# SYSTEM SECURITY PLAN

1. **APPLICATION/SYSTEM IDENTIFICATION**

## Application/System Category

* + - Indicate whether the application/system is a Major Application or a General Support System.
    - A Major Application is "an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application."
    - A General Support System is an "interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people."

## Application/System Name/Title

* + - Application: SMART SALON APPLICATION
    - Desktop application

## Responsible Organization

* + - Organization responsible for the application/system: SSA company

## Information Contact(s)

-- Name: Minh Hoang Tran

-- Title: CEO

-- Address: 3\*\*\* Zephyr, Summerville, SC- 11111

-- Phone Number: 858 855 1255

-- Fax Number: 855-885-8588

-- E-mail Address: Minh@gmaill.com

## Assignment of Security Responsibility

Person(s) responsible for security of the application/system and an alternate emergency contact.

-- Name: Minh Hoang Tran

-- Title: CEO

-- Address: 3\*\*\* Zephyr, Summerville, SC- 11111

-- Phone Number: 858 855 1255

-- Fax Number: 855-885-8588

-- E-mail Address: Minh@gmaill.com

## Application/System Operational Status

-- Under Development

-- Undergoing a major modification

**A.7 General Description/Purpose**

The purpose of this application is to serve as a cost-free, secure, and user-friendly desktop management system for small salons such as hair salons, barbershops, and massage therapy studios. The application streamlines core business operations including appointment scheduling, technician/client management, and check-in functionalities.

**Information Processed:**

* Client information such as: Name, Email
* Appointment check-in book
* Hair service such as haircut, hair color, highlight, …
* Employee information such as names and email. Phone number, address, …

**Processing Flow:**

1. **Input:** Admin or workers input customer and service data via a secure login interface.
2. **Process:** The system validates and stores information and manages technician data.
3. **Output:** Information is displayed in the user interface (UI), printed as service tickets, or exported for reports.

**User Organizations:**

* **Internal:** Admin, technicians
* **External:** customers (indirectly, via check-in)

**A.8 Application/System Environment**

**Technical Description:** The application will be developed using Electron and Node.js, offering a cross-platform desktop experience. It will run on Windows and macOS systems and use local file-based storage initially (e.g., JSON, SQLite), with potential expansion to cloud storage.

**Security Concerns:**

* Use of open networks (e.g., Wi-Fi) in salons can introduce vulnerabilities.
* Devices used (tablets, desktops) may be shared among staff

**Primary Platforms:**

* Desktop (Windows/macOS) Electron framework
* Code written in JavaScript using VS Code

**Components:**

* **Frontend:** Electron UI components
* **Backend:** Node.js logic and local database
* **Security Software:** Password-protected login, access control layers, basic data encryption (Could use antivirus if needed)

**System Locations:**

* The application will be installed and operated locally by salon devices (desktop/laptop devices owned by the salon).

**A.9 Application/System Interconnection/Information Sharing**

**System Interconnections:**

* At the initial stage, the application will function as a **standalone desktop application** with no external system connections.
* If integrated with external systems (e.g., calendar tools, payment processors)

**Security Concerns:**

* If future updates involve syncing data to cloud or external platforms
* Password breach from internal network.

**Interconnection Rules:**

* Any system integration will require:
  + Written approval for shared access
  + Defined access roles and data use guidelines
  + End-to-end encryption of shared information

**A.10 Applicable Laws or Regulations Affecting the Application/System**

The following laws/regulations are applicable due to the handling of personally identifiable information (PII):

* General Data Protection Regulation (GDPR) (if used in the EU)
* California Consumer Privacy Act (CCPA) (if used in California)
* Children’s Online Privacy Protection Act (COPPA) (if customers under 13 are handled)
* State-level data breach notification laws
* Computer Fraud and Abuse Act (CFAA) – for unauthorized access protections
* Privacy Act of 1974 – applies if used by a U.S. federal agency (unlikely here but mentioned for context)

**A.11 Information Sensitivity and Criticality Assessment**

**Types of Information Handled:**

* Client names, contact details
* Staff work PII and service records
* Financial transaction records

**Protection Requirements:**

* **Confidentiality**  
  Sensitivity: High  
  Personal customer and financial data must be protected from unauthorized access. Access is limited by role (e.g., workers can't view other records).
* **Integrity**  
  Sensitivity: Medium to High  
  Data such as appointments and income tracking must not be altered without proper authorization to ensure business accuracy.
* **Availability**  
  Sensitivity: Medium  
  The application must be consistently available during business hours. Limited downtime is acceptable, but frequent outages can severely disrupt operations.

