IT Standard Operating Procedure

Department: Information Technology | Version: [1.0]

Document ID: [SOP-DEPT-###] | Effective Date: [MM/DD/YYYY]

1. Purpose

This Standard Operating Procedure establishes guidelines for IT operations to ensure system reliability, security, and efficient service delivery in accordance with industry best practices and organizational requirements.

2. Scope

This procedure applies to all IT personnel, system administrators, developers, and support staff responsible for maintaining and supporting technology infrastructure.

This procedure applies to:

- IT operations and support staff
- System and network administrators
- Application developers and DevOps engineers
- Security and compliance personnel
- Help desk and service desk teams

Exclusions:

[Describe any activities, processes, or personnel NOT covered by this SOP]

3. Definitions

The following terms have specific meanings within this procedure. Defined terms are capitalized when used throughout this document.

Term	Definition
CAB	Change Advisory Board - change approval authority

© 2026 LawAgreements.com. All rights reserved.

MTBF	Mean Time Between Failures - reliability measurement
MTTR	Mean Time to Repair - average recovery time from failures
RPO	Recovery Point Objective - maximum acceptable data loss
RTO	Recovery Time Objective - maximum acceptable downtime
SLA	Service Level Agreement - defined service delivery standards

4. Responsibilities

The following roles and positions have specific responsibilities for this procedure:

Role/Position	**Responsibilities**
[IT Director/CIO]	Will provide strategic direction and approve major changes and policies
[IT Manager]	Will oversee daily operations and ensure service level targets are met
[System Administrator]	Will maintain systems, perform updates, and respond to incidents
[Network Administrator]	Will manage network infrastructure and connectivity
[Security Analyst]	Will monitor security events and enforce security policies
[Help Desk Staff]	Will provide first-line support and ticket management

5. General IT Procedures

5.1 Change Management

All changes to production systems must follow the change management process:

© 2026 LawAgreements.com. All rights reserved.

1. Submit change request through ticketing system with full documentation
2. Assess impact, risk level, and required resources
3. Obtain appropriate approvals based on change type (standard, normal, emergency)
4. Schedule change window with notification to affected stakeholders
5. Implement change with documented rollback plan ready
6. Verify change success through testing and monitoring
7. Document results and close ticket with resolution details

5.2 Incident Management

1. Log incident in ticketing system immediately upon detection or report
2. Classify severity using the Incident Severity Matrix and assign priority
3. Perform initial diagnosis and triage to identify affected services
4. Escalate if beyond support tier capability or if SLA breach is imminent
5. Implement workaround to restore service, then permanent fix if different
6. Document resolution details including root cause and preventive measures
7. Conduct post-incident review for P1/P2 incidents within 5 business days

5.3 Security Protocols

The following security requirements apply to all IT systems and personnel:

- ☐ Multi-factor authentication enabled for all privileged access
- ☐ Passwords meet complexity requirements (12+ chars, mixed case, numbers, symbols)
- ☐ Access reviews conducted quarterly for all systems
- ☐ Security patches applied within 30 days (critical patches within 72 hours)
- ☐ Data encryption required for sensitive information at rest and in transit
- ☐ Security awareness training completed annually by all staff

6. Incident Severity Matrix

Use the following matrix to classify incident severity and determine response requirements:

Severity	Description	Response Time	Resolution Target	Escalation
P1 - Critical	Complete system outage affecting all users, major security breach,	15 minutes	4 hours	Immediate to IT Director

© 2026 LawAgreements.com. All rights reserved.

	data loss			
P2 - High	Major feature unavailable, significant performance degradation, security concern	30 minutes	8 hours	1 hour to IT Manager
P3 - Medium	Minor feature issue, single user affected, workaround available	2 hours	24 hours	4 hours if unresolved
P4 - Low	Cosmetic issue, enhancement request, informational inquiry	8 hours	5 business days	As needed

WARNING: P1 incidents require 24/7 response. On-call personnel must acknowledge within 15 minutes.

7. Service Level Agreement Definitions

7.1 Availability Targets by Service Tier

Service Tier	Uptime Target	Max Monthly Downtime	Maintenance Window	Support Hours
Tier 1 - Business Critical	99.99%	4.3 minutes	Scheduled only, off-hours	24/7/365
Tier 2 - Important	99.9%	43.8 minutes	Weekends preferred	Business hours + on-call
Tier 3 - Standard	99.5%	3.6 hours	As scheduled with notice	Business hours
Tier 4 - Dev/Test	Best effort	N/A	As needed	Business hours

© 2026 LawAgreements.com. All rights reserved.

