



Security White Paper

Updated 1 October 2026

wework

Executive Summary

Guided by the principles of ISO/IEC 27001 Information Security Management, WeWork Japan takes a multi-layered approach to security. This helps our customers use our Workplaces with confidence.

Physical Security (Facility, Access, and Visitor Management)

We work to ensure the safety of our locations through the management of access records, visitor records, CCTV Surveillance, Private Offices, and Common Areas.

Technical Security (Wi-Fi, Network, and IT Options)

We work to mitigate risks in shared environments through Wi-Fi, wired LAN, communication encryption, and restrictions on device-to-device communication.

Organisational and Personnel Security (Structure, Rules, and Operational Management)

We are committed to continual improvement through our security management structure, employee awareness and training, Supplier Management, log management, incident response, internal inspections and audits, and Corrective Action.

Protection of Personal Information and Data

In accordance with applicable legislation, internal regulations, and published policies, we protect personal information, access information, equipment usage history, and CCTV Surveillance footage appropriately.

Division of Responsibilities with Customers

We clarify the scope provided and managed by WeWork Japan and the scope to be managed by the customer. We emphasise maintaining a secure usage environment through mutual cooperation.

.

General Notes on This Document

Security measures, service details, optional responses, and the availability of records, logs, and footage described in this white paper may vary depending on the location, building specifications, contract plan, usage area, equipment status, individual conditions, and legal or contractual restrictions.

Access records, visitor records, CCTV Surveillance footage, logs, Network configurations, internal operational procedures, audit materials, and other Information may contain personal information or Information requiring security protection. We assess requests to confirm or provide such Information on a case-by-case basis. In doing so, we consider the purpose and necessity of the request, the scope of Information requested, contract conditions, applicable legislation, personal information protection, third-party rights, and security requirements. Information is provided only within the scope that can be disclosed.

Where you have specific security requirements, please verify the provision conditions for each target location prior to contracting or commencing use.

.

Table of Contents

Executive Summary	2
General Notes on This Document	3
1. Basic Approach to Security	7
1.1 WeWork Japan's Approach to Security	7
1.2 Security Domains Covered	8
1.3 Approach to Disclosed and Undisclosed Information	8
1.4 Continual Improvement	9
2. Physical Security	9
2.1 Basic Approach to Physical Security	9
2.2 Access Management	10
2.3 Visitor and Worker Management	10
2.4 Management of Areas Where Information Assets are Handled	11
2.5 CCTV Surveillance and Crime Prevention Measures	11
2.6 Physical Management of Documents, Devices, and Removable Media	12
2.7 Information Management in Private Offices and Common Areas	12
2.8 Location Differences Regarding Physical Security	12
3. Technical Security	13
3.1 Basic Approach to Technical Security	13
3.2 Standard Internet Connection Services	13
3.3 WeWork Wi-Fi Security	14

3.4 Guest Network	15
3.5 Wired LAN Connection	15
3.6 Network Segregation and Dedicated Networks	16
3.7 Support for Customer-Specific Networks	16
3.8 Approach to Brought-in Devices and Access Points	17
3.9 Equipment Management in IT Closets	17
4. Organisational and Personnel Security	18
4.1 Basic Approach to Organisational and Personnel Security	18
4.2 Security Management Structure	18
4.3 Identification and Risk Assessment of Information Assets	19
4.4 Information Classification and Handling	20
4.5 Confidentiality Obligations and Management of Confidential Information	20
4.6 Awareness and Training for Employees	21
4.7 Supplier Management and Management of Contracted Workers	21
4.8 Operational Management of Accounts and Permissions	22
4.9 Log Collection and Management	22
4.10 Incident Response Structure	23
4.11 Internal Inspections, Audits, and Corrective Action	23
4.12 Continual Improvement	24
5. Protection of Personal Information and Data	24
5.1 Basic Approach to the Protection of Personal Information	24

6. Division of Responsibilities with Customers	25
6.1 Basic Approach to the Division of Responsibilities	25
6.2 Main Scope Managed and Operated by WeWork Japan	25
6.3 Main Scope to be Managed by the Customer	26
6.4 Shared Responsibilities	27
6.5 Division of Responsibilities by Area	28
6.6 Differences Based on Location and Contract Conditions	31
6.7 Requests for Maintaining a Secure Usage Environment	32
7. Certifications, Third-Party Evaluations, and Referenced Frameworks	33
7.1 ISO/IEC 27001 Certification Status and Scope of Application	33
7.2 Third-Party Evaluations and External Audits	34
7.3 Referenced Security Frameworks	34
7.4 Utilisation of the NIST Cybersecurity Framework	34
7.5 Reference to Practical Security Controls such as CIS Controls	35
8. Enquiries and Additional Disclosures	35
8.1 Enquiries Regarding Security	35
8.2 Responses to Security Questionnaires	36
8.3 Approach to Additional Disclosures	36
8.4 Positioning of This White Paper	37
8.5 Updates and Continual Reviews	37
8.6 Related Information	38

1. Basic Approach to Security

In this white paper, corporate, organisational, and individual customers who contract or use WeWork Japan's services are collectively referred to as "Customers". Registered users who actually use WeWork Japan's Workplaces are referred to as "Members" in accordance with our service terminology. Those visiting Members and event participants are referred to as "Guests" or "Visitors".

