SOP: Restricted Area Access Protocol for Visitors

This SOP establishes the **restricted area access protocol for visitors**, outlining procedures for identifying restricted zones, verifying visitor authorization, issuing temporary access permits, escorting visitors, and maintaining security logs. The goal is to ensure controlled and safe access to sensitive areas, protect confidential information and assets, and prevent unauthorized entry by visitors.

1. Purpose

To define and standardize the process for granting, controlling, and monitoring visitor access to restricted areas, ensuring security and compliance with company policies.

2. Scope

This SOP applies to all visitors requesting entry into company-designated restricted areas, as well as to all employees involved in the visitor access process.

3. Definitions

Term	Definition
Restricted Area	Any location or zone within company premises where entry is limited to authorized personnel only.
Visitor	An individual who is not an employee and requires access to company premises for a temporary period.
Access Permit	A temporary identification or pass allowing limited access to a specified area for a defined duration.
Escort	An authorized employee responsible for accompanying and supervising the visitor within restricted zones.

4. Responsibilities

- **Security Staff:** Enforces this protocol, verifies authorization, issues permits, and maintains logs.
- **Hosts:** Submit access requests, accompany visitors, and ensure compliance with security rules.
- **Visitors:** Follow all instructions, wear access permits visibly, and remain with their escorts at all times within restricted areas.

5. Procedure

1. **Identification of Restricted Areas:**
   All restricted zones must be clearly marked with signage and listed in the official site security documentation.
2. **Visitor Authorization:**
   - Host employee submits a visitor access request to security at least 24 hours in advance.
   - Request must include visitor's full name, purpose of visit, areas to be accessed, date and time of visit, and host contact information.
   - Security reviews and approves or denies the request based on policy.
3. **Check-in Process:**
   - Visitor signs in at the reception/security desk and presents valid government-issued identification.
   - Visitor is briefed on safety, confidentiality, and conduct expectations.
4. **Issuance of Temporary Access Permits:**
   - Upon approval, visitors are issued a dated, numbered badge or permit identifying authorized access zones.

- Permits must be worn visibly at all times while on site.
  5. **Escort and Supervision:**
     - Visitor must be accompanied by a designated host or security staff at all times within the restricted area.
     - Host is responsible for the visitor's adherence to rules and for reports of any incidents.
  6. **Logging and Documentation:**
     - All entries and exits of visitors are recorded in the security log with time stamps, visitor and host names, and permit numbers.
     - Logs are maintained for audit and compliance reviews.
  7. **Exit Procedure:**
     - Visitor returns the permit/badge to security upon departure.
     - Security ensures visitor is signed out and confirms no security breaches occurred during visit.

6. Security and Confidentiality

- Photographs, notes, or removal of materials from restricted areas are strictly prohibited unless pre-authorized in writing.
- Any suspicious activity or security incidents must be reported immediately to the security manager.

7. Records Management

- Visitor logs, access permits, and incident reports are retained as per company data retention policies.

8. Compliance

- Noncompliance may result in disciplinary actions for employees or denial of future access for visitors.

9. Revision History

Version	Date	Description	Approved By
1.0	2024-06-01	Initial SOP Release	Security Manager