Information Security Governance Policy

Document Name: Corporate Information Security Governance Policy

Document ID: IT-INFOSEC-CP001

1. PURPOSE

1.1. This policy codifies our commitment to protecting Information across the enterprise.

1.2. Information is a critical and essential asset to Dana. Sound business decisions cannot be made without reliable and timely Information. Maintaining the confidentiality, integrity and availability of this Information is essential to making good business decisions and protecting Dana intellectual property investments.

1.3. Dana, as a company, has the responsibility to ensure its Information, Information Systems and intellectual property entrusted to us by our customers, business partners and employees are properly protected and used for appropriate business purposes.

2. SCOPE

2.1. This document applies to all Dana IT operations globally.

3. RESPONSIBILITY

3.1. The Information Security, Risk Management, and Compliance (ISRMC) department is responsible for policy maintenance activities including reviews and revisions. The ISRMC department is responsible for monitoring compliance with this policy and may enlist other departments to assist in the enforcement of this policy.

3.2. Dana will appoint an Information Security Lead to develop and monitor ISRMC policies, standards, controls, practices, and programs to ensure that Dana's Information and Information Systems are secure from unauthorized access, protected from inappropriate alterations, physically secure and available to authorized users in a timely fashion while enabling Dana to meet its business objective in the most effective and timely manner possible.

4. DEFINITIONS

4.1. **Information –** A definable piece of communication or representation of knowledge that has value to the organization. Examples of Information include, but are not limited to the following: databases, data files, reports, documents, contracts, agreements, system documentation, research information, user manuals, training material, procedures, business continuity plans, audit trails, archived information, strategic plans, or business implementation roadmaps.

4.2. **Information Owner** - The party or parties accountable for ensuring the appropriate use of Information. The Information Owner must be a Dana employee.

4.3. **Information Security Incident** - Any incident which compromises the confidentiality, integrity or availability of Information and creates a potential threat for loss or disruption to business operations, reputation or assets and is also a violation of security policies or general security practices.

4.4. **Information System -** A discrete set of technology resources organized for the creation, storage, processing, transmission, use or disposal of Information.

5. POLICY STATEMENTS

5.1. Dana will define and document a comprehensive set of Information Security policies that outline management's position on information security. These policies will set forth the program and authorize corresponding Standards and Procedures required for implementation of these policies.

5.2. Information security policies will cover the following topics or areas:

5.2.1. Establishment of an information security organization and its services.

5.2.2. Management of employee roles, responsibilities, and corporate training.

5.2.3. Management of asset use, including classification and handling of information.

5.2.4. Management of access to networks, applications, and other Information Systems.

5.2.5. Management of the use of cryptographic control.

5.2.6. Management of physical and environmental controls used to protect Dana data and equipment from damage or unauthorized use.

5.2.7. Management of operations security related to IT operations, malware protection, backup and restoration activities, event management and logging of Information Systems, application configuration management, vulnerability management, security monitoring and response, the use of cloud computing and endpoint configuration.

5.2.8. Management of communications security related to the security of Dana networks, Information transfer internal and external to Dana and access to Dana Information from outside Dana owned networks.

5.2.9. Management of the confidentiality, availability and integrity during acquisition, development and maintenance of Information Systems related to requirements of Information Systems, development, and support process and how test data is leveraged.

5.2.10. Management of Information Security Supplier Risk Management program.

5.2.11. Management of Information Security Incidents.

5.2.12. Management of information security aspects of business continuity during and recovery from Information disasters.

5.2.13. Management of information technology risk and compliance.

March 28, 2023