# Cloud Security Policy

In providing cloud services to customers under its ISO/IEC 27017 certification, the Company establishes this Cloud Security Policy, which addresses security matters specific to cloud services, in addition to its Information Security Basic Policy.
This Policy is established under the Company's Information Security Basic Policy.
This Policy applies to the following cloud services: “PreferredAI Work Suite” and “Preferred Computing Platform (PFCP).”

## 1．Information Security Requirements Applied to the Design and Implementation of Cloud Services

- The Company designs and implements its cloud services in accordance with customers’ information security requirements and this Policy.

## 2．Risks Associated with Cloud Services

- The Company implements appropriate controls to address risks related to cloud services identified through risk assessments.

## 3．Multi-tenancy and Segregation Between Cloud Service Customers (Including Virtualization)

- Where cloud services are used by multiple customers, the Company ensures information security for each customer by appropriately employing proven virtualization technologies, container technologies, and application-level access controls to logically segregate data and processing operations on a per-customer basis.

## 4．Access to Customer Assets by Company Employees

- Except where necessary to provide the services set forth in the Company's

terms of service, the Company does not access customer assets without the customer's prior consent.

## 5. Access Control

- The Company implements appropriate authentication methods for customer access to cloud services.

## 6. Notifications to Customers

- Notifications concerning the cloud services used by customers will be provided by posting them on the Company's website, notifying the customer's representative, or using other appropriate means.

## 7. Access to and Protection of Customer Data Handled Within Cloud Services

- Within the scope of the Company's responsibilities as set forth in the terms of service, the Company implements appropriate access management and protection measures for customer data handled within its cloud services.

## 8. Management of Customer Accounts

- Except as otherwise provided in the Company's terms of service, customers are responsible for the management and operation of their own accounts.

## 9. Information Sharing Regarding Incident Notification, Response, and Forensic Investigation

- If the Company detects unauthorized activity or violations related to the use of its cloud services, it will share information with the customer for the purposes of notification of such activity or violations, investigation, and forensic support.

Established on August 19, 2026
Daisuke Okanohara
Representative Director and CEO
Preferred Networks, Inc.