiloh will meet or exceed all legal requirements to protect our systems and data.
- To ensure resources are in place to respond, contain, and eliminate ongoing and/or potential system compromises.
- To educate our employees on the importance of Information Security Management.

These objectives are targets that are achieved through continuous improvement initiatives and identifying and reducing the risks to information security. The Dura-Shiloh Information Security Management System (ISMS), driven with commitment from top leadership, provides security policies, procedures, and guidance on best practices to support these objectives.

2. SCOPE:

The scope of this procedure is relevant to the Global Information Technology.

This procedure applies to all locations designated as Dura-Shiloh and its subsidiaries, employees, contingent employees, and any other individuals or entities who use and/or manage access to Dura-Shiloh applications, systems, networks, and/or electronic data.

3. REFERENCE DOCUMENTATION:

- PR-MP06.01. 01.02 Management Responsibility and Authority
- F-MP06.01.01.02.01 Management Responsibility and Authority RACI Chart
- PR-MP06.01.01.03 Management Review
- F-MP06.01.01.03.01 ISMS Management Review Record

4. MEASURABLES:

Measurables for the effectiveness of the ISMS will be documented in the IT Business Plan Deployment and Management Review elements.

- MP06.01.01.03 ISMS Management Review Record
- MP06.03.02.01 Business Plan Deployment and Key Process Indicators
- PR-MP06.03.02.01 Business Plan Deployment and Key Process Indicators

The IT Director is accountable for adherence to this procedure and will communicate the Responsibilities and Authorities, which are essential to the ISMS.

5. DEFINITIONS AND ACRONYMS:

ISMS	Information Security Management System
BPD	Business Plan Deployment
KPI	Key Performance Indicators

6. PROCEDURE/REQUIREMENTS:

Information Security Policy

6.1. Management Commitment:

Top Management will demonstrate leadership and commitment with respect to the ISMS by:

- Ensuring the Information Security Policy and the information security objectives are established and are compatible with the strategic direction of the organization.
- Ensure the integration of the ISMS requirements into the organization's processes.
- Ensuring the resources needed for the ISMS are available.
- Communicating the importance of effective information security management and conforming to the ISMS requirements.
- Ensuring that the ISMS achieves its intended outcome(s).
- Directing and supporting employees to contribute to the effectiveness of the ISMS.
- Promoting continual improvement.
- Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

6.2. Roles and responsibilities:

Management Responsibility & Authority as designated in the following:

- PR-MP06.01.01.02.01 Management Responsibility & Authority
- F-MP06.01.01.02.01 Management and Authority RACI Chart

The security of information is an extremely important issue that impacts not only the personnel in the areas connected with Information Systems, but also all people that operate within the Company, at any level, and for any reason.
Each one of them is responsible for knowing, complying with, and enforcing the requirements described within this policy and all related technical and organizational measures as detailed within the Dura-Shiloh Information Systems Management System (ISMS).

IT Director
The IT Director reports to the CIO and promotes the creation and application of an adequate system for the protection of information and management of associated risks. This position manages and delegates certain responsibilities associated with the creation, control, and application of the Dura-Shiloh Information Systems Management System to the roles listed below.

- IT Directors & Senior Management
- IT Managers
- IT Staff
- Global Functional Leadership

Every Department/ Functional Manager is required, according to his own functions and responsibilities, to know, apply, and disseminate all the rules regarding information security.
Every Department/Functional Manager has the following responsibilities:

- Protecting and classifying the proprietary information of his Department/Function.
- Authorizing access to information for users on a need-to-know basis.

- Audit application of IT security rules by carrying out specific inspections in accordance with Dura-Shiloh's ISMS and instructions as issued by the officers in charge of managing IT security.
- Ensuring that all the people that use proprietary information of the Department/Function are aware of their security obligations and complete internal security training as required.
- Informing Customers, Suppliers, Consultants, or Auditors that perform activities on behalf of Dura-Shiloh of the level of protection required for processing of information.

- All Employees
- Legal/Regulatory
- Customers
- Suppliers/External Services
- External Auditors

Information Security Officer (ISO)

The Information Security Officer is a specialized role within the IT organization. This role reports to the IT Director and has the following responsibilities.

- Develops and maintains Dura-Shiloh's Information Security Management System (ISMS) and related security standards and policies.
- Prepares and coordinates plans and reporting for compliance with ISMS controls.
- Works in close collaboration with other IT management and team members and relies on their specialized support for implementing technical solutions to manage the risks associated with systems, networks, applications, and information management and security processes.
- Discusses risk assessments and the consistency of protection measures with the owners of the data as well as providing guidance on classifying information and processes with information owners.
- With the support of Human Resources, responsible for activities related to the dissemination of the Security policies and related employee training.
- Responsible for the continuous monitoring of the adequacy and effectiveness of the ISMS through assessment, including participation as required in internal and external audits.
- Maintain certification for Information Security principles (ISO 27001).

Facility Security Roles

Each facility within the enterprise requires a designate for security.

- Plant or Site Manager
- Internal Auditor Security (qualified, non-IT)

6.3. Policy Publication

- The Dura-Shiloh Information Security Policy (this document) and related ISMS policies and procedures are available for all users via internal Dura-Shiloh company portal.
- The Dura-Shiloh Information Security Policy (this document) is available to business partners via the Dura-Shiloh website (version updated annually at a minimum).

6.4. Policy Review

- During the quarterly management review, ISMS documents changed or reviewed within the period will be discussed and approved. Changes may occur whenever there is a material change in Dura's business practices, including any changes to technology, policies, roles, and responsibilities. Each document includes a revision history with a summary of the changes made and the date the change was made.

- The global helpdesk is programmed to initiate an automatic task prior to the Q4 management review to ensure that ISMS documents not assessed in the last 12 months are reviewed.
- The IT Director and the Information Security Officer must approve any changes to this policy and are responsible for communicating changes to affected parties.

6.5. **Compliance**

- All employees must read and acknowledge this policy during induction, or annual refresher via our training platform.
- Non-compliance with this policy may result in serious consequences for the organization and its employees. These consequences may include legal penalties, fines, lawsuits, regulatory scrutiny, loss of reputation, customer dissatisfaction, business interruption, and disciplinary action. Therefore, it is the responsibility of all employees to comply with the policy and report any breaches or incidents.
- Non-compliance will be investigated, and corrective actions will be taken as necessary.

7. REVISION HISTORY:

Revision Level	Summary of Revision	Revised By	Date of Revision	Section(s) revised or added
00	Initial Creation	Laura Flanagan	03/21/2018	
01	Revision/Annual Review	Peter Hollex	01/16/2019	
02	Modified to include more detail about content of mgmt. review	Neil Jones	02/17/2022	
03	Title Change – Director, IT – Security & Compliance, spelling correction, and addition of Facility Security Roles	Teresa McCann	9/28/2022	
04	Dura-Shiloh Template Change and revision numbering correction and title corrections. Revised objective wording, added policy publication & compliance sections based on TISAX auditor suggestions.	Neil Jones Teresa McCann	7/5/2023	01 – Objective 02 – Scope 03 - Reference 6.3 - Policy Publication 6.4 - Policy Review 6.5 - Compliance

8. STANDARD CLAUSES:

ISO9001	IATF16949	ISO14001	ISO50001	ISO27001	ISO45001	CSR's
				4.4, 5.1, 5.2, 5.3, TISAX 1.1.1, 1.2.1, 1.2.2		