**🖥️ IT Support & Troubleshooting Playbook**

**Table of Contents**

1. Introduction to IT Support
2. IT Support Team Roles & Responsibilities
3. Hardware Issues & Solutions
4. Software Issues & Solutions
5. Network & Connectivity Troubleshooting
6. Security & Compliance Guidelines
7. Ticketing System & Workflow
8. Escalation Matrix & SLAs
9. Remote Support Best Practices
10. IT Documentation & Knowledge Base
11. Reporting & Metrics
12. FAQs & Troubleshooting
13. Appendices (Checklists, Templates, Tools)

**1. Introduction to IT Support**

IT support is a crucial backbone for organizational productivity. It ensures employees have reliable access to technology and can resolve issues quickly, minimizing downtime.

**1.1 Purpose of this Playbook**

This playbook provides:

* Step-by-step troubleshooting guidelines.
* Standard operating procedures (SOPs) for IT incidents.
* Escalation protocols and service-level expectations.

**1.2 Scope**

Covers all aspects of IT support including:

* Hardware, software, and network troubleshooting.
* Security incident management.
* Employee support workflows and reporting.

**1.3 IT Support Goals**

* Resolve issues efficiently and accurately.
* Maintain system uptime and business continuity.
* Ensure data security and compliance with policies.

**2. IT Support Team Roles & Responsibilities**

**2.1 IT Manager**

* Oversees all IT operations.
* Defines support strategies and monitors KPIs.
* Coordinates with other departments on IT projects.

**2.2 Support Technicians**

* Provide first-level support to employees.
* Diagnose and resolve hardware, software, and network issues.
* Escalate complex issues to senior IT staff.

**2.3 System Administrators**

* Manage servers, networks, and cloud infrastructure.
* Handle security updates, backups, and access control.
* Perform regular maintenance and system monitoring.

**2.4 Security Officers**

* Monitor and enforce security policies.
* Respond to cybersecurity incidents.
* Train employees on secure practices.

**3. Hardware Issues & Solutions**

**3.1 Common Hardware Problems**

* Laptop/desktop won’t start.
* Peripheral device failure (printer, keyboard, mouse).
* Monitor/display issues.
* Battery or charging problems.

**3.2 Troubleshooting Steps**

1. Check power connections and battery.
2. Verify external devices are connected correctly.
3. Restart the system and check for error messages.
4. Test with alternate devices to isolate the issue.

**3.3 Replacement & Repair**

* Determine if the hardware is under warranty.
* Log a repair ticket with serial numbers and issue description.
* Follow company procedures for loaner equipment if needed.

**4. Software Issues & Solutions**

**4.1 Common Software Problems**

* Application crashes or freezes.
* Software installation errors.
* License or activation issues.
* Compatibility conflicts with OS or other applications.

**4.2 Troubleshooting Steps**

1. Restart the application or system.
2. Check for updates or patches.
3. Verify system requirements and compatibility.
4. Clear cache, temporary files, or reset settings.
5. Reinstall software if necessary.

**4.3 Specialized Software Support**

* Provide SOPs for proprietary or role-specific tools.
* Maintain documentation for recurring issues and solutions.

**5. Network & Connectivity Troubleshooting**

**5.1 Common Network Problems**

* No internet connection.
* Slow network performance.
* VPN connection failure.
* Wi-Fi connectivity issues.

**5.2 Troubleshooting Steps**

1. Verify device connectivity (Wi-Fi, LAN cable).
2. Check router, modem, or network status lights.
3. Ping network resources to test connectivity.
4. Restart networking devices if needed.
5. Verify VPN credentials and configurations.

**5.3 Advanced Troubleshooting**

* Use network diagnostic tools (tracert, ipconfig, nslookup).
* Escalate persistent issues to network administrators.
* Document recurring issues for proactive monitoring.

**6. Security & Compliance Guidelines**

**6.1 IT Security Policies**

* Password management and rotation.
* Multi-factor authentication (MFA) requirements.
* Acceptable use policy for devices and applications.

**6.2 Threat Detection & Response**

* Antivirus and malware monitoring.
* Phishing and suspicious email reporting.
* Logging and monitoring unauthorized access attempts.

**6.3 Data Protection**

* Secure storage and encryption of sensitive data.
* Regular backups and disaster recovery protocols.
* Compliance with GDPR, HIPAA, or other relevant regulations.

