项目文档

# Functional Requirement

ID Function Requirement  
LOG-001 Complaint Logging The system shall allow frontline complaint handling staff to log complaints via tablet or computer.  
LOG-002 Complaint Logging The system shall enforce mandatory fields for key complaint information, including contact details, complaint type, date/time, and affected account.  
LOG-003 Complaint Logging The system shall provide optional fields for additional context, such as a summary of the issue and immediate actions taken.  
LOG-004 Complaint Logging The system shall display a confirmation or summary screen before submitting a complaint for review.  
CLASS-001 Complaint Classification The system shall automatically classify complaints into high-risk or less urgent categories based on keywords, complaint type, and customer history.  
CLASS-002 Complaint Classification The system shall highlight the key phrases and criteria used in classification to build user trust and understanding.  
CLASS-003 Complaint Classification The system shall allow the officer to review and confirm the classification result.  
NOTIFY-001 Notification Management The system shall automatically notify relevant personnel (e.g., manager, specialist) when a complaint is flagged as high-risk.  
NOTIFY-002 Notification Management The system shall escalate unresolved complaints automatically after 24 hours.  
NOTIFY-003 Notification Management Notifications shall be delivered via dashboard alerts or direct messages to ensure urgency.  
ROUTE-001 Complaint Routing The system shall route complaints to the appropriate department or officer based on predefined categories, keywords, and location.  
ROUTE-002 Complaint Routing The system shall support load balancing to assign complaints based on current department workload.  
ROUTE-003 Complaint Routing The system shall prioritize routing for emergency or sensitive issues.  
ROUTE-004 Complaint Routing The system shall suggest alternative teams if the assigned department is overloaded.  
SUPP-001 Support and Suggestions The system shall provide smart suggestions for complaint type and department based on keywords entered by the user.  
SUPP-002 Support and Suggestions The system shall maintain an audit trail to track who accessed or modified a complaint record and when.  
SUPP-003 Support and Suggestions The system shall enable secure communication channels for correspondence with complainants.

# External Description

## 5.1 Regulatory/Legal Constraints  
  
- \*\*CST-REG-001:\*\* The system shall comply with all applicable data protection and privacy regulations, including but not limited to GDPR and local data governance laws.   
 \*Priority:\* Must Have   
 \*Rationale:\* Ensures legal compliance and protects the organization from potential legal liabilities.   
 \*Source:\* NFR-12 (Compliance)   
 \*Acceptance Criteria:\* All data processing and storage activities must be validated against current regulatory standards by an external audit.  
  
- \*\*CST-REG-002:\*\* The system shall maintain audit logs for a minimum of \*\*12 months\*\*, with the capability to extend the retention period based on internal or regulatory requirements.   
 \*Priority:\* Should Have   
 \*Rationale:\* Provides a legal and operational record for dispute resolution and compliance verification.   
 \*Source:\* NFR-11 (Audit Logs)   
 \*Acceptance Criteria:\* Audit logs shall be tested for retention, accessibility, and searchability across a 12-month period.  
  
## 5.2 Hardware Constraints  
  
- \*\*CST-HW-001:\*\* The system shall be compatible with \*\*Windows 10/11\*\*, \*\*macOS 12 or higher\*\*, and \*\*Android/iOS 12 or higher\*\* for tablet access.   
 \*Priority:\* Must Have   
 \*Rationale:\* Ensures accessibility across the primary devices used by frontline staff and complainants.   
 \*Source:\* 5.1 (Operating Environment)   
 \*Acceptance Criteria:\* Compatibility testing shall be conducted across all listed operating systems and devices before deployment.  
  
- \*\*CST-HW-002:\*\* The system shall be deployed on \*\*cloud infrastructure\*\* with \*\*auto-scaling capabilities\*\* to handle fluctuating complaint volumes.   
 \*Priority:\* Must Have   
 \*Rationale:\* Ensures the system can dynamically adjust to high or low complaint traffic without downtime or performance degradation.   
 \*Source:\* 5.1 (Operating Environment)   
 \*Acceptance Criteria:\* Cloud deployment shall be validated for auto-scaling functionality during load testing scenarios.  
  
