IT Helpdesk Knowledge Base

Week 1 Analysis & Procedures

Generated: September 19, 2025

Based on Comprehensive Ticket Analysis

Table of Contents

1. Executive Summary

Week 1 of the IT Helpdesk operation demonstrated exceptional performance with a 100% resolution rate. All 13 tickets were resolved within the same business day, with no escalations required. The team successfully handled various incident types, with password-related issues being the most common. This knowledge base captures the patterns, procedures, and best practices established during the first week.

Key Achievements:

- ✓ 100% ticket resolution rate achieved
- ✓ All tickets resolved same day
- ✓ Zero escalations required
- ✓ 6 knowledge base articles created
- ✓ 5 prevention strategies identified
- ✓ Perfect agent performance across all team members

2. Incident Patterns Analysis

Incident Type	Frequency	Priority	Resolution Time
Password Reset Requests	4 tickets	Medium	Same Day
Account Lockouts	3 tickets	Medium	Same Day
Recurring Lockouts	1 ticket	Medium	Same Day
Account Disabled	2 tickets	Medium	Same Day
Outlook Authentication	1 ticket	Low	Same Day
MFA Device Issues	1 ticket	High	Same Day
Password Expiration	1 ticket	Medium	Same Day
Temporary Access	1 ticket	Low	Same Day
Security Incidents	1 ticket	High	Same Day

Key Insights:

- Password-related issues account for 54% of all tickets (7 out of 13)
- Medium priority tickets are most common (77% of total)
- All incidents resolved within same business day
- No recurring issues or unresolved tickets
- Security incidents require immediate attention (High priority)

3. Solution Playbook

Standardized procedures for resolving common IT helpdesk issues. Each procedure follows a 5-step process to ensure consistent and effective resolution.

3.1 Password Reset Procedure

1. Verify user identity through company app/phone system
2. Access Active Directory Users and Computers (ADUC)
3. Locate user account: @username
4. Reset password using 'Reset Password' function
5. Set temporary password with complexity requirements

KB Article: KB_Password_Reset

3.2 Account Unlock Procedure

1. Check Active Directory for account lockout status
2. Verify lockout was due to failed login attempts
3. Use ADUC to unlock user account
4. Reset failed login counter to zero
5. Verify account is now accessible

KB Article: KB_Password_Reset

3.3 Recurring Lockout Resolution

1. Analyze lockout source using LockoutStatus.exe tool
2. Identify multiple lockout sources across domain controllers
3. Check for cached credentials on user devices
4. Clear all cached credentials from devices
5. Reset user password to clear cached bad passwords

KB Article: KB_Password_Reset

4. Agent Performance Analysis

Agent Name	Total Tickets	High Priority	Medium Priority	Low Priority	Resolution Rate
Azola Xabadiya	4 tickets	1	3	0	100%
Keawin Koesnel	6 tickets	1	4	1	100%
System Admin	3 tickets	0	3	0	100%

Performance Highlights:

- All agents achieved 100% resolution rate
- Keawin Koesnel handled the most tickets (6)
- Azola Xabadiya and Keawin Koesnel handled high-priority security incidents
- System Admin focused on standard password and account issues
- No performance issues or training needs identified

5. Common Issues & Solutions

5.1 User forgot password

Symptoms: Cannot log in, password not working

Solution: Reset password via ADUC, provide temporary password

Prevention: Send password expiration reminders

5.2 Account locked after failed attempts

Symptoms: Account locked message, cannot access systems

Solution: Unlock account in ADUC, reset failed login counter

Prevention: Educate users on correct password entry

5.3 Recurring account lockouts

Symptoms: Account locks repeatedly even with correct password

Solution: Clear cached credentials from all devices

Prevention: Regular credential cache maintenance

5.4 Account disabled unexpectedly

Symptoms: Login denied, account may be disabled

Solution: Re-enable account if authorized, document reason

Prevention: Review account disablement policies

5.5 Outlook authentication prompts

Symptoms: Outlook keeps asking for password

Solution: Clear credential cache, reset Office 365 password

Prevention: Regular Office 365 credential refresh

6. Escalation Procedures

Guidelines for when and how to escalate issues beyond the helpdesk team. Proper escalation ensures timely resolution of complex or high-impact incidents.

Issue Type	When to Escalate	Level 1	Level 2
High Priority Security	Immediate	IT Security Team	CISO
Recurring Lockouts	After 2 failed attempts	Senior IT Support	IT Director
Multiple User Issues	More than 5 users affected	IT Manager	IT Director
System-wide Problems	Authentication system down	System Administrator	IT Director
Access Violations	Unauthorized access attempts	IT Security Team	CISO

Documentation Required for Escalation:

- Security incident report and log files
- Resolution attempts and user impact assessment
- User list and affected systems
- System status and error logs
- Access logs and authorization documents

7. Week 1 Performance Summary

Metric	Value	Notes
Total Tickets Handled	13 tickets	All tickets from Week 1 successfully processed
Tickets Resolved	13 tickets	No outstanding or unresolved tickets
Resolution Rate	100%	Perfect resolution rate achieved
Average Resolution Time	Same Day	All tickets resolved within same business day
Most Common Issue Type	Password Reset (4 tickets)	Password-related issues most frequent
Highest Priority Issues	2 High Priority tickets	MFA device lost and security incidents
Agent Performance Rating	Excellent (100% resolution rate)	All agents performed exceptionally well
User Satisfaction	High	Users received prompt and effective support
Knowledge Base Articles	6 KB articles	Comprehensive knowledge base established
Process Improvements	5 prevention strategies	Proactive measures identified for common issues

Key Success Factors:

- Standardized procedures for common issues
- Quick response time and same-day resolution
- Comprehensive documentation and knowledge sharing
- Effective agent training and performance
- Proactive identification of prevention strategies

8. Recommendations & Next Steps

8.1 Immediate Actions (Week 2)

- Implement password expiration reminder system
- Create user education materials for password management
- Set up automated credential cache cleanup schedule
- Review and update account disablement policies
- Establish regular Office 365 credential refresh procedures

8.2 Medium-term Improvements (Month 1)

- Develop self-service password reset portal
- Implement automated account lockout monitoring
- Create user training program for common issues
- Establish regular knowledge base review process
- Set up performance metrics dashboard

8.3 Long-term Strategic Goals (Quarter 1)

- Reduce ticket volume through prevention strategies
- Implement advanced security monitoring and alerting
- Develop predictive analytics for common issues
- Create comprehensive user self-service portal
- Establish IT service management best practices

--- End of Week 1 Knowledge Base ---

Generated on September 19, 2025 at 11:20 AM