"Workers" refers to external parties other than our employees who enter WeWork Japan locations, workspace areas, facility management areas, IT Closets, and other managed areas for the purposes of cleaning, security, facility maintenance, inspection, repair, construction, delivery, installation and maintenance of Network equipment, and other operations.

In this white paper, the usage environment including office spaces, Common Areas, meeting rooms, communication environments, shared facilities, and facility operations provided by WeWork Japan is collectively referred to as "Workplace" or "Workplace Environment". When describing the form of office services flexibly used by multiple companies and users, we use the term "Flexible Office".

1.1 WeWork Japan's Approach to Security

As a company providing Flexible Offices, WeWork Japan emphasises continuing to provide a secure and safe environment for all users. We regard enabling customers to conduct their business safely in a highly secure environment as an important element of our service quality.

WeWork Japan is an affiliate of SoftBank, which provides communications infrastructure that supports society in Japan. Guided by the value of providing a stable environment, we work to maintain and continually improve the safety and stability of our Workplace Environment.

1.2 Security Domains Covered

This white paper covers the following security areas related to the Workplaces provided by WeWork Japan:

Physical security regarding access management to locations, visitor management, CCTV Surveillance, and Private Offices.

Technical security regarding Networks, account management, log management, device management, and vulnerability remediation.

Organisational and personnel security regarding security policies, management structures, employee training, Supplier Management, audits, and incident response.

Protection of personal information and data regarding the handling of personal information, visitor information, access information, and footage information.

Division of Responsibilities to clarify the scope provided and managed by WeWork Japan and the scope to be managed by the customer.

By systematically organising these areas, we demonstrate WeWork Japan's approach to security and the overall picture of our specific initiatives.

1.3 Approach to Disclosed and Undisclosed Information

In this white paper, we explain Information necessary for customers to use our services with confidence, within the scope permitted for public disclosure.

Detailed security management procedures, Network configurations, specific monitoring and detection conditions, detailed log specifications, and internal operational procedures are generally not disclosed, as their disclosure could increase security risks.

WeWork Japan seeks to balance transparency with security. We provide Information that can be disclosed so that customers can carry out the necessary

checks when using our services, while carefully managing Information that requires protection for security reasons.

1.4 Continual Improvement

Security is not a one-time effort. The business environment, technological landscape, threat trends, and customer usage patterns are constantly changing. We must continually review the necessary Security Controls accordingly.

WeWork Japan works to maintain and improve its security levels through ongoing risk identification and review of Security Controls. Our activities include employee awareness and training, internal reviews and inspections, internal audits within the applicable ISMS scope, incident response, and Corrective Action.

We review our operations and documentation as needed in response to customer requests, security questionnaires, changes in legislation, guidelines and industry standards, and the expansion of our business and services.

2. Physical Security

2.1 Basic Approach to Physical Security

WeWork Japan works to ensure physical safety through access management, visitor management, workspace management, CCTV Surveillance, disaster prevention equipment, and cleaning and hygiene management at our locations, enabling Members to use the Workplaces with confidence.

Both system-based and physical security measures are important for protecting Information Assets. Physical security includes managing areas where Information is handled, controlling access to those areas, securely storing documents, devices and removable media, and managing Visitors. By implementing physical Security Controls suited to the characteristics of the locations and usage areas, we strive to maintain a secure and safe Workplace Environment.

2.2 Access Management

Access management is a fundamental control to ensure that Members with Access Rights, Visitors, WeWork employees, and Workers can use the facilities within their respective authorised scopes.

WeWork Japan conducts access management using IC key cards, smart locks, reception services, and guest pre-registration systems, depending on the characteristics of the locations and usage areas. Access management here refers to appropriately controlling entry to facilities and managed areas, ensuring that authorised individuals can use them within their respective authorised scopes. The types and scope of records collected and managed may vary depending on the location, equipment specifications, usage area, and service details.

Based on the approach described in "General Notes on This Document" at the beginning of this document, we verify the necessity and target scope before responding to requests to confirm or provide access records. Note that some access information may be provided depending on contract conditions or as a paid service.

2.3 Visitor and Worker Management

Where Visitors or Workers enter our locations, WeWork Japan manages their access through reception services and guest registration.

Where Visitors or Workers enter workspaces, facility management areas, or other managed areas, we verify the purpose of the visit, work details, entry areas, and work hours. Where necessary, we manage this through accompaniment by individuals with Access Rights, confirmation at reception, prior application, or supervision.

2.4 Management of Areas Where Information Assets are Handled

WeWork Japan appropriately selects locations to handle Information Assets based on the importance of the Information and the nature of the work, implementing management suited to the characteristics of the area.

