IT Helpdesk Ticketing and Incident Escalation SOP

Purpose

To establish a standardized and efficient process for the intake, triage, troubleshooting, escalation, and resolution of IT issues. This SOP applies to all staff, contractors, and interns, and covers support delivered through the internal ticketing system.

1. Priority Matrix
2. Once received, prioritize the ticket based on the following urgency vs. impact matrix:

|  |  |  |
| --- | --- | --- |
| **Priority Level** | **Definition** | **Examples** |
| P1 – Critical | High impact + high urgency, system-wide failure, executive-level issue, or security breach | Director locked out, malware/virus outbreak, server failure, critical data loss |
| P2 – High | High impact + low urgency or moderate impact + high urgency | Shared printer down, hardware damage for key staff, staff account lockout |
| P3 – Medium | Moderate impact + moderate/low urgency, affects individual productivity but work continues | Slow computer, missing files, routine login problems |
| P4 – Low | Low impact + low urgency, routine, cosmetic, or assistive requests | Phone setup, label printing, general IT inquiries |

NOTE: Directors’ issues are automatically P1 unless otherwise noted.

1. Escalation Triggers

Escalate a ticket when:

* Issue exceeds target resolution time

|  |  |
| --- | --- |
| P1 | Four business hours |
| P2 | One business day |
| P3 | Two business days |
| P4 | Three business days |

* Affects multiple users, systems, or departments
* Involves security, data, or compliance risk
* Vendor support is required
* User or supervisor requests escalation
* Issue is recurring or reappears after previous fixes

1. Troubleshooting and Tiered Escalation

**Tier 1**

1. Identify initial response time:

|  |  |
| --- | --- |
| P1 | One business hour |
| P2 | Two business hours |
| P3 | Four business hours |
| P4 | Eight business hours |

1. Follow general troubleshooting protocols.
2. Use remote support via Quick Assist as appropriate.
3. Document all steps, time spent, and findings.
4. Resolve within 1 business day or escalate.

**Tier 2**

1. Use system logs, diagnostics, network tools, and remote access.
2. Assign to appropriate IT personnel with domain expertise.
3. Update ticket with detailed steps, findings, and daily progress.
4. Resolve within 2 business day or escalate.

**Tier 3**

1. Assign to IT Lead.
2. Evaluate cross-system dependencies or organizational impact.
3. Initiate Data Breaches SOP if sensitive data is involved.
4. Notify affected departments and stakeholders.
5. Coordinate with vendors or external support as necessary.
6. Remote Support Procedures
7. Initiate a session via Quick Assist.
8. Share code with the user and confirm permission before proceeding.
9. Maintain user privacy and avoid accessing personal or unrelated files.
10. Document the session in the support ticket.
11. Terminate session immediately after support is complete and confirm resolution.
12. Communication Protocols

* User updates: Notify end users within four business hours if resolution will be delayed.
* Major incidents: Must be communicated to leadership within one business day.
* Documentation: maintain contact logs, timestamps, and technician actions in ticketing system.

1. Resolution and Closure
2. Confirm resolution with requestor.
3. Update ticket with troubleshooting steps, final fix or workaround, root cause (if known), time spent, and any system or configuration changes.
4. Updated related asset management records, if applicable.
5. Close the ticket.

This SOP must be reviewed annually or upon major infrastructure or tool changes, a critical incident, or updated organization policies.