

Information Security Policy

The DIC Group recognizes that the protection of information property that the DIC Group owns or manages is important in conducting business. Information security is one of the important items in the management of the business, and we therefore have established the following information security policy.

The “information property” referred to this security policy shall mean all the information that the DIC Group owns, manages, or which is used or developed by our business operations, including software, hardware, and other equipment, as well as the information systems of the DIC Group comprising of software, hardware, and other equipment and the data contained in these systems.

1. Control system for information security

To maintain the confidentiality, integrity, and availability of information (*) for the purpose of proper control and use of information property that the DIC Group owns or manages, the DIC Group will implement in-house control system for information security.

2. Compliance to laws and in-house rules

The DIC Group will establish in-house rules on information security in accordance with the laws and social norms, and assure that all directors and employees including part-time employees, temporary staff, and contract staff, will be compliant with the in-house rules and applicable laws.

3. Implementation of education

The DIC Group will continually provide education on information security for all directors and employees to aim for thorough compliance to the laws, social norms, and in-house rules.

4. Control of information property

The DIC Group will implement relevant information security measures to prevent an illegal access, leakage, falsification, loss, destruction, usage obstruction, etc. to the information property.

5. Measures in case of an incident

In the event of a breach of security involving our information property, such as a serious leakage, hacking or other unauthorized disclosure of information, the DIC Group will immediately apply corrective action and take measures to prevent breaches from re-occurring.

6. Review and improvement

The DIC Group will regularly execute all necessary reviews and improvements of our control system for information security.

7. Action against violations

In the event of a breach of information security policy and/or in-house rules on information security, the DIC Group will take strict measures based on the company's employee regulation, contract and relevant laws.

(*)

Confidentiality: Ensure that only the person authorized to access can access the information.

Integrity: Protect information and the processing method to be accurate and complete.

Availability: Ensure the access to information and to the relating property when the authorized user requires.

DIC Corporation