Common Areas, workspaces, and facility management areas where Network equipment is installed require different levels of management. We work to ensure the security of each area by combining access management, user management, and facility management.

Where highly confidential Information is handled, we instruct employees to use appropriate locations such as meeting rooms or back offices, depending on the nature of the Information and the work. We also request customers and Members to be mindful of screen displays, conversations, and the handling of documents and devices depending on the usage location, such as Common Areas or meeting rooms.

2.5 CCTV Surveillance and Crime Prevention Measures

WeWork Japan installs and operates CCTV cameras in Common Areas for crime prevention, investigation of accidents and incidents, user protection, and facility management.

We manage CCTV Surveillance footage within the scope necessary for security management and restrict viewing access to those with a legitimate business need. We protect footage appropriately from the perspective of personal information and data protection.

2.6 Physical Management of Documents, Devices, and Removable Media

WeWork Japan emphasises the physical management of documents, devices, and removable media to prevent the theft, loss, unauthorised viewing, or improper disposal of Information Assets.

For confidential documents, removable media and portable devices, controls may include avoiding leaving items unattended, secure storage, and appropriate disposal, depending on their purpose and the importance of the Information. We also provide awareness and training to help prevent documents and devices from being exposed to third parties or removed without authorisation when employees leave their desks or at the end of the working day.

2.7 Information Management in Private Offices and Common Areas

WeWork Workplaces feature flexible usage patterns combining Private Offices, meeting rooms, Common Areas, and lounges.

While WeWork Japan provides Security Controls such as facility, equipment, and access management, we also request Members to manage Information appropriately according to their usage location.

In particular, where Confidential Information is handled in Common Areas or meeting rooms, we recommend that Members be mindful of shoulder surfing or conversations being overheard by people nearby, and use more appropriate locations such as Private Offices or meeting rooms where necessary.

2.8 Location Differences Regarding Physical Security

Physical security measures may vary depending on the location, building specifications, contract plan, usage area, and the presence of exclusive zones.

Where you have specific requirements regarding access management, smart locks, CCTV Surveillance, out-of-hours security, IT Closets, server equipment installation, or additional security requirements, please verify the equipment specifications, operational conditions, and the availability of additional support at the target location prior to contracting or commencing use.

3. Technical Security

3.1 Basic Approach to Technical Security

WeWork Japan provides Standard Internet Connection Services and various IT options to ensure Members can use a stable communication environment.

In a Flexible Office, multiple companies and users use services within the same location. The Network environment requires a balance of convenience, stability, segregation, and safety.

While providing a standard internet connection environment, WeWork Japan offers options such as dedicated VLANs, dedicated Wi-Fi, dedicated global IPs, and equipment hosting, based on the customer's usage patterns and security requirements.

3.2 Standard Internet Connection Services

WeWork Japan provides Standard Internet Connection Services that Members can use without additional costs. The standard services primarily include the following connection methods:

Wireless LAN connection service for Members

Wireless LAN connection service for Guests

Wired LAN connection service available within Private Offices

Wired LAN connection service available in certain meeting rooms

The Standard Internet Connection Service is a shared communication environment used by multiple companies, organisations, and users within the same location.

WeWork Japan works to mitigate risks in this shared environment through authentication, encryption, and restrictions on device-to-device communication.

Where customer-specific security requirements, traffic control, monitoring, closed network connections, fixed IPs, or dedicated segments are required, please consider individual configurations such as dedicated Networks, dedicated VLANs, or dedicated Wi-Fi.

The standard Network provides an internet connection environment. WeWork Japan does not manage or monitor the contents of connections to the customer's internal Networks, business systems, or cloud services. For access to your company's systems and business data, please implement Security Controls on your side, such as VPNs, zero-trust access, device authentication, and multi-factor authentication, where necessary.

3.3 WeWork Wi-Fi Security

WeWork Wi-Fi is the standard wireless LAN connection service available to Members within the facilities.

WeWork Wi-Fi works to mitigate risks associated with the shared environment by utilising per-user authentication, communication encryption, and restrictions on device-to-device communication*.

This suppresses unnecessary communication with other user devices connected to the same wireless LAN, mitigating risks arising from device-to-device communication in a shared environment.

Due to the nature of a shared Network, customers must appropriately manage their own devices, accounts, business data, and connection methods to their own systems.

Authentication methods, encryption standards, and supported protocols may change depending on location equipment, provided services, device compatibility, and operational conditions. We do not disclose detailed configuration information in public documents for security reasons.

*Services requiring peer-to-peer communication cannot be used due to restrictions on device-to-device communication.

3.4 Guest Network

WeWork Japan provides a wireless LAN connection service for Guests visiting Members.

The Guest Network is provided separately from the Member Network and is intended for a different purpose. Guests may use the Network after completing the designated authentication procedures.

