

Confidentiality Control and Information Security

We consider the prevention of confidential information leakage and defense against external attacks on information as indispensable for business activities.

We promote confidentiality control and information security activities on the basis of the recognition that not only our company's information, but also our clients' information is property which needs to be appropriately controlled and handled.




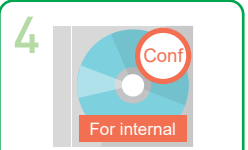

Basic way of thinking

We are striving to increase awareness regarding confidentiality control by stipulating "We will strictly control confidential information in compliance with the rules and endeavor to prevent disclosure" in the "Employee Code of Conduct," appointing confidential information management supervisors and confidential information handlers in each department and conducting meetings and self-checks in workplaces.

Also, in order to protect the company, and thus our

employees, we are working on the development of a work environment that is safe and easy to work in through physical and technological defenses such as restrictions on access rights and lock controls, psychological controls such as computer operation log records and confidential category identification, and the dissemination of leakage cases, etc., as the "five measures against information leakage," the content of which complies with guidelines in Japan and overseas.

Five measures

Physical and technological defenses		Psychological controls		Development of a work environment that is safe and easy to work in
Access control  1 Measures that make it difficult for people to get close to confidential information • Restrictions of access rights • Lock control • Paperless	Making it difficult to take out  2 Measures that make it difficult for people to take out confidential information • Prohibition of using / bringing in private USB memory sticks • Encryption of electronic data • Restrictions on uploading to places outside the company	Securing visibility  3 Creating an environment in which leakage is easily detected • "No admittance except for authorized persons" signboards • Keeping the workplace neat and in order • Computer operation log records	Improved awareness regarding confidential information  4 Indicate that the information is confidential • "Confidential" indication • Conclusion of non-disclosure agreement • Conducting training	Sustainment and improvement of trusting relationships  5 Raise awareness of employees • Promotion of communication • Notification of leakage cases

* Created on the basis of the "Protection and Use of Trade Secrets" published by the Ministry of Economy, Trade and Industry in June 2016

Examples of physical and technological defenses

Aiming to reduce the risk of information leakage, we introduced multifunctional machines for IC card authentication in November 2017.

Also, we conduct unannounced belongings checks every half a year in order to enhance employees' awareness of confidentiality control.



Introduction of multifunctional machines for IC card authentication



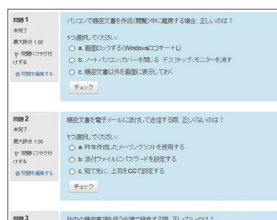
Belongings check

Examples of psychological controls

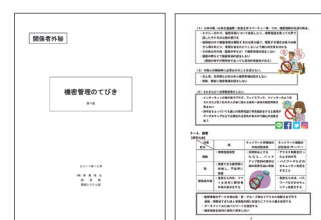
We held an e-learning course aimed at general employees in October 2018 and approximately 4,000 people took the course.

We dealt with anticipated scenarios that we could expect to see in various, every day work situations. We deepened our knowledge of such risks through that course.

Also, we revised the Guide to Confidentiality Control in December 2017. The guide explains everything from the definition of confidentiality to how to respond in the event of an incident, in an easy-to-understand manner with illustrations.



E-learning screen



Guide to Confidentiality Control (extract)

Implementation

Approximately **4,000** people