SOP: Issuance of Company Identification and Access Credentials

This SOP defines the process for the **issuance of company identification and access credentials**, covering eligibility verification, documentation requirements, credential creation, and distribution procedures. It ensures secure and efficient management of employee and visitor identification to maintain workplace safety and access control.

1. Purpose

To establish a standardized procedure for verifying eligibility, processing documentation, creating, and distributing company identification and access credentials to authorized personnel and visitors.

2. Scope

This SOP applies to all employees, contractors, vendors, and visitors who require company-issued identification and access credentials.

3. Responsibilities

- **Human Resources (HR):** Initiates and verifies eligibility for ID issuance.
- **Security Department:** Oversees credential creation and distribution, maintains access controls.
- **IT Department:** Supports system setup for electronic credentials (if applicable).
- **Recipients:** Ensure safekeeping and appropriate use of issued IDs and credentials.

4. Procedure

1. **Eligibility Verification**
    - HR verifies employment status or visitor authorization.
    - Collects required personal data and documentation (see Section 5).
2. **Documentation Requirements**
    - For employees: Offer letter, government-issued ID, photo.
    - For visitors: Authorization letter/email, government-issued ID.
3. **Credential Creation**
    - Capture photograph (on-site or submit an approved photo).
    - Assign identification number and access permissions as per role.
    - Print physical ID card and/or configure electronic access credentials.
4. **Distribution**
    - HR/Security provides IDs to the recipient in person, upon verification.
    - Recipient signs an acknowledgment of receipt and compliance with company ID usage policy.

5. Documentation Requirements

Recipient Type	Required Documents
Employee	Offer Letter, Government-issued ID, Recent Photo, Security Clearance (if applicable)
Visitor/Contractor	Authorization Letter/Email, Government-issued ID, Company Point-of-Contact, Visit Purpose

6. Access Level Assignment

- Access rights are determined based on the recipient's role and area of responsibility.
- Security maintains an access level matrix and reviews it regularly.
- Requests for changes or additional access must be submitted through HR or departmental management.

7. Lost or Stolen Credentials

- Report immediately to HR and Security.
- Deactivate lost/stolen credential in the system.
- Request and process re-issuance as per standard documentation requirements.

8. Record Keeping

- Maintain a secure log of all issued, active, deactivated, and expired IDs.
- Retention period: Minimum of 2 years after ID expiration or employee separation.

9. Review and Revision

- This SOP will be reviewed annually or as required to reflect legal, procedural, or technological changes.

10. References

- Company Security Policy
- Employee Handbook
- Access Control Matrix (if applicable)