The Guest Network is provided separately from the Members' business-use environment while supporting convenient Network access for Visitors.

We ask customers to provide appropriate guidance to their Visitors regarding the purpose of use, the handling of Confidential Information, and Information management during meetings.

3.5 Wired LAN Connection

WeWork Japan provides environments where wired LAN connections can be used in Private Offices and certain meeting rooms.

Wired LANs in Private Offices may be used to connect PCs, printers, and other business equipment. Wired LANs in meeting rooms may be used for purposes requiring stable communications, such as web conferencing.

The standard wired LAN forms part of WeWork Japan's standard Network. Where a customer requires a Network environment segregated from other users, please consider using individual options such as a dedicated VLAN.

3.6 Network Segregation and Dedicated Networks

Depending on the customer's security requirements, WeWork Japan may be able to provide individual Network configurations distinct from the standard Network.

For example, by combining options such as dedicated Networks, dedicated Wi-Fi, and fixed IPs, it is possible to implement configurations suited to the customer's usage patterns.

The availability, scope, specifications, costs, and implementation conditions of these options may vary depending on the location, floor, contract plan, building specifications, and Network equipment. Where you wish to use these, please verify their availability and operational conditions at the target location prior to contracting or implementation.

3.7 Support for Customer-Specific Networks

Business requirements may necessitate a unique Network configuration using the customer's own routers, lines, or Network equipment.

Under certain conditions, WeWork Japan will consider requests to bring customer-provided Network equipment into a location. We will review factors such as installation space, wiring, power supply, IT Closet availability, and work procedures.

These are not provided uniformly as standard services. Availability depends on the location, contract plan, IT Closet availability, building constraints, construction feasibility, and operational conditions.

Customers must independently configure, operate, monitor, maintain, and manage the security of their own equipment, communication lines, and systems.

3.8 Approach to Brought-in Devices and Access Points

To ensure wireless quality and a stable communication environment within our locations, WeWork Japan generally restricts the use of customer-provided Wi-Fi access points, Wi-Fi routers, mobile routers, and other devices that provide or relay Wi-Fi communications.

Where a customer configures their own Wi-Fi access points, Wi-Fi routers, or mobile routers, radio interference with the Wi-Fi equipment provided by WeWork Japan may occur, potentially affecting the communication quality within the facility and the usage environment of other users.

As a general rule, customers must use the standard wireless LAN service provided by WeWork Japan or an individually approved Network configuration.

The restrictions in this section primarily target devices and functions that provide or relay Wi-Fi communications. They do not target infrared communications, Bluetooth communications, or 4G/5G communications acting as mobile phone networks. However, mobile routers that use 4G/5G networks to provide Wi-Fi connections emit Wi-Fi signals and are therefore generally subject to restriction.

3.9 Equipment Management in IT Closets

WeWork Japan may accommodate customer equipment in IT Closets at select locations.

Where access to or work in the relevant area is required, arrangements are coordinated through a WeWork Japan representative in accordance with designated procedures. Where the customer or contractors appointed by the customer perform the work, prior application, verification of work details, supervision, and exit confirmation may be required.

Conditions vary by location and building specifications, including available installation space, power supply, permitted working hours, and construction

feasibility. Customers remain responsible for the installation, power management, maintenance, replacement, monitoring, backup, and troubleshooting of their own equipment.

4. Organisational and Personnel Security

This chapter explains the organisational processes that support the operation of technical Security Controls, including security policies, management structures, employee training, Supplier Management, account and permissions management, log management, and incident response.

4.1 Basic Approach to Organisational and Personnel Security

WeWork Japan positions Information Security as a comprehensive initiative that includes management, organisation, employees, business processes, Supplier Management, and incident response, rather than solely technical measures.

For Security Controls to function effectively on an ongoing basis, systems and equipment alone are not enough. We also need an appropriate operational structure, an understanding of Information Security among employees, and sound decisions and actions in daily work.

We work to ensure the provision of safe and secure services by establishing a security management structure, appropriately managing Information Assets, providing awareness and training to employees, collaborating with suppliers, and maintaining an incident response structure.

4.2 Security Management Structure

WeWork Japan positions Information Security as an important management theme and has established a structure to implement Information Security policies, manage risks, operate Security Controls, respond to incidents, and drive improvement activities.

Matters relating to Information Security are managed through collaboration among relevant departments, incorporating perspectives from Information Systems, legal, facility operations, sales, and customer support. For Information Assets held and used by each department, we clarify management responsibilities based on the nature of the work and the importance of the Information, conducting necessary verifications and improvements.

Where a significant security issue or incident occurs, we report to relevant parties including senior management. After confirming the scope of impact, causes, and urgency, we determine and implement response policies, Corrective Action, and Measures to prevent recurrence.

4.3 Identification and Risk Assessment of Information Assets

WeWork Japan identifies Information Assets handled in its operations and manages their storage locations, Access Rights, retention periods, and handling methods according to their importance and purpose of use.