7.2 Response Time Matrix

Response times based on service tier and incident priority:

	P1	P2	P3	P4
Tier 1	15 min	30 min	2 hrs	8 hrs
Tier 2	30 min	1 hr	4 hrs	24 hrs
Tier 3	1 hr	2 hrs	8 hrs	48 hrs
Tier 4	4 hrs	8 hrs	24 hrs	5 days

8. Disaster Recovery Checklist

In the event of a disaster affecting IT systems, execute the following phases:

8.1 Immediate Response (0-4 hours)

- ☐ Assess nature and scope of disaster (type, affected systems, estimated duration)
- ☐ Activate disaster recovery team and establish command center
- ☐ Notify IT Director, management, and key stakeholders
- ☐ Determine if DR site activation is required based on RTO/RPO
- ☐ Begin damage assessment and documentation
- ☐ Initiate communication plan to inform affected users

8.2 Recovery Phase (4-24 hours)

- ☐ Activate backup systems at DR site if required
- ☐ Restore data from most recent verified backup
- ☐ Verify data integrity through checksums and spot checks
- ☐ Test critical business functions with business unit leads
- ☐ Document recovery progress and any issues encountered
- ☐ Provide regular status updates to stakeholders (every 2-4 hours)

8.3 Restoration Phase (24+ hours)

- ☐ Plan controlled return to primary systems when safe
- ☐ Synchronize data between DR and primary sites
- ☐ Perform controlled failback with rollback plan ready
- ☐ Verify all systems operational and performance acceptable
- ☐ Conduct post-incident review within 5 business days
- ☐ Update disaster recovery procedures based on lessons learned

© 2026 LawAgreements.com. All rights reserved.

8.4 Emergency Contacts

Role	Name	Phone	Email
DR Coordinator	[Name]	[Phone]	[Email]
IT Director	[Name]	[Phone]	[Email]
Network Lead	[Name]	[Phone]	[Email]
Database Admin	[Name]	[Phone]	[Email]
Cloud Provider Support	[Vendor Name]	[Support Line]	[Support Email]

9. Access Control Audit Log

Document all access control reviews, changes, and audits:

Date	System/ Application	User(s) Affected	Change Type	Approved By	Verified By

9.1 Quarterly Access Review Checklist

Complete this checklist during quarterly access reviews:

Item	Completed	Notes
All active user accounts reviewed for continued necessity	☐	
Privileged/admin access verified and documented with business justification	☐	

© 2026 LawAgreements.com. All rights reserved.

Terminated employee access confirmed removed within 24 hours of departure	☐	
Service and system accounts reviewed, documented, and password rotated	☐	
External/vendor access validated and limited to minimum necessary	☐	
Dormant accounts (90+ days inactive) identified and disabled	☐	
Access review reports generated, signed, and filed for audit	☐	

10. Emergency and Exception Procedures

10.1 Emergency Response

In case of emergency, follow the procedures below. Safety of personnel takes priority over all other considerations.

1. **1.** Ensure immediate safety of all personnel in the area
2. **2.** Contact emergency services if required (911 or local emergency number)
3. **3.** Notify supervisor/manager immediately
4. **4.** Follow facility emergency evacuation procedures if applicable
5. **5.** Document the incident using the Incident Report form

10.2 Exception Handling

When standard procedures cannot be followed due to unusual circumstances:

1. **1.** Assess the situation and identify the specific deviation required
2. **2.** Obtain verbal approval from [Supervisor/Manager] before proceeding
3. **3.** Document the exception, including justification and approver
4. **4.** Complete the Exception Request Form within 24 hours
5. **5.** Submit for formal review during the next scheduled procedure review

© 2026 LawAgreements.com. All rights reserved.

WARNING: Exceptions should only be made when necessary and must be properly documented. Repeated exceptions may indicate the need for procedure revision.

11. Related Information

The following documents and references relate to this procedure:

Category	Reference
Related Policies	Information Security Policy, Acceptable Use Policy, Data Classification Policy
Related SOPs/Procedures	SOP-IT-002 Change Management, SOP-IT-003 Incident Response, SOP-IT-004 Backup and Recovery
Related Forms	Change Request Form, Incident Report Form, Access Request Form, DR Test Results Form
External References	ISO 27001 Information Security, NIST Cybersecurity Framework, SOC 2 Type II Requirements

12. Document Control

SOP Owner	[IT Operations Manager]
Approved By	[Chief Information Officer / IT Director]
Contact Email	[it-operations@company.com]
Contact Phone	[(XXX) XXX-XXXX]
Review Schedule	Annual or upon significant infrastructure changes, security incidents, or regulatory updates

13. Revision History

Document all revisions to maintain a complete audit trail:

Version	Date	Changes
1.0	[MM/DD/YYYY]	Initial release

© 2026 LawAgreements.com. All rights reserved.

14. Authorization and Approval

Name	Role	Signature	Date
	Prepared By		
	Reviewed By		
	Approved By		

15. Documentation of Training

I have read and understand the content of this Standard Operating Procedure. I have received training specific to the procedures, hazards, and emergency protocols described herein.

Note: All personnel who will perform tasks covered by this SOP must sign below prior to conducting any work. Additional signature pages may be attached as needed.

Printed Name	Signature	Date
[Manager/Supervisor]		

DISCLAIMER

© 2026 LawAgreements.com. All rights reserved.

This Standard Operating Procedure template is provided by LawAgreements.com for general informational and organizational purposes only. It does not constitute legal, professional, or compliance advice.

Organizations should customize this template to reflect their specific operational requirements, industry regulations, and applicable laws. LawAgreements.com recommends consulting with qualified legal, safety, or industry professionals before implementing any procedures in regulated environments.

By using this template, you acknowledge that LawAgreements.com is not liable for any outcomes resulting from its use or modification.

© 2026 LawAgreements.com. All rights reserved.