Standard Operating Procedure (SOP)	**LOMBOK IX ACCESS** Jl Sukamulia, Rempung, Kec. Pringgasela, Kabupaten Lombok Timur, Nusa Tenggara Bar. 83661	**2025**

Purpose	The purpose of this policy is to establish standard operating procedures and access controls for the data center facility to ensure the comprehensive security of its physical assets, data, and overall infrastructure.
Scope	This policy applies to all individuals requiring access to the data center facility, including but not limited to: 1. All Employees (Permanent and Contract) 2. Vendors 3. Partners 4. Any other third party with authorized technical purposes.
Definitions	1. Data Center: A centralized facility housing network infrastructure, including servers, storage systems, networking equipment, and other supporting hardware. 2. Restricted Access: An area that may only be entered by specifically authorized personnel. 3. Access Log Book: A physical or digital record used to document the entry and exit of all personnel to and from a restricted area.
Supporting Resources	To support a secure and documented access process, the following resources and equipment will be utilized: 1. Access Cards (RFID) 2. Data Center Access Request Forms 3. Visitor IDs or Temporary Badges 4. CCTV Surveillance and Automated Door Control Systems

		5. Access Log Books (Physical or Electronic)
Access Request Procedure		
No	**Procedure**	**Description**
1.	Submitting an Access Request	Access requests must be submitted by the user (both internal and external) through one of the following channels: • Official Form: By filling out the provided Data Center Access Request Form. • Internal Ticketing System: By creating a request ticket through the designated system. Submission Deadlines: • Routine/Internal Access: A minimum of D-1 (one business day) prior to the visit. • Vendor/Third-Party Access: A minimum of D-3 (three business days) prior to the visit.
2.	Required Account Information	Each request must include the following contact information for the responsible party: 1. ID Card of the Owner/Customer 2. Contact Phone Number of the Owner/Customer 3. Name of the Technical Lead 4. Phone Number of the Technical Lead 5. Name of the Finance Lead 6. Phone Number of the Finance Lead Note: If the contact details are the same as the owner's, the fields can be filled with the customer's name and contact information accordingly.
3.	Details of Attending Personnel	The personnel who will be entering the Data Center must provide the following details: 1. Full Name 2. ID Number (KTP/NIP) and Company of Origin

		3. Purpose of the Visit 4. Planned Date and Time of Access 5. Estimated Duration of Access 6. List of Equipment Being Brought In (using a separate form that includes Device Name, Serial Number, and Quantity).
4.	Authorization and Approval	All requests will be reviewed and approved by authorized personnel. Approval will be granted in the form of: ● An Access Code (for internal personnel). ● Official confirmation via email, WhatsApp, or a signature on the request form (for external parties).

Data Center Entry Procedure

No	Procedure	Description
1.	Check-in Process at Reception / Security Post	As part of the initial procedure, all personnel must undergo a verification process at the reception or security area, which includes: 1. Verification of official identification (ID Card/Driver’s License/Company ID). 2. Recording personal details in the Access Log Book. 3. Submission of the approved access permit. 4. An inspection of all carried items to be checked against the approved list, such as: ○ Laptops ○ USB Drives ○ Cameras ○ Toolbox
2.	Escort and Supervision	1. Vendors or any external parties are required to be escorted and supervised at all times by a designated internal staff member (PIC).

		2. External personnel are not permitted to enter the Data Center unaccompanied.

Regulations Inside the Data Center

No	Procedure	Description
1.	No Food or Drinks Allowed	To prevent equipment damage and maintain the cleanliness of the data center, food and beverages are strictly prohibited.
2.	Footwear Must Be Removed	To prevent dirt, dust, and other particles from entering the highly sensitive environment and to minimize the risk of static electricity.
3.	Aktivitas dicatat pada log operaional	All actions performed must be recorded in the operational log, including the name of the personnel, time, and a description of the activity.
4.	Accessing Other Racks/Servers is Prohibited	Personnel are restricted to accessing only their designated racks. Accessing racks belonging to other parties is forbidden without prior authorization or an official work order from the equipment owner.
5.	No Equipment May Be Left Behind	All items brought into the data center must be brought out upon exit, unless the equipment has been granted prior approval for permanent installation in a rack.
6.	Maintain Cleanliness and Order	All cabling and connection panels must be left in a tidy and organized manner without disrupting or damaging the access or equipment of other tenants in the facility.

Data Center Exit Procedure

No	Procedure	Description
1.	Data Center Exit Procedure	Upon completing all activities, personnel must follow the check-out process, which includes: 1. Security personnel will log the official exit time.

		2. An inspection of all equipment will be conducted to ensure all items are accounted for. 3. All access cards or temporary badges must be returned to security personnel.
2.	Activity Reporting	Following a visit, the designated internal escort (PIC) is required to complete a brief report. 1. The report must include daily access data: company name, personnel names, activities performed, and timestamps. 2. The final status of the activity (e.g., completed or pending) must be clearly noted.
Monitoring and Auditing		1. The facility is monitored by 24/7 CCTV surveillance. 2. All surveillance recordings are securely stored for a minimum period of 90 days. 3. Periodic access audits will be conducted by the designated security team.

Violations and Sanctions

No	Violation Level	Examples and Sanctions
1.	Severe	Failure to properly sign the access log. ● A formal verbal warning will be issued.
2.	Moderate	Entering the facility without a valid or authorized access permit. ● A written warning will be issued, and the individual may be blacklisted from future access.
3.	Severe	Theft, property damage, or any act of sabotage within the Data Center. ● Immediate termination of contract/employment and/or legal action will be pursued.