Information Assets include paper documents, electronic data, business systems, Networks, removable media, access records, visitor records, CCTV footage, contract information, customer information, and personal information.

We assess risks relating to these Information Assets from the perspectives of confidentiality, integrity, and availability. Based on the assessed level of risk, including its potential impact and likelihood, as well as business necessity, we review and implement appropriate Security Controls.

Where changes occur in the business environment, service details, system configurations, legislation, guidelines, or threat landscape, we review the relevant risk assessments and Security Controls as necessary.

4.4 Information Classification and Handling

WeWork Japan appropriately classifies and handles Information Assets according to their importance and confidentiality.

Information critical to management, customer information, personal information, contract information, technical information, and Information that should be shared on a restricted basis for business purposes are managed so they can only be viewed and used within the necessary scope.

When creating, acquiring, editing, copying, transmitting, storing, or disposing of Information Assets, we verify the Information Classification, purpose of use, disclosure scope, retention period, and handling methods, managing them according to their classification. When transmitting or sharing important Information, we implement protective measures suited to the nature of the Information, such as access control, encryption, and verification of recipients.

4.5 Confidentiality Obligations and Management of Confidential Information

WeWork Japan manages Confidential Information to ensure that employees do not use information obtained in the course of their duties for non-business purposes or improperly disclose it to third parties.

Where Confidential Information needs to be shared with external parties, we confirm the recipient, purpose, and scope of the Information, establishing non-disclosure agreements where necessary.

When employees leave their duties due to resignation, transfer, or contract termination, we verify loaned items, accounts, Access Rights, and retained Information to help prevent access that is no longer required and the unauthorised removal of Information.

4.6 Awareness and Training for Employees

WeWork Japan provides awareness and training to help employees understand their Information Security roles and responsibilities, make appropriate decisions, and take appropriate action in their daily work.

Our awareness and training cover Information Classification and handling, personal information protection, account and password management, phishing prevention, device use, secure communication, and incident reporting.

We review and update our training content in response to changes in the business environment, threat landscape, business processes, legislation, and guidelines, with the aim of improving employees' security awareness and practical skills.

4.7 Supplier Management and Management of Contracted Workers

Where suppliers or contracted Workers have access to our Information Assets, facilities, equipment, or services, WeWork Japan identifies the necessary security requirements based on the nature of the work, the importance of the Information involved, the areas they can access, and their access to systems.

When engaging suppliers or before they begin work, we define the necessary conditions based on the nature of the work and associated risks. These include responsibilities, Information handling, confidentiality, sub-contracting, Access Rights, incident communication, management of loaned items, and the return or deletion of Information upon contract termination.

We review each supplier's management practices based on the outsourced work and associated risks. Where we determine improvement is necessary, we require Corrective Action or improvements.

We also manage external parties engaged in cleaning, security, facility maintenance, and building management. Depending on their work, location,

working hours, and potential access to Information Assets, appropriate measures may include contractual controls, access management, supervision, and accompaniment.

4.8 Operational Management of Accounts and Permissions

WeWork Japan grants Permissions to business systems and Information Assets only to the extent necessary for business operations.

We manage the issuance, modification, and deletion of accounts and Permissions based on the purpose of use and assigned duties. Where access is no longer required due to transfer, resignation, or contract termination, we promptly review or remove Permissions.

As a rule, accounts are not shared. Where sharing is justified, we clarify the purpose, users, and management responsibilities before implementing necessary controls. We verify Access Rights according to business necessity and risks, ensuring no unnecessary or excessive Permissions remain.

4.9 Log Collection and Management

WeWork Japan collects and manages logs to the extent necessary for operational and security management purposes. This allows us to understand the usage status of Information Systems and utilise the logs for investigating Unauthorised Access, inappropriate operations, or incidents.

We define how logs are managed based on the purpose of use, legislation, contracts, internal regulations, and security requirements. This includes the scope and retention periods of logs, Viewing Access, and whether logs may be provided. We limit Viewing Access to those with a legitimate business need.

When we receive a request to confirm or provide logs, we assess the necessity and scope of the request in accordance with the approach described in "General Notes on This Document".

4.10 Incident Response Structure

WeWork Japan maintains an incident response structure to address Information leaks, loss, Unauthorised Access, malware infections, system failures, unauthorised use, and other security concerns.

Where an incident or suspected incident is detected, we promptly share relevant information with the appropriate parties, assess the scope of impact, investigate the cause, take initial response measures, seek to prevent further damage, restore affected systems, and consider Measures to prevent recurrence.

Where a significant impact is anticipated, we report the matter to relevant parties, including senior management, and take the necessary decisions and actions.

Where WeWork Japan confirms a security incident related to the facilities, Networks, access management, or personal information management provided by WeWork Japan that may significantly affect customers, we notify affected customers promptly, based on the information known at the time and taking into account applicable contractual conditions, legislation, personal information protection requirements, the progress of the investigation, and the need to prevent further or secondary harm.

