Information Security

Policy

The NLM Group continuously provides employees with information security education and awareness-raising, and is actively promoting the use of cutting-edge technologies such as generative AI in its business operations. As part of this, in June 2025, we established "Guidelines for the Business Use of Generative AI Tools," developing a system to respond to risks associated with the use of AI. These guidelines clarify the risks, such as copyright and ethical concerns in using generative AI in business operations, and specify the appropriate scope and procedures for use. With these guidelines, we aim to maximize the benefits of technological innovation, ensure our credibility as an organization, and sustainably increase our corporate value.

Framework

The Information System Segment takes a leading part in promoting comprehensive management of information security risks within the NLM Group. We are continuously implementing the following initiatives with the aim of strengthening IT governance and responding appropriately to security incidents.

1. Audit activities for establishing IT governance

We conduct an information systems audit once a year for each group company and department. The audit focuses on the following items to confirm operational status, identify areas for improvement, and follow up on corrective actions.

- Appropriateness of access rights management
- Backup and troubleshooting systems
- System vulnerability countermeasure status

We provide feedback on the results of these audits to reflect them in IT policies across the group, leading to improvement activities that will help reduce risks.

2. Establishment and operation of a security incident response system

In October 2020, we established a security incident response team, "NLM-CSIRT," and are working to strengthen our incident response capabilities through the following activities:

- Establishment of incident prevention and response procedures (protection/monitoring/ detection)
- Security education for all employees (e-learning via LMS)
- Implementation of targeted email training and incident response training on a regular basis

Through these activities, we aim to raise our employees' security awareness and establish a system for rapid response in the event of an incident.

FY2024 Initiatives

As in the previous fiscal year, measures to strengthen security were taken in parallel with measures to strengthen system management and control regarding the business systems of the Group as a whole.

Identification of the current status of systems and implementation of measures to prevent information leaks and other security measures

Measures	Plan/result	Evaluation
Diagnosing IT issues at all sites	Plan: 38 sites Result: 38 sites	○
Performing penetration tests at all sites	Plan: 162 servers Result: 58 servers in the first half + 104 servers in the second half	○
Training to address targeted email attacks	Plan: 2 times a year Result: Implemented in August and March	○
Holding liaison meetings with staff from Japan and other countries	Plan: 2 times a year in Japan, 2 times a year overseas Result: Held in Japan in May and November Held overseas in September (Southeast Asia) and October (China)	○
Strengthening CSIRT	Plan: Implementation of incident training, 2 times a year Result: Implemented in December	△*1
Introduction of external security monitoring services	Service selection completed and operation to begin in FY2025	○
Implementation of security e-learning program	Plan: Implementation for all employees Result: Implementation completed	○

Ongoing implementation of data backup and restoration and disaster recovery measures

Measures	Plan/result	Evaluation
Implementing disaster recovery tests of critical systems	Plan: 10 servers Result: 10 servers	○
Review of information tools to be used in the event of a disaster	Information tools are being studied.	△*2

Continuing review of management regulations and compliance with IT general controls (ITGC)

Measures	Plan/result	Evaluation
Revision of the Group Information System Management Regulations	Revision of the password policy (October) Formulation of guidelines for the business use of generative AI	○
Making all systems ITGC compliant	Full system operation from FY2024 evaluation	○

○: Planned figure/number of events achieved. △: Planned figure/progress not achieved.
*1 Training for all relevant departments was completed by December 2024, and a review of training details for FY2025 was started
*2 System selection planned to be completed within FY2025