Doosan Enerbility

Information Security Policy

1. Information Security Strategy & Policy

Doosan Enerbility places top priority on building customer trust and accordingly recognizes data protection as a fundamental corporate responsibility. To this end, the company has established and implemented corporate-wide information security guidelines based on the ISO 27001, the international standard for information security.

The information security policy is aimed at systematically identifying the various risks, such as Cloud data breaches, insider's act of negligence and security weaknesses in the supply chain, and devising specific countermeasures to address these risks. Moreover, all employees are obligated to familiarize themselves with the information security policy and comply with the set guidelines. The same level of information security is also required when entering into contracts with external partners, and strict control measures are taken against potential threats posed by third parties.

The information security policy is regularly reviewed by the senior management and updated as needed. It serves as the standard for all security activities of the company.

2. Information Security Organization & Framework

Doosan Enerbility has a dedicated organization for systematically handling information security, one that is centered around the Chief Information Security Officer (CISO). The CISO oversees the establishment and implementation of the company's information security policy, while concurrently holding the position as

Chief Privacy Officer (CPO), whose main responsibility is overseeing the company's legal and ethical obligations.

The information security department handles security details at the working-level, including the policy operation, system inspections, accident response and employee training. The corporate-wide security system is managed through close collaboration with all the other departments.

All employees have data protection accountabilities related to their respective work, and are obligated to comply with detailed security guidelines, such as those relating to account management, the detection and reporting of anomalies, and handling of sensitive information. External partner companies are also required to undergo preliminary security checks and are applied security provisions that are included as mandatory contractual obligations, all of which are used to effectively control external risks.

3. Information Security Infrastructure

Doosan Enerbility has implemented an assortment of security mechanisms for the purpose of cultivating a secure digital environment and is continuously improving upon the relevant technologies and policies. Through regularly conducted risk assessments, various security mechanisms are being applied, such as firewalls, intrusion prevention systems, access control, encryptions and two-factor authentications. Critical data, in particular, is saved after data encryption, and unauthorized data modifications or data leaks is prevented by keeping a record of the data change history and by operating a data restoration system. Sensitive data is categorized and managed by security grade, with protective measures being taken across the entire lifecycle from the point of data storage to disposal. The results of internal audits and external inspections are actively reflected in the system improvements thereafter, and the supporting infrastructure is managed in a flexible manner to enable swift responses to newly detected threats. Such efforts serve as the basis for ensuring data integrity and security.

4. Information Security Verifications & Evaluations and Related Activities

Doosan Enerbility has its security system objectively reviewed based on the international standard, the ISO 27001. Equipped with a Global Security Operations Center (GSOC) that is operated 24/7, real-time monitoring of potential information security threats is performed, with immediate action being taken whenever any abnormal behavior or infiltration attempt is detected. In the event of an infiltration incident, swift action will be taken according to the guidelines outlined in the manual prepared on response measures. A structured management process is in place, which includes cause analysis of incidents and measures aimed at preventing recurrences.

The employees are required to take a training program on information security at least once every year and to participate in various campaign programs aimed at promoting information security awareness, such as phishing simulation drills. Preventive measures are also being taken against potential threats from third parties by conducting regular security checks on external partner companies and checking on the faithful implementation of security agreements. These activities constitute an integral part of the company's ongoing efforts to strengthen its information security system and safeguard the overall business environment.