To the extent practicable, such notification may include a summary of the event, the anticipated scope of impact based on the information available at the time, interim measures taken, matters requiring further investigation, actions we ask customers to consider or verify, and the anticipated next steps.

4.11 Internal Inspections, Audits, and Corrective Action

WeWork Japan periodically conducts internal inspections and audits to assess the effectiveness of our Information Security management. These cover Information Asset management, Access Rights, Supplier Management, training, incident

response, log management, personal information protection, and the operation of other Security Controls.

Where issues are identified through internal inspections and audits, incident response, supplier reviews, or customer requests, we investigate the causes and determine and implement appropriate Corrective Action or improvements.

We verify the effectiveness of the measures implemented to help prevent recurrence and improve Security Controls.

4.12 Continual Improvement

WeWork Japan continually reviews security management based on the business environment, threat trends, legislation and guidelines, customer requests, and the results of incidents and audits.

We improve Information Security policies, risk assessments, Security Controls, training content, Supplier Management, access management, incident response, log management, and personal information protection where necessary.

5. Protection of Personal Information and Data

5.1 Basic Approach to the Protection of Personal Information

WeWork Japan treats Information relating to customers, Members, Visitors, business partners, employees, job applicants, and other individuals as critical Information Assets and protects it appropriately.

Within the Workplace Environment provided by WeWork Japan, we may handle personal information necessary to provide services, maintain a secure environment, manage security, and comply with legislation. This includes contract information, user information, visitor information, access information, meeting room reservation and usage information, enquiry information, and footage information.

In accordance with applicable legislation, internal regulations, our Privacy Policy, and our "Handling of Personal Information", WeWork Japan works to ensure that this personal information is acquired, used, stored, managed, provided, and disposed of appropriately.

For further details, please refer to our published "Handling of Personal Information".

6. Division of Responsibilities with Customers

6.1 Basic Approach to the Division of Responsibilities

WeWork Japan provides a Workplace Environment encompassing workspaces, shared facilities, building management, office security, and cleaning and hygiene management, enabling customers and Members to conduct business activities with confidence.

As WeWork Workplaces are Flexible Offices shared by diverse companies and users, maintaining security requires both WeWork Japan's controls and appropriate management of users, devices, and Information by customers.

Our basic approach is to clarify the scope provided and managed by WeWork Japan and the scope to be managed by the customer, emphasising that both parties cooperate to maintain a secure usage environment.

6.2 Main Scope Managed and Operated by WeWork Japan

Within the Workplace Environment we manage and operate, WeWork Japan is primarily involved in the following areas, working with building owners, property management companies, and other relevant parties where necessary:

Provision and operation of workspaces such as Common Areas, Private Offices, and meeting rooms.

Standard access management mechanisms using IC key cards, smart locks, etc.

Visitor management through guest registration systems and reception services.

Installation and operation of CCTV Surveillance within WeWork Japan's operational scope.

Management of equipment and fixtures within WeWork Japan's operational scope.

Coordination and alignment with relevant parties regarding building facilities, security, and disaster prevention.

Arrangement and operational management of cleaning and hygiene in Common Areas and Private Offices.

Provision and maintenance of shared facilities and fixtures, such as high-speed internet, printers, and disposal bins.

Handling enquiries regarding location operations and daily operational support.

These Security Controls and operational responses form part of the standard services and security management provided by WeWork Japan. However, specific provision details and the scope of WeWork Japan's involvement may vary depending on the location, contract plan, building specifications, and usage conditions.

6.3 Main Scope to be Managed by the Customer

Customers remain responsible for managing the security of their own users, Information, devices, systems, and data.

The following areas are primarily the customer's responsibility:

Adding, modifying, or deleting company users, and reviewing Permissions upon resignation or transfer.

Appropriate management of IC key cards, apps, and accounts.

Management of the company's devices, smartphones, removable media, and Network equipment.

Access management for the company's systems, cloud services, and data.

Device and system measures such as connection methods to company systems, device authentication, encryption, anti-malware measures, and patch application.

Management of documents, devices, Confidential Information, personal information, furniture, and fixtures within Private Offices.

Inviting Visitors, verifying the purpose of their visit, and managing their behaviour during the visit.

Information management when using shared printers, disposal bins, meeting rooms, and phone booths.

Even where WeWork Japan provides the Workplace Environment and standard services, customers must appropriately manage Information, devices, accounts, systems, and data related to their own business.

6.4 Shared Responsibilities

Matters involving both the facilities or services provided by WeWork Japan and the customer's environment may require cooperation between WeWork Japan and the customer.

The main areas of Shared Responsibilities include:

Confirming circumstances where suspicious individuals, unauthorised entry, theft, loss, or equipment abnormalities occur.

Supporting investigations where access records, visitor records, or CCTV Surveillance footage need to be reviewed.

Confirming the scope of impact and considering Measures to prevent recurrence when a security incident occurs.

Verifying individual requirements regarding exclusive zones, dedicated Networks, or server equipment installation.

