Article 1. General Provisions

1. Purpose

Lunit, as a medical AI company developing deep learning-based medical artificial intelligence technology to assist in the diagnosis and treatment using medical images, safely and effectively protects the personal information and information assets of stakeholders, including users, shareholders, and business partners, centered around the information security organization, in compliance with relevant domestic and international laws and compliance requirements. To this end, all Lunit employees must strive to achieve the following objectives through the establishment and operation of an information security management system.

1. Protect the company's critical information assets, including customer personal data and information system infrastructure.
2. Limit the use of information and information assets strictly to authorized business purposes.
3. Prohibit the use or disclosure of information and information assets for non-business or unauthorized purposes.
4. Prevent unauthorized access to, alteration of, or interference with information and information assets.
5. Comply with all applicable laws, regulations, and internal policies relating to personal data protection and information security.

2. Scope of Application

This policy applies to all employees of Lunit, its subsidiaries, all tangible and intangible information assets owned by Lunit, and to partners, vendors, contractors, and their personnel who participate in Lunit's business activities or utilize Lunit's tangible or intangible information assets.

Article 2. Information Security and Personal Information Protection Guidelines

3. **Information Security Organization:** In accordance with relevant laws, including the Personal Information Protection Act, Lunit has appointed a Chief Information Security Officer (CISO) and a Chief Privacy Officer (CPO) to oversee information security operations. This includes the establishment and management of an information security committee, risk analysis, as well as the response to and recovery from security incidents.
4. **Information Security Management System:** Information security regulations, guidelines, and procedures are reviewed and maintained at least annually through consultation and approval with relevant departments.
5. **Protection of Information Assets and Compliance:** We enhance the overall level of security and maintain up-to-date regulations through annual information security level

assessments, security consulting, and security training for employees at domestic and overseas entities. We also acquire security certifications and utilize the GRC (Governance, Risk, and Compliance) management platform.

- **Infrastructure Security**: Vulnerability assessments are performed annually on legacy and cloud infrastructure.
- **Data Security**: Data encryption, de-identification, and access control.
- **Development and Application Service Security**: Vulnerability assessments and service safety verification through in-house and professional penetration testing companies.
- **Information Security Certification**: Information security certifications are consistently maintained through annual internal audits and regular renewals from third-party independent audit institutions.

Certifications:

- ISO27001:2022
- CyberEssential Plus

6. **Personal Information Protection:** We define detailed standards concerning the processing of personal information, types of personal information breaches, and preventive measures. In accordance with these standards for ensuring the security of personal information, we manage personal information safely by implementing administrative safeguards (establishment of personal information management plans, designation of personal information processing systems and responsible personnel, response to personal information breach incidents, and conduct personal information training), technical safeguards (access control, encryption, and the installation and operation of security programs), and physical safeguards (defining security zones, controlling physical access, and securing printed materials).

7. **Security Incident Response:** To identify and manage security incidents, we define incident types and operate a security incident response organization and system to enable immediate response to all types of security incidents.

8. **Strengthening Employee Security Awareness:** We conduct regular information security campaigns, training, and phishing email drills to enhance employee security awareness and promote security as a part of daily work.

Article 3. Privacy Policy

Lunit places the highest importance on the protection of personal information and complies with the Personal Information Protection Act and other applicable laws and regulations of the Republic of Korea, as well as relevant privacy guidelines that must be observed by

personal information handlers. In accordance with Article 30 of the Personal Information Protection Act, Lunit has established and publicly discloses this Privacy Policy to protect users' personal information and to ensure the prompt and efficient handling of any related inquiries or complaints. This Privacy Policy applies uniformly not only to Lunit's official website but also to all business sites, subsidiaries, business activities, and relationships where Lunit collects, uses, or processes personal information, as specified in [Section 2. Scope of Application].

9. Items of personal information to be processed:

Lunit processes the following categories of personal information.

1. **Representative Website Product Inquiries:** Name, email, phone number, country, title, organization/company name, nature of inquiry
2. **Job application and recruitment inquiry on recruitment website:**
    i. Job Application
        1. Required: Name, address, phone number, cell phone number, e-mail, resume (Nationality, eligibility for veterans and disabled persons, academic background and grades, work experience, military service, overseas experiences, social activity, languages and other skills, awards, hobbies, talents, self-introduction, etc)
        2. Optional: additional submissions (skills, cover letters, portfolios, etc)
3. **Providing SCOPE Services**
    i. Required: Name, e-mail
    ii. Optional: cell phone number
4. **Product Technical Assistance:** email
5. **Product Educational Assistance:** email
6. **Other information items that may be automatically generated and collected during service use on the Internet:** IP addresses, cookie, MAC addresses, service use records, visit records, and locations

10. Purpose of Processing Personal Information:

Lunit processes personal information for the following purposes. Your personal information processed by Lunit is not used for any purpose other than the purposes specified in the following, and we will take necessary measures when any change occurs in the purposes of use, such as obtaining additional consent in accordance with Article 18 of the Personal Information Protection Act.

