IT Standard Operating Procedures (SOP)

Document Title: IT SOP – Enterprise Service Desk & Operations

Company: Asterion Digital Services Pvt. Ltd.

Effective Date: 01 Jan 2025

Document Owner: Head – IT Operations

Applies To: All employees, contractors, and third-party vendors accessing company IT systems

---

1. Purpose and Scope

This document defines the standard operating procedures governing IT service delivery, infrastructure operations, access management, incident response, and change management at Asterion Digital Services Pvt. Ltd. The objective is to ensure system availability, data security, regulatory compliance, and predictable service levels across all business units.

This SOP applies to: - Corporate IT systems - Cloud platforms (AWS, Azure) - Data platforms (Databricks, Snowflake, PostgreSQL) - End-user computing devices - Network and security infrastructure

---

2. IT Service Desk Overview

2.1 Service Desk Operating Model

The IT Service Desk operates on a **follow-the-sun model** with primary support based in India.

Support Hours: - Business Days: 8:00 AM – 8:00 PM IST - Emergency Support (P1): 24x7 on-call

Channels Supported: - ServiceNow Portal (primary) - Email: it-support@asterion.com - Microsoft Teams – #it-helpdesk

All requests must be logged in ServiceNow to be officially tracked.

---

3. Incident Management

3.1 Incident Classification

Priority	Description	Example	Target Resolution
P1	Critical business outage	VPN down, PROD data pipeline failure	4 hours
P2	Major degradation	Databricks login failure	8 hours
P3	Minor issue	Outlook sync issue	2 business days
P4	Request / inquiry	Software install	3 business days

3.2 Incident Workflow

1. Incident logged in ServiceNow
2. Auto-assignment to L1 support
3. Escalation to L2 / L3 if unresolved
4. Root Cause Analysis (RCA) for P1/P2
5. Closure with user confirmation

---

4. Request Fulfillment

4.1 Access Requests

All access requests must include: - Business justification - Manager approval - Data Owner approval (for sensitive systems)

Default Access (Day 1): - Email, Teams, VPN - Jira (read-only) - Confluence

Additional Access Examples: - Databricks: Platform Team approval - Snowflake PROD: Data Governance approval

Standard SLA: 1–2 business days after approval

---

5. Identity & Access Management (IAM)

5.1 User Lifecycle

• Joiner: Access provisioned on DOJ
• Mover: Access modified within 1 business day
• Leaver: Access revoked within 2 hours of HR notification

5.2 Privileged Access

- Admin access is time-bound
- Requires CAB approval
- Logged and audited monthly

---

6. Change Management

6.1 Change Types

Change Type	Description	Approval
Standard	Low risk, repeatable	Pre-approved
Normal	Planned changes	CAB
Emergency	Urgent PROD fix	CIO + CAB post-review

6.2 Change Window

- Non-PROD: Anytime
- PROD: Sat 10 PM – Sun 6 AM IST

---

7. Release & Deployment

7.1 Environment Segregation

- DEV → QA → UAT → PROD
- Direct PROD deployments are prohibited

7.2 Approval Matrix

- QA Sign-off: QA Lead
- Business Sign-off: Product Owner
- PROD Deploy: IT Ops Lead

---

8. Data Platform Operations

8.1 Databricks

- Cluster cost monitored daily
- Auto-termination after 30 mins idle
- PROD jobs deployed via CI/CD only

8.2 Snowflake

- Role-based access control
- Time Travel enabled for 7 days
- Data retention per compliance policy

---

9. Backup & Disaster Recovery

9.1 Backup Policy

System	Frequency	Retention
Databases	Daily	30 days
File Servers	Daily	60 days

9.2 DR Testing

- Conducted twice annually
- RTO: 4 hours
- RPO: 30 minutes

---

10. Security Operations

10.1 Endpoint Security

- Antivirus mandatory
- Disk encryption required
- USB ports restricted

10.2 Incident Response

- Security incidents reported within 30 minutes
- IR team activated immediately
- Legal & Compliance notified for PII breaches

---

11. Vendor & Third-Party Access

- Time-bound access only
- NDA mandatory
- Activity logging enabled

---

12. Audit & Compliance

- ISO 27001
- SOC 2 Type II
- GDPR compliance for EU clients

Audit logs retained for 1 year minimum.

---

13. SOP Violations

Failure to follow SOPs may result in: - Access revocation - Disciplinary action - Termination (in severe cases)

---

14. Review & Updates

This SOP is reviewed annually or upon major system changes.

Last Reviewed: Dec 2024

---

15. Appendix – Common Scenarios

- Lost laptop → Incident + InfoSec notification
- Accidental PROD change → Emergency CAB
- Data leak suspicion → Security IR process

End of Document