PARADIN ENVIROTECH

Software Requirements Specification

# ShieldCert System - System Administration Module

Version: 1.0

Date: 2025-12-22

Status: Draft

https://www.securewithpaladin.com

# Table of Contents

# 1 Document Information

| Field | Value |
|---|---|
| Project Name | ShieldCert System - System Administration Module |
| Version | 1.0 |
| Date | 2025-12-22 |
| Project Manager | TBD |
| Tech Lead | TBD |
| Qa Lead | TBD |
| Platforms | ['Web'] |
| Document Status | Draft |
| Client | Paladin Envirotech |
| Document Code | SHIELDCERT-ADMIN-122025 |

# 2 Project Overview

## 2.1 What Are We Building

### 2.1.1 System Function

System administration platform providing user management, role-based access control, master data management, audit trail monitoring, and system configuration capabilities that support all operational modules with security, compliance, and administrative oversight.

### 2.1.2 Users

- System Administrators: Complete system management and configuration
- IT Managers: User access and security oversight
- Compliance Officers: Audit trail monitoring and reporting
- Operations Managers: Master data configuration and maintenance

### 2.1.3 Problem Solved

Provides centralized user management, ensures consistent access control across all modules, maintains configurable master data, enables comprehensive audit monitoring, and supports system-wide configuration management.

### 2.1.4 Key Success Metric

100% role-based access control enforcement, complete audit trail coverage, centralized master data management, and streamlined user administration.

## 2.2 Scope

### 2.2.1 In Scope

- User creation, management, and role assignment
- Role and permission management system
- Master data configuration for all dropdown lists
- Comprehensive audit trail monitoring and reporting

- Access control enforcement across all modules
- System configuration management

### 2.2.2 Out Of Scope

- Advanced analytics and business intelligence
- Integration with external identity providers
- Automated user provisioning from HR systems
- Advanced security monitoring and threat detection

# 3 User Requirements

## 3.1 User Management

| Feature Code | I Want To | So That I Can | Priority | Notes |
|---|---|---|---|---|
| FT-USER-MANAGE | Create, edit, and manage user accounts | Control system access and maintain user information | Must | Complete user lifecycle management with role assignment |
| FT-ROLE-MANAGE | Create and manage user roles with permissions | Define access levels and system capabilities | Must | Granular permission assignment and role-based access control |

## 3.2 Master Data

| Feature Code | I Want To | So That I Can | Priority | Notes |
|---|---|---|---|---|
| FT-MASTER-DATA | Manage all system master data and dropdown lists | Maintain consistent reference data across modules | Must | Centralized configuration for all system reference data |

## 3.3 Audit Monitoring

| Feature Code | I Want To | So That I Can | Priority | Notes |
|---|---|---|---|---|
| FT-AUDIT-TRAIL | View comprehensive audit trails for all system functions | Monitor system usage and ensure compliance | Must | Complete activity logging with user, action, and |

| Feature Code | I Want To | So That I Can | Priority | Notes |
|---|---|---|---|---|
| | | | | timestamp tracking |

# 4 Master Data Entities

- SOW Types
- Payment Terms
- Countries
- US States
- Currencies
- Product Types
- Manufacturers
- Sales Order Types
- Sales Channels
- Incoterms
- Shipment Methods
- Carriers
- Order Statuses (Inbound/Outbound)
- Services
- Packaging Types
- Grading Comments
- Container/Truck Types
- Truck Sizes

# 5 Data Model

## 5.1 Entities

### 5.1.1 User

#### 5.1.1.1 Description

System user accounts

#### 5.1.1.2 Key Fields

- user_id (Primary Key)
- username (Unique)
- email (Unique)
- first_name
- last_name
- status (Active/Inactive)
- created_date
- last_login_date
- password_hash
- failed_login_attempts

### 5.1.2 Role

#### 5.1.2.1 Description

User roles and permissions

#### 5.1.2.2 Key Fields

- role_id (Primary Key)
- role_name (Unique)
- description
- status (Active/Inactive)
- created_date

- created_by

### 5.1.3 Permission

#### 5.1.3.1 Description

System permissions

#### 5.1.3.2 Key Fields

- permission_id (Primary Key)
- permission_name
- module
- action (Create, Read, Update, Delete)
- description

### 5.1.4 Auditlog

#### 5.1.4.1 Description

System audit trail

#### 5.1.4.2 Key Fields

- audit_id (Primary Key)
- user_id (Foreign Key)
- module
- action
- entity_type
- entity_id
- old_values (JSON)
- new_values (JSON)
- timestamp
- ip_address
- user_agent

# 6 Business Rules

- Each user must have at least one role assigned
- Roles can have multiple permissions
- Users can have multiple roles
- All system actions must be logged in audit trail
- Master data changes reflected system-wide immediately
- User account lockout after failed login attempts
- Role-based access control enforced on all modules

# 7 Sign Off

## 7.1 Approval

| Role | Name | Signature | Date |
|---|---|---|---|
|  |  |  |  |

## 7.2 Document History

| Version | Date | Changes Made | Changed By |
|---|---|---|---|
| 1.0 | 2025-12-22 | Initial System Administration module SRS | SRS Development Team |