Customer Support Ticketing System – SLA Monitoring Enhancement

Functional Requirements Specification

Document Type: Functional Requirements
Project: Customer Support Ticketing System
Related Change Request: CR-SLA-001
Version: 1.0
Author: András Hunyor – Business Analyst (Operations / IT Focus)
Date: [aktuális dátum]

---

1. Purpose of Document

This document defines the functional requirements for the SLA Monitoring Enhancement described in Change Request CR-SLA-001.
The scope is limited to system-level changes required to support SLA visibility, alerting, and breach tracking.

---

2. In-Scope Functionality Overview

The following functional areas are covered:

- SLA time tracking per ticket
- SLA status visualization
- SLA warning and breach alerts
- SLA breach logging for reporting

---

3. Functional Requirements

FR-01: SLA Time Tracking per Ticket

Description:
The system shall calculate and track SLA time for each active ticket based on the applicable SLA definition.

Acceptance Criteria:

- SLA timer starts when the ticket enters an active state
- SLA timer pauses when the ticket is in a waiting or on-hold state

- SLA timer stops when the ticket is resolved or closed

FR-02: SLA Status Visualization

Description:
The system shall display the current SLA status for each ticket using visual indicators.

Business Rules:

- Green: SLA time remaining > warning threshold
- Amber: SLA time remaining ≤ warning threshold
- Red: SLA breached

Acceptance Criteria:

- SLA status is visible to agents at ticket level
- SLA status is visible to managers at queue level

FR-03: Pre-Breach SLA Alerts

Description:
The system shall generate automated alerts when a ticket reaches the defined SLA warning threshold.

Acceptance Criteria:

- Alert is triggered when SLA remaining time falls below the configured threshold
- Alert is sent to the assigned agent and relevant team lead
- Alert frequency is configurable to prevent duplication

FR-04: SLA Breach Notification

Description:
The system shall generate an alert when an SLA breach occurs.

Acceptance Criteria:

- SLA breach alert is generated immediately upon breach
- Alert includes ticket ID, SLA type, and breach timestamp
- Alert is logged for audit and reporting purposes

FR-05: SLA Breach Logging

Description:
The system shall record all SLA breaches for reporting and analysis.

Acceptance Criteria:

- SLA breach events are stored with timestamp and ticket reference
- Breach data is available for operational reporting
- Historical SLA breach data is retained according to system policy

---

4. Non-Functional Considerations (Out of Scope)

Non-functional requirements such as performance, security, and scalability are outside the scope of this document and are addressed separately.

---

5. Dependencies and Assumptions

Dependencies:

- Existing SLA definitions are available and maintained
- Notification service is operational

Assumptions:

- SLA thresholds are configurable at system level
- Users will receive training on new SLA indicators

---

6. Traceability

Requirement ID	Related CR
FR-01	CR-SLA-001
FR-02	CR-SLA-001
FR-03	CR-SLA-001
FR-04	CR-SLA-001
FR-05	CR-SLA-001

End of Document