Information Security Policy

Basic Principle

N Lab Inc. provides systems to hospitals and testing facilities for the digital slide-based processing of pathology diagnoses. In addition, we are actively engaged in the research and development of pathology AI, which will undoubtedly play an increasingly vital role in the future of medicine. These activities involve handling sensitive data, including medical and personal information.

Although our digital slide systems are designed so that personal information is not accessible from external sources, much of the medical industry still relies on paper-based records. Information assets handled in our business—including valuable data entrusted to us by our clients—are essential to our operations and management.

We recognize the importance of protecting these information assets from risks such as data leakage, damage, or loss. All executives and employees are committed to complying with this policy and maintaining the confidentiality, integrity, and availability of information assets through proactive information security practices.

Basic Policy

1. Compliance and Security Framework

We establish and operate our information security activities in accordance with this policy and comply with all relevant laws, regulations, standards, and contractual obligations related to information security.

2. Risk Assessment and Management

We define clear criteria for analyzing and evaluating risks such as data leakage, damage, or loss. A structured risk assessment process is implemented and regularly reviewed to ensure that appropriate and effective security measures are taken.

3. Organizational Structure and Education

We maintain a clear information security structure, led by the responsible executive, and assign defined roles and responsibilities. All personnel are regularly educated and trained to understand the importance of information security and to handle information assets appropriately.

4. Audits and Continuous Improvement

We conduct regular audits and reviews of information handling and compliance with this policy. Any identified issues are promptly addressed through corrective actions.

5. Incident Response and Business Continuity

We establish procedures to respond to and manage security incidents appropriately. In the

event of an incident, we act swiftly to minimize damage and apply corrective measures. Special attention is given to incidents that may disrupt operations, with frameworks for business continuity that include periodic testing and review.

6. Information Security Management System (ISMS)

We have established an ISMS to achieve the objectives defined in our basic principle. This system is operated, reviewed, and continuously improved to enhance our information security posture.

Established: January 21, 2024

N Lab Co., Ltd

Yuka Kitamura, CEO