**7. Ticketing System & Workflow**

**7.1 Ticketing Process**

1. Employee submits a ticket via IT service portal or email.
2. IT support reviews and categorizes the ticket.
3. Assign priority level based on impact and urgency.
4. Provide resolution or escalate if required.

**7.2 Ticket Prioritization**

| **Priority** | **Description** | **Response Time** | **Resolution Time** |
| --- | --- | --- | --- |
| P1 | Critical system failure | 30 min | 4 hours |
| P2 | Major disruption | 1 hour | 8 hours |
| P3 | Minor issue | 4 hours | 24 hours |
| P4 | Low priority/Request | 24 hours | 3 days |

**7.3 Ticket Closure**

* Ensure the issue is resolved and employee confirms.
* Document solution in knowledge base.
* Update ticket status and categorize for reporting.

**8. Escalation Matrix & SLAs**

**8.1 Escalation Levels**

* **Level 1:** First-line support, basic troubleshooting.
* **Level 2:** Senior technicians for advanced issues.
* **Level 3:** System administrators or vendors for critical incidents.

**8.2 Escalation Procedure**

1. Initial assessment and troubleshooting.
2. Escalate to next level if issue exceeds resolution scope or SLA time.
3. Notify employee and update ticket progress.

**8.3 Service-Level Agreements (SLAs)**

* Define maximum response and resolution times per priority.
* Track SLA compliance via reporting dashboards.

**9. Remote Support Best Practices**

**9.1 Tools for Remote Support**

* Remote desktop applications (TeamViewer, AnyDesk, Zoom).
* VPN access and secure network connections.

**9.2 Guidelines**

* Verify employee identity before accessing systems.
* Log all remote sessions for auditing purposes.
* Ensure data confidentiality during support.

**9.3 Common Remote Fixes**

* Software updates and configuration changes.
* Network and VPN troubleshooting.
* Password resets and account management.

**10. IT Documentation & Knowledge Base**

**10.1 Importance of Documentation**

* Provides a central reference for recurring issues.
* Reduces time to resolution.
* Ensures knowledge transfer among IT team members.

**10.2 Knowledge Base Content**

* Troubleshooting guides.
* SOPs for software and hardware.
* Security alerts and mitigation instructions.

**10.3 Maintaining the Knowledge Base**

* Regularly update articles.
* Add lessons learned from incident resolution.
* Use search-friendly categories and tagging.

**11. Reporting & Metrics**

**11.1 IT Performance Metrics**

* Ticket volume and resolution time.
* SLA compliance percentage.
* First-contact resolution rate.
* Employee satisfaction scores.

**11.2 Reporting Frequency**

* Weekly, monthly, and quarterly reports.
* Include analysis, trends, and recommendations.

**11.3 Continuous Improvement**

* Identify recurring issues and implement preventive measures.
* Conduct periodic audits of IT systems and support processes.

**12. FAQs & Troubleshooting**

**12.1 Common Questions**

* How do I reset my password?
* What do I do if my laptop won’t start?
* How do I connect to the VPN remotely?

**12.2 Problem Resolution**

* Step-by-step troubleshooting guides for common issues.
* Escalation procedure if self-help solutions fail.
* Contact information for IT support and emergencies.

**13. Appendices (Checklists, Templates, Tools)**

**13.1 IT Onboarding Checklist**

| **Task** | **Responsible** | **Deadline** | **Status** |
| --- | --- | --- | --- |
| Setup email & accounts | IT | Day 1 | Pending |
| Install required software | Employee/IT | Day 2 | Pending |
| Configure VPN access | IT | Day 2 | Pending |
| System orientation | IT | Week 1 | Pending |

**13.2 Incident Report Template**

**Issue Description:**  
**Device/Software Affected:**  
**Steps Taken:**  
**Resolution:**  
**Escalation Level:**  
**Date & Time Resolved:**

**13.3 SLA Matrix Example**

| **Priority** | **Max Response Time** | **Max Resolution Time** |
| --- | --- | --- |
| P1 | 30 min | 4 hours |
| P2 | 1 hour | 8 hours |
| P3 | 4 hours | 24 hours |
| P4 | 24 hours | 3 days |

**13.4 Remote Support Guidelines**

* Always verify employee credentials.
* Log session start and end times.
* Confirm resolution before closing ticket.