Responding to customer security questionnaires, audits, and procurement reviews.

When confirming or providing records, footage, technical information, operational information, or other undisclosed Information, we will respond within the scope that can be disclosed, based on the approach described in "General Notes on This Document" at the beginning of this document.

6.5 Division of Responsibilities by Area

The following outlines the roles of WeWork Japan and the customer regarding key security management areas in the Workplace Environment provided by WeWork Japan.

Area	WeWork Japan's Main Scope	Customer's Main Scope
Workspace	Provision and operation of Common Areas, Private Offices, and meeting rooms.	Appropriate use by users; management of company Information and property.
Access Management	Provision of access management mechanisms using IC key cards, etc.	User registration, Permissions management, and appropriate management of cards, etc.

Area	WeWork Japan's Main Scope	Customer's Main Scope
Visitor Management	Provision of mechanisms such as guest registration and reception services.	Inviting Visitors, verifying visit purposes, and managing Visitors during their stay.
CCTV Surveillance	Installation and operation of CCTV Surveillance in Common Areas, etc.	Information management within company zones; informing Visitors and employees.
Private Offices	Provision of Private Offices and smart locks.	Locking the zone; management of documents, devices, and Confidential Information.
Network	Provision of a standard Network environment.	Management of company devices, accounts, and systems.
Shared Facilities	Provision and maintenance of printers, disposal bins, and fixtures.	Preventing printouts, discarded documents, and removable media from being left behind.

Area	WeWork Japan's Main Scope	Customer's Main Scope
Cleaning and Hygiene	Cleaning and disinfection maintenance of Common Areas and exclusive areas.	Organising and managing company property, confidential documents, and personal belongings.
General Incident Response	Confirmation and initial response regarding facilities and provided services.	Investigation and response regarding company devices, data, and business operations.
Suspicious Persons and Unauthorised Entry	Verification of access records, on-site response, and necessary communication.	Verification of company users and Visitors.
Theft in Private Offices	Verification of facility records and cooperation in investigations where possible.	Identification of company assets; handling police and insurance matters.
Customer Device Malware Infection	Verification of impact on the standard Network.	Device investigation, containment, and recovery.

Area	WeWork Japan's Main Scope	Customer's Main Scope
Network Outage	Verification and recovery of the provided service scope.	Verification of company equipment, VPNs, and cloud environments.
Protection of Personal Information	Protection of personal information acquired and managed by WeWork Japan.	Protection of personal information acquired and held by the customer.

Note that for individual Network requirements such as dedicated Networks, fixed IPs, router installation, or site-to-site VPNs, the availability of support varies depending on the location, contract plan, and Network specifications, requiring prior verification.

6.6 Differences Based on Location and Contract Conditions

The services and security measures provided by WeWork Japan may vary depending on the location, building specifications, contract plan, usage area, presence of exclusive zones, and use of optional services.

Where you have specific security requirements regarding Private Offices, exclusive floors, smart locks, IT Closet usage, additional access management, dedicated Networks, or individual equipment requirements, please verify the provision details, equipment specifications, operational conditions, and availability of additional support at the target location prior to contracting or commencing use.

6.7 Requests for Maintaining a Secure Usage Environment

WeWork Japan implements physical, technical, and organisational Security Controls to help customers use our Workplaces with confidence.

Security in a shared environment also relies on all Members using the Workplace appropriately. We ask customers to remind their users to manage IC key cards and accounts appropriately, lock their PCs when away from their desks, avoid leaving confidential documents unattended, manage Visitors and Information appropriately when using shared facilities, and promptly report any suspicious activity.

Through clear roles and cooperation with our customers, WeWork Japan will continue to work to maintain a secure and safe Workplace Environment.

Reference: Main Services Provided by WeWork Japan

The services available, including workspaces, meeting spaces, shared facilities and fixtures, building management, office security, community teams, cleaning, disinfection, and hygiene management, vary by location and contract plan. For the latest details, please contact our sales representatives or refer to our official documentation.

7. Certifications, Third-Party Evaluations, and Referenced Frameworks

7.1 ISO/IEC 27001 Certification Status and Scope of Application

WeWork Japan has established and operates an Information Security Management System (ISMS) based on ISO/IEC 27001, and has obtained ISO/IEC 27001 certification for its Headquarters and Shinjuku location.

The certification status is as follows:

Item	Details
Certification Standard	JIS Q 27001:2023 (ISO/IEC 27001:2022)
Registered Organisation	WWJ Corp.
Certification Registration Number	IR0234
Scope of Registration	Operational management of shared offices
Associated Locations	Headquarters, Link Square Shinjuku
Certification Body	IMJ Certification Body of Registration Center Co., Ltd

The scope of the ISO/IEC 27001 certification is limited to the registered organisation, scope of registration, and associated locations described in the certification registration Information. For locations outside the certification scope, we are guided by the Information Security management principles established within the certified scope. We implement security management appropriate to each location, taking into account its characteristics, building specifications, services provided, and operational conditions.

