

Basic Policy on Information Security



The Achilles Group (“the Group”) is committed to Group-wide information security, based on the following policy. We aim to protect information assets from threats including security incidents, damage due to fire or other physical threat, cybercrime, etc., whether the assets belong to the Group or are entrusted to us by our customers. By so doing we are living up to the trust placed in us by our customers and society.

1. Provide products and services that are safe and secure

The Group strives to provide products and services that customers can use safely and securely from the point of view of the security of customer information.

2. Managerial responsibility

The Group strives to continuously improve organizational information security led by management.

3. Compliance with laws and contractual obligations

The Group complies with all laws, regulations, norms, and contractual obligations related to information security, meeting the expectations of our customers and society.

4. Establishment of an internal system

The Group has in place a management system that includes provisions for information security measures, and regularly assesses how the system is running and makes improvements as required.

5. Education and training

The Group carries out the necessary education and training for directors and employees to heighten awareness of the importance of Information assets and the prevention of data leaks.

6. Response to policy violations and incidents

The Group shall take appropriate action in response to the occurrence of an information security-related legal violation, contractual breach, or other incident, and work to prevent any recurrence.

7. Ongoing measures

The Group implements information security measures continuously to protect against various threats to information assets.