## 5.3 Interface Constraints  
  
- \*\*CST-IF-001:\*\* The system shall integrate with \*\*existing enterprise systems\*\* (e.g., CRM, case management, internal messaging platforms) for data exchange and workflow coordination.   
 \*Priority:\* Must Have   
 \*Rationale:\* Facilitates seamless operation with the organization’s existing infrastructure, reducing manual effort and data silos.   
 \*Source:\* 5.1 (Operating Environment)   
 \*Acceptance Criteria:\* Integration points shall be defined, and each shall be verified with a working prototype or test case.  
  
- \*\*CST-IF-002:\*\* The system shall support \*\*HTTPS and TLS 1.3\*\* for secure communication between the user interface and backend services.   
 \*Priority:\* Must Have   
 \*Rationale:\* Ensures secure transmission of complaint data and prevents unauthorized interception.   
 \*Source:\* 5.2 (Network Setup)   
 \*Acceptance Criteria:\* Network traffic shall be analyzed to confirm that all communication is encrypted and compliant with TLS 1.3.  
  
## 5.4 Design and Implementation Constraints  
  
- \*\*CST-DI-001:\*\* The system shall implement \*\*role-based access controls\*\* to restrict unauthorized access to complaint records and features.   
 \*Priority:\* Must Have   
 \*Rationale:\* Maintains data integrity and ensures that only authorized personnel can perform actions based on their role.   
 \*Source:\* NFR-4 (Security)   
 \*Acceptance Criteria:\* Role-based access shall be verified by testing user permissions and access logs.  
  
- \*\*CST-DI-002:\*\* The system shall implement \*\*multi-factor authentication (MFA)\*\* for all user roles.   
 \*Priority:\* Must Have   
 \*Rationale:\* Prevents unauthorized access and enhances the overall security of the system.   
 \*Source:\* 5.4 (Security Requirements)   
 \*Acceptance Criteria:\* MFA shall be tested for all user types, ensuring it is enforced during login.  
  
- \*\*CST-DI-003:\*\* The system shall support \*\*regular security audits and penetration testing\*\* to identify and mitigate vulnerabilities.   
 \*Priority:\* Must Have   
 \*Rationale:\* Ensures the system remains secure over time and can adapt to emerging threats.   
 \*Source:\* 5.4 (Security Requirements)   
 \*Acceptance Criteria:\* A schedule for security audits and penetration testing shall be defined and followed for at least the first 6 months post-deployment.  
  
- \*\*CST-DI-004:\*\* The system shall be designed with a \*\*simple and intuitive user interface\*\* suitable for frontline staff with minimal training.   
 \*Priority:\* Must Have   
 \*Rationale:\* Reduces the learning curve and improves adoption and efficiency among users.   
 \*Source:\* NFR-7 (Usability)   
 \*Acceptance Criteria:\* Usability testing shall be conducted with 10 frontline staff members, with a success rate of at least 90% for core complaint logging and classification tasks.  
  
## 5.5 Other Constraints  
  
- \*\*CST-OT-001:\*\* The system shall not complicate the officer’s workflow; it shall \*\*support, not hinder, daily tasks\*\*.   
 \*Priority:\* Must Have   
 \*Rationale:\* Maintains productivity and reduces resistance to system adoption.   
 \*Source:\* NFR-8 (Usability)   
 \*Acceptance Criteria:\* A time-based efficiency test shall be conducted to ensure that complaint logging and processing take no more than 3 minutes per case.  
  
- \*\*CST-OT-002:\*\* The system shall \*\*automatically detect and alert on suspicious activity\*\*, such as multiple failed login attempts or unauthorized access attempts.   
 \*Priority:\* Must Have   
 \*Rationale:\* Enhances security and enables proactive response to potential threats.   
 \*Source:\* 5.4 (Security Requirements)   
 \*Acceptance Criteria:\* A test shall simulate 100 failed login attempts and verify that the system triggers alerts within 1 minute.  
  
---