

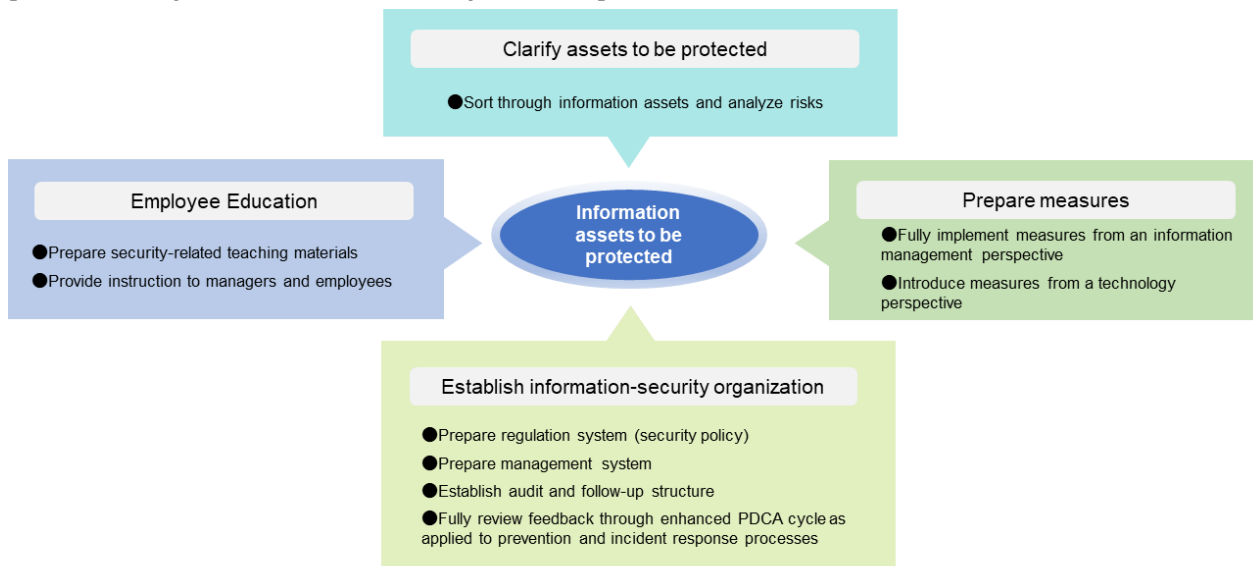
## Information Protection and Management

### (1) Basic Approach

The environment surrounding corporate information security has recently undergone a significant transformation. This situation is posing a number of pressing issues for businesses to address, such as large-scale cyberattacks, economic security, and many governments tightening personal information protection laws, including the EU’s General Data Protection Regulation (GDPR).

At the Proterial Group, we recognize that it is our important corporate social responsibility to appropriately manage, protect and utilize confidential information provided by our customers and business partners, our proprietary technology information, and personal and other information we hold (hereinafter “information assets”). Based on this recognition, the Group formulated the Basic Policy of Information Security (presently Information Security Policy) in April 2004. We have subsequently developed related rules and internal structures, thus promoting information security activities on an ongoing manner. After the departure from the Hitachi Group in January 2023, we are promoting the Proterial Group’s information security management independently.

#### [Basic concept of information asset protection]



### (2) Classifying Information Assets to Be Protected

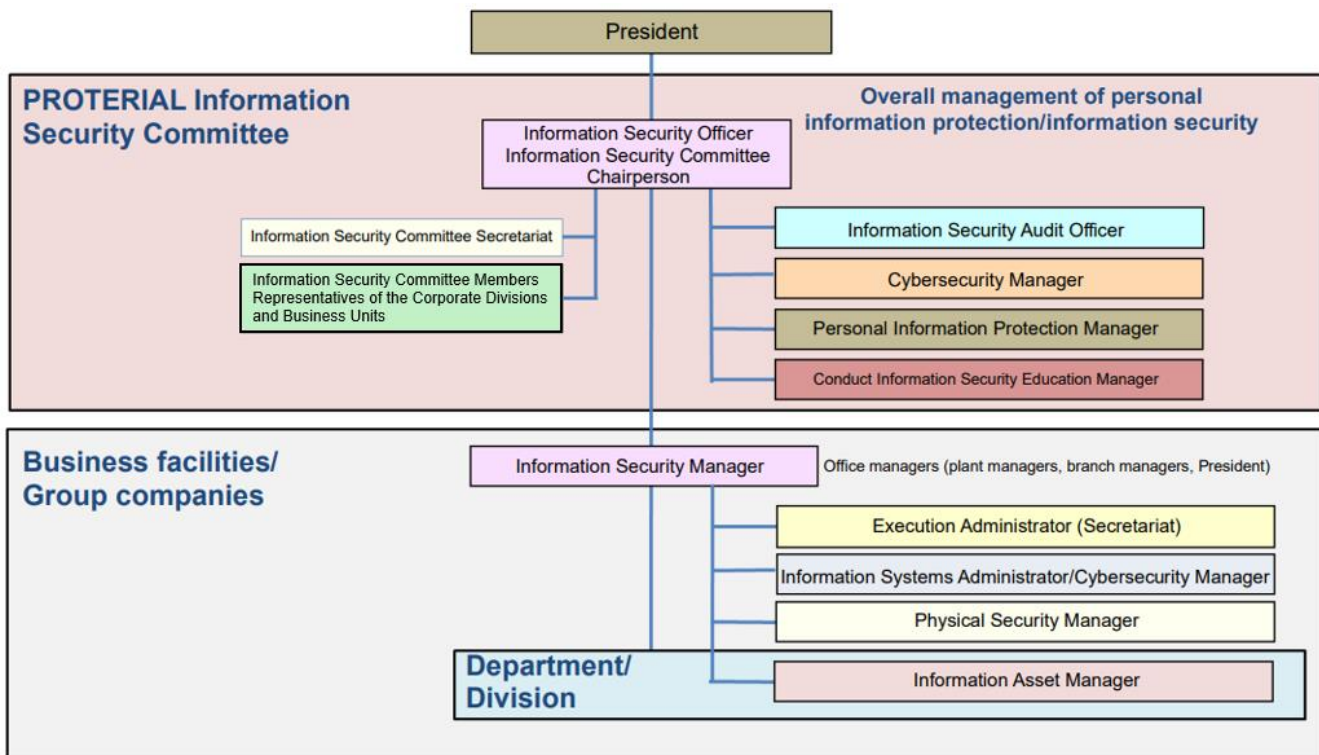
In order to classify information assets to be protected, the Proterial Group conducts information security self-audits every year, chiefly to identify information assets and analyze related risks. In fiscal 2022 and 2023, we omitted the self-audit due to reviews made on the information asset management methods and related rules in response to the departure from the Hitachi Group. We are planning to resume the practice from fiscal 2024.