# APPLICATION/SYSTEM PROTECTION REQUIREMENTS CHART

|  |  |  |  |
| --- | --- | --- | --- |
| **Application/System Protection Requirements** | **High** | **Medium** | **Low** |
| Confidentiality |  |  |  |
| Integrity |  |  |  |
| Availability |  |  |  |

# DETAILED APPLICATION/SYSTEM PROTECTION REQUIREMENTS CHART

|  |  |  |  |
| --- | --- | --- | --- |
| **Information Type** | **Confidentiality (High, Medium or Low)** | **Integrity** | **Availability** |
| Administrative |  |  |  |
| Financial |  |  |  |
| Grant/Contract |  |  |  |
| Patient |  |  |  |
| Proprietary |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Research |  |  |  |
| Privacy Act |  |  |  |
| Other (specify) |  |  |  |

**B. MANAGEMENT CONTROLS**

**B.1 Risk Assessment and Management**

* **Methodology**: The risk assessment was performed using a qualitative analysis method, identifying threats and vulnerabilities.
* **Team**: Created by Minh Hoang Tran in 2024 - 2025.

**B.2 Review of Security Controls**

* There is no formal independent review that has been created yet.
* Planned: A peer security review and advisor evaluation are scheduled once development reaches the beta stage (June 2025).
* Any findings will be documented, and necessary updates will be implemented immediately.

**B.3 Rules of Behavior**

* Rules include:
  + Passwords must be strong and confidential.
  + Need to log-in before using the application
  + Only admins can access full customers and employee data.
  + Employees may only view appointment schedules and basic service details.
  + Unauthorized data sharing is strictly prohibited.
* Rules are provided during account setup and require user agreement (checkbox confirmation and electronic signature).
* See **Appendix A** for the full Rules of Behavior document.

**B.4 Planning for Security in the Life Cycle**

* **Initiation**: Project idea focused on minimizing cost and improving data security.
* **Development/Acquisition**: In-progress using Electron, Node.js, and JavaScript; includes security design (login, role-based access).
* **Implementation**: Will include secure deployment, encrypted databases, and testing (planned June 2025).
* **Operation/Maintenance**: Updates and patches will be scheduled monthly post-release.
* **Disposal**: Procedures will be developed for securely deleting customer data when required.

**B.5 Authorization to Process**

* **Requested By**: Minh Hoang Tran Developer/Owner of the project
* **Request Date**: April 2025
* **Status**: completed, waited for approval

**C. OPERATIONAL CONTROLS**

**C.1 Personnel Security**

* Only registered salon employees can access the app via user accounts.
* Admins have access to all data.
* User roles limit access to only the data needed for job responsibilities.
* Accounts are closed immediately upon employment termination.
* All activity is logged, and users are responsible for their actions.

**C.2 Physical and Environmental Protection**

* The application will run on secured devices located in salons (laptops, desktops).
* Physical protection includes:
  + Devices stored in locked rooms after hours.
  + Antivirus software installed.
  + Encrypted backups stored on external drives in secure storage.

**C.3 Production, Input/Output Controls**

* A built-in check-in module ensures only scheduled customers are served.
* Print tickets that are like a receipt without any customer information.
* Output containing sensitive data is password-protected.
* All changes to the system or user accounts are logged.
* No hardcopy data is produced unnecessarily; sensitive printed documents are shredded.

**C.4 Contingency Planning**

* Daily incremental backups.
* Backups stored on secure external drives.
* A recovery plan is in development to restore the system within 24 hours in case of a crash or breach.

**C.5 Hardware and Software Maintenance Controls**

* Only the developer or authorized IT personnel may perform maintenance.
* Emergency fixes are documented and logged.
* All software is open-source or licensed.
* All changes go through version control and change documentation.
* No live customer data is used for testing; synthetic test data will be used.

**C.6 Data Integrity/Validation Controls**

* Antivirus software is scheduled to auto-scan weekly.
* Logs are reviewed weekly for signs of intrusion.
* Message authentication ensures booking requests haven’t been tampered with.

**