1. **Representative Website Product Inquiries:** Responding to inquiries about Lunit's Products (Insight CXR, Insight MMG, SCOPE)
2. **Job application and recruitment inquiry on recruitment website:** Managing recruitment process, providing recruitment information, notification for each selection process, handling recruitment inquiries, etc.
3. **Providing SCOPE Services:** providing Scope IO services
4. **Product Technical Assistance:** providing technical assistance for any of Lunit's products
5. **Product Educational Assistance:** providing education and training for any of Lunit's

Outsourced Companies	Outsourced Tasks
Workable Software Limited	Operation of recruitment website and recruitment management computer system and handling of related complaints
AWS	Data archiving and infrastructure management
Fivecloud	IT system maintenance
Miracle Four Man	Information desk management

products

11. Period of Processing and Retaining Personal Information:

Lunit handles and retains personal information only during the period specified by relevant statutes for retaining and using personal information or the period to which each User consents when we collect the User's personal information.

The period using which a User's personal information is handled and retained is as follows:

1 **Representative Website Product Inquiries:** until permission is rescinded
2 **Job application and recruitment inquiry on recruitment website:** 2 years
3 **Providing SCOPE Services:** until the end of the service
4 **Product Technical Assistance:** until permission is rescinded
5 **Product Educational Assistance:** until permission is rescinded

As a general rule, Lunit does not use or provide personal information without the data subject's consent.

However, in accordance with applicable laws and regulations, the criteria for determining whether additional use or provision without the data subject's consent is permissible are as follows:

- Whether the additional use or provision is related to the original purpose of collection
- Whether the additional use or provision is reasonably foreseeable considering the circumstances under which the personal information was collected or based on customary processing practices
- Whether the additional use or provision unfairly infringes upon the interests of the data subject
- Whether necessary measures have been taken to ensure safety, such as pseudonymization or encryption

12. Outsourcing of Personal Information Processing:

In accordance with Article 26 of the Personal Information Protection Act, Lunit outsources the processing of a User's personal information to maintain its websites as follows:

When executing an outsourcing agreement, Lunit agrees on responsibilities such as the prohibition of processing of personal information other than for the purpose of performing outsourced tasks, technical and administrative protection measures,

restrictions on re-outsourcing, management and supervision of the outsourced companies, and compensation for damages, in accordance with Article 26 of the Personal Information Protection Act, and supervise whether the outsourced companies handles personal information safely.

In case of any change to the outsourced tasks or companies, Lunit will promptly disclose the information through this Privacy Policy.

13. International Transfer of Personal Information:

Lunit may transmit or manage the User's personal information overseas for the purpose of service provision and user convenience as follows:

Name of Recipient	**Workable Inc.**	**Amazon Web Services, Inc.**
Contact	support@workable.com	aws-korea-privacy@amazon.com
Items of personal information transferred	Name, Nationality, Address, Eligibility for Veterans and Disabled Persons, Phone number, Mobile number, Education, Grades, Military services, Work experiences, Overseas experiences, Social activity, Languages and other skills, Awards, Hobbies, Talents, Cover Letter	Name, E-mail, Phone number
The country to which the personal information is transferred, Transferred Data, and transferred method	USA, transferring data over the network to servers located in the Workable's service areas	USA (Oregon region), Movement of data location through the network
The purpose for transferring personal information	Operation of recruitment website and recruitment management computer system; handling of related complaints	Data archiving and infrastructure management
Retention Period	Until the end of the recruitment process	3 years

※ Users may refuse the transfer of their personal information to foreign countries through the company's privacy protection officer or designated personnel. If a user refuses the transfer of their personal information to foreign countries, the company will exclude that user's personal information from being transferred abroad. However, in this case, the user may not be able to use services for which the transfer of personal information abroad is a mandatory part of the service.

14. Destruction of Personal Information:

Lunit destroys a User's personal information after the period during which the personal information is retained ends or the purposes of handling the personal information have been attained.

If Lunit is required by the relevant laws or regulations to retain personal information even when the agreed retention period is over or after achieving the purpose of its collection, Lunit shall transfer the said personal information (or personal information file) to a separate database or another storage space.

The procedure, deadlines, and methods for destroying it are as follows:

1 **Procedure for Destruction**: Lunit selects personal information (or personal information file) subject to destruction, obtains approval from the person in charge of personal information protection, and destroys it.

2 **Methods for Destruction**: Personal information stored in electronic file formats is to be deleted using technical means which makes the information unrecoverable. Personal information recorded and stored in paper is to be destroyed through shredding or incineration.