### (3) Establishing Information Security Management System

The Proterial Group recognizes promoting information security activities as an important management issue, and has thus established the Group’s information security management system based on our General Rules for Information Security Management, which set forth the formation of the Information Security Committee chaired by the Information Security Officer reporting directly to the President. In order to confirm effective application of the system to information security activities, the Information Security Audit Officer is appointed to be responsible for a range of tasks to establish audit follow-up procedures and enhance PDCA activities for prevention and recurrence prevention processes for thoroughgoing feedback. This way, we have engaged in information security activities in a sustainable fashion.

In response to the needs of the times, the Information Security Committee has been reinforced, principally by appointing a Cybersecurity Manager in 2017 to address the growing threats of cyberattacks, and a Privacy Protection Manager in 2020 to cope with privacy-related risk and compliance issues.

## [Proterial Group Information Security Management Structure (conceptual scheme)]



### (4) Preparation of Measures

Proterial has systematically implemented measures against external risks such as targeted attacks and other unauthorized access and computer viruses, internal risks such as the unauthorized removal, loss, or theft of confidential information from the Company or the sending of e-mails to unintended recipients, and other risks including natural disasters.

In a bid to reduce the above-stated risks that may cause information leakage, we carry out both managerial measures and technical measures.

Managerial measures implemented on an ongoing basis include: inspecting the personally owned PCs and devices of all employees who have a Group e-mail address to find and delete business information; requiring the employees to submit, through the website, a written pledge not to retain business information in their personally owned PCs and devices; and ensuring that employees understand and observe the rules of managing smartphones and other mobile devices for preventing the loss of such devices.

Major technical measures include: introducing a filtering system to monitor all e-mails sent externally for preventing external leaks of information assets; and installing erroneous transmission prevention software on all business PCs of the Proterial Group as a countermeasure against the sending of e-mails to unintended recipients. Following the departure from the Hitachi Group, we have implemented measures against cyber attacks, principally by installing EDR and WAF software, building the SASE platform, and implementing a 24/7 cybersecurity surveillance system to protect from external threats.

Also, as the new organization resulting from the departure in January 2023, we employed external consulting services between April and August in 2023 to receive evaluations on information security systems and support with addressing issues identified, in a bid to promote information security measures suitable to the era of digitalization.

### (5) Employee Education

Each year, the Company provides information security education for all employees (including temporary staff, etc.) who use IT equipment in the Proterial Group. This education is designed to instill an understanding of rules related to the use of IT equipment for business and the handling of information assets. In order to improve capabilities to protect from targeted e-mail attacks, which have been becoming ever more sophisticated and posing a growing threat of ransomware infection, relevant training is run on an ongoing basis to raise the security awareness of individual employees. In February 2024, a company-wide drill was carried out.

## **(6) Protection and Respect for Intellectual Property**

Proterial practices the principle set forth in its Codes of Conduct that reads: “We will protect our own intellectual property, respect third-party intellectual property, and use both effectively for smooth business operations.”

Specifically, to appropriately protect and effectively apply intellectual property created in such processes as research, development, and manufacturing, Proterial acquires the rights to inventions, ideas and designs created by employees in the course of their work, in accordance with the Company’s rules, which have been established through legally stipulated procedures. With the global expansion of our business, we acquire and maintain the rights to these creations as intellectual property rights inside and outside Japan, forming assets that will support the sustainable growth of the Proterial Group. We take appropriate action against infringements of our intellectual property rights, including exercise of our rights through legal action.

At the same time, we strive to prevent infringements of the intellectual property rights of others and smoothly advance our business. To that end, we investigate the intellectual property rights of others globally, in advance of all stages of research, development, design, etc., for new products and technologies, in accordance with Proterial’s rules. If that investigation reveals a need to use the intellectual property rights of others, we acquire the necessary licenses.

We also provide our employees with ongoing education and training about intellectual property, to instill awareness of the protection and respect of our intellectual property rights and those of others.