7.2 Third-Party Evaluations and External Audits

WeWork Japan undergoes assessments, audits, and evaluations by external organisations where necessary to assess the adequacy and effectiveness of our Information Security management.

External perspectives help us identify issues that may not be apparent through internal inspections alone. We use these findings to improve Security Controls, review our operations, and take Corrective Action.

For security and contractual reasons, we may limit the disclosure of detailed external audit results, audit procedures, individual findings, and internal documents.

7.3 Referenced Security Frameworks

With ISO/IEC 27001 as our primary framework, WeWork Japan refers to domestic and international security frameworks, guidelines, and industry standards where necessary to evaluate and improve Security Controls.

We use these frameworks not merely to demonstrate formal compliance, but to understand risks, organise Security Controls, prioritise improvements, and strengthen accountability internally and externally.

7.4 Utilisation of the NIST Cybersecurity Framework

WeWork Japan uses concepts from frameworks such as the NIST Cybersecurity Framework where necessary to systematically organise cybersecurity risks.

The NIST Cybersecurity Framework 2.0 provides a framework for organisations to manage cybersecurity risks through the functions of Govern, Identify, Protect, Detect, Respond, and Recover.

We use these concepts to structure our approach to security governance, risk identification, protection, detection, response, and recovery, and to review our overall security measures.

7.5 Reference to Practical Security Controls such as CIS Controls

We may refer to collections of practical Security Controls, such as CIS Controls, as reference information when reviewing technical and operational Security Controls.

However, this white paper does not declare compliance or comprehensive application of CIS Controls. Within our ISO/IEC 27001-based Information Security management framework, WeWork Japan references multiple frameworks and Security Controls where necessary to manage security according to our business characteristics, risks, and service provision formats.

8. Enquiries and Additional Disclosures

8.1 Enquiries Regarding Security

For questions about WeWork Japan's security, please contact us via the enquiry form on the WeWork Japan official website, or through your sales representative or designated point of contact.

Depending on the nature of the enquiry, we will work with the relevant departments and respond within the scope that can be publicly disclosed. The Information available and the details of our response may vary depending on the location, contract plan, usage conditions, and specific security requirements.

8.2 Responses to Security Questionnaires

Customers may ask us to complete security questionnaires or answer specific questions as part of procurement reviews or reviews by their information systems, legal, or audit teams.

WeWork Japan responds to security questionnaires and individual questions to the extent necessary for customers to evaluate or contract for our services. We determine the appropriate scope and method of response based on published

materials, this white paper, contract conditions, the relevant location and services, and the sensitivity of the Information requested.

Detailed Network configurations, internal operational procedures, monitoring and detection conditions, log specifications, supplier information, audit results, and other undisclosed Information are not provided as public documents. We consider requests for additional disclosure on a case-by-case basis, taking into account contracts, non-disclosure agreements, legislation, personal information protection, and security requirements.

8.3 Approach to Additional Disclosures

WeWork Japan places importance on providing customers with appropriate security-related Information so that they can use our services with confidence.

Detailed security management information may include Information that, if disclosed, could affect the safety of WeWork Japan or our customers. We respond to requests for additional materials, detailed Information, and evidence within an appropriate scope, taking into account contracts, non-disclosure agreements, legislation, personal information protection, and security requirements.

Examples of Information that may be disclosed include our certification status, an overview of our management structure and physical security measures, an overview of Network services, an explanation of the Division of Responsibilities, and published Information on personal information protection.

8.4 Positioning of This White Paper

This white paper is a public document intended to help customers understand WeWork Japan's approach to security and our primary initiatives.

This document does not take precedence over individual contracts, service specifications, terms of service, the "Handling of Personal Information", or other contractual or published documents. Service details, conditions of provision,

pricing, and availability may vary depending on the individual contract, location, contract plan, and usage conditions.

This document reflects the Information available at the time it was prepared and may be revised without notice in response to changes in legislation, technical environments, threat trends, service specifications, or operational structures.

This document is an English translation of the Japanese original for reference purposes only. In the event of any discrepancy or conflict between the English and Japanese versions, the Japanese original shall prevail.

8.5 Updates and Continual Reviews

WeWork Japan reviews and updates this white paper as necessary in response to reviews of security management, changes to service specifications, legislation or guidelines, customer requests, and the results of audits or inspections.

If you have questions about the latest version of this white paper or its contents, please contact us via the enquiry form on the WeWork Japan official website, or through your sales representative or designated point of contact.

8.6 Related Information

For details on how WeWork Japan handles personal information, please refer to our published "Handling of Personal Information".

For questions about specific service details, locations, contract plans, or security arrangements, please refer to our official website or contact your designated point of contact.

We hope this white paper helps you understand WeWork Japan's approach to security and our primary initiatives. WeWork Japan will continue to work with our customers to maintain and improve a secure and safe Workplace Environment.