15. Rights and Obligations of Information Subject:

① The data subject may exercise their rights (hereinafter referred to as "exercise of rights") at any time with respect to Lunit, including the right to access, correct, delete, suspend processing, withdraw consent, refuse automated decisions, or request an explanation.

※ Requests for access, correction, or deletion of personal information regarding children under the age of 14 must be made directly by the child's legal guardian. For data subjects who are minors aged 14 or older, they may exercise their rights regarding their personal information either by themselves or through their legal guardian.

② An information subject may exercise the rights specified in paragraph (1) above via written documents or e-mail, etc. In such cases, Lunit will promptly take the required actions. Lunit will confirm whether the person who requested access, correction, deletion, or suspension of processing according to the rights of the information subject is the person or a legal representative.

③ In case of a User requests the correction or deletion of his/her personal information, Lunit does not use or disclose the relevant personal information to any third party until the correction or deletion is complete.

④ A User may exercise his/her rights through an agent such as his/her legal representative or a person with a mandate. In such cases, the User shall submit a power of attorney as specified in attached Form 11 of Notification on the Methods of Personal

Information Processing
⑤ Users must not infringe on their own privacy or the privacy of other people collected by Lunit by violating the Act on the Protection of Personal Information
⑥ The rights of the information subject may be restricted in accordance with Article 35, Paragraph 4 or Article 37, Paragraph 2 of the Personal Information Protection Act.
⑦ If the personal information is specified as the collection target in other laws, the personal information may not be deleted even if you request the deletion of the personal information.
⑧ If the data subject has given consent to the fact that automated decisions will be made, or if it has been notified in advance through a contract or other means, or if there is a clear legal provision, the refusal of automated decisions will not be allowed, and only a request for explanation and review is possible. Additionally, a request for refusal or explanation of automated decisions may be rejected if there is a legitimate reason, such as a concern that could unfairly infringe upon the life, body, property, or other interests of others.
⑨ Lunit verifies whether the person exercising their rights is the data subject or a legitimate representative.

16. Measures for Ensuring Safety of Personal Information:

Lunit has taken the following measures necessary for ensuring safety, in compliance with Article 29 of the Personal Information Protection Act:

1. **Administrative measures:** Establishment/Implementation of internal management plans, regular training of employees, etc.
2. **Technical measures**: Management of access to systems processing personal information, installation of access control systems, encryption of identifiable information, and installation of security programs.
3. **Physical measures:** Access control to computer rooms and data storage rooms

17. Installation and Operation of Automatic Personal Information Collection Devices:

Lunit uses “cookies” that store and loads user information to give you the best experience on our website. Cookies are small pieces of information sent from the Website’s server to the browsers in the User’s computers. Some of them are stored in the User’s hard disk drive.

1. **Purpose of Using Cookies:** These cookies enable Lunit to anonymously track how Users access and browse our website, thereby enabling us to optimize and improve our service.
2. **Cookie Installation, Use, and Refusal:** You can refuse to store cookies by changing the setting at the [Tools] > [Internal Option] > [Personal Information] Menu on the Top of the Web Browser Screen. Your refusal to store cookies does not disadvantageously affect your use of the Website.

18. **Privacy Officers**

Lunit has appointed the following persons as its Personal Information Protection Officer for the coordination of all tasks related to the processing of personal information, addressing information subjects’ complaints regarding the processing of personal

information, and providing remedies for damages.

Chief Privacy Officer	Privacy Manager
Name: Jungin-Lee Department: Information Security Team, Infrastructure Department E-mail: jilee@lunit.io	Name: Seungwoo Jung Department: Information Security Team, Infrastructure Department E-mail: jsw@lunit.io

Please contact the Chief Privacy Officer or Privacy Manager for any question, complaint, and remedy related to personal information during the use of Lunit's services. Lunit will promptly respond to and process your inquiry.

19. **Request to Inspect Personal Information:**
A User may request Lunit to permit him/her to inspect his/her personal information under Article 35 of the Personal Information Protection Act. Lunit will strive to ensure that such requests will be processed without delay.

Department in charge of personal information request
Name: Seungwoo Jung Department: Information Security Team, Infrastructure Department E-mail: jsw@lunit.io

20. Remedies for Violation of Rights and Interests:
Please make inquiries to the following organizations if you need to report or consult in regards to the violation of personal information.

- Personal Information Dispute Mediation Committee (http://www.kopico.go.kr / (Toll Free) 1833-6972)
- Personal Information Infringement Report Center (http://privacy.kisa.or.kr / (Toll Free) 118)
- The Cyber Crime Investigation Team of the Supreme Prosecutors' Office (http://www.spo.go.kr / (Toll free) 1301)
- The Cyber Terrorism Response Center of the National Police Agency (http://cyberbureau.police.go.kr / (Toll free) 182)

21. Modification of Privacy Policy:
Lunit may amend its Privacy Policy to reflect any legal or service changes. Lunit shall promptly notify such amendment in advance.