Standard Operating Procedure (SOP)

Document Title: Internal Data Access & Incident Response SOP

Version: 1.3
Effective Date: 1 March 2024
Department: Engineering & Security
Owner: Head of Platform Security

---

1. Purpose

This Standard Operating Procedure (SOP) defines the required process for requesting, granting, auditing, and revoking access to internal data systems. It also outlines the mandatory steps for responding to suspected or confirmed data security incidents.

This SOP applies to all full-time employees, contractors, and interns with access to internal systems.

---

2. Definitions

- **Sensitive Data:** Any data classified as Confidential or Restricted, including customer information, authentication credentials, financial records, and proprietary source code.
- **Access Request:** A formal request submitted by an employee to gain access to a specific internal system or dataset.
- **Incident:** Any event that may compromise the confidentiality, integrity, or availability of internal systems or data.
- **Security Team:** The internal team responsible for information security, incident response, and access governance.

---

3. Access Request Procedure

3.1 Eligibility

Only employees who have completed mandatory security training within the last 12 months are eligible to request access to sensitive data systems.

Contractors and interns require explicit approval from both their manager and the Security Team.

3.2 Submitting an Access Request

All access requests must be submitted through the Internal Access Portal.

Each request must include:

- Employee name and role
- System(s) being requested
- Business justification for access
- Duration of access (temporary or ongoing)

Incomplete requests will be automatically rejected.

3.3 Approval Workflow

Access requests follow this approval sequence:

1. Direct manager approval
2. System owner approval
3. Security Team approval

Access is granted only after **all three approvals** are completed.

3.4 Access Provisioning

Once approved, access is provisioned within **two business days**.

All granted access is logged and associated with:

- Employee ID
- Timestamp of approval
- Expiration date (if applicable)

---

4. Access Review & Revocation

4.1 Quarterly Access Reviews

The Security Team conducts quarterly access reviews to ensure all access remains appropriate.

Managers are responsible for confirming whether their team members still require access.

4.2 Immediate Revocation Events

Access must be revoked immediately under the following circumstances:

- Employee termination
- Role change that no longer requires access
- Detection of unauthorized or suspicious activity

Revocation must occur within **24 hours** of the triggering event.

---

5. Incident Response Procedure

5.1 Incident Identification

An incident may be identified through:

- Automated security alerts
- Employee reports
- Third-party notifications

All suspected incidents must be reported to the Security Team **immediately**.

5.2 Incident Classification

Incidents are classified into three severity levels:

- **Low:** No sensitive data involved; minimal impact
- **Medium:** Limited exposure of sensitive data
- **High:** Significant data exposure or system compromise

Severity classification is determined by the Security Team.

5.3 Incident Response Steps

For **all incidents**, the following steps must be followed:

1. Contain the incident to prevent further damage
2. Preserve logs and evidence
3. Assess scope and impact
4. Notify relevant stakeholders
5. Remediate root cause

For **High severity incidents**, executive leadership must be notified within **2 hours**.

5.4 Post-Incident Review

A post-incident review must be conducted within **5 business days** of incident resolution.

The review must document:

- Timeline of events
- Root cause analysis
- Corrective actions taken
- Preventative measures

---

6. Non-Compliance

Failure to comply with this SOP may result in disciplinary action, up to and including termination of employment.

Exceptions to this SOP require written approval from the Head of Platform Security.

---

7. Document Control

- This SOP is reviewed annually.
- Changes must be approved by the Security Team.
- The latest version is published in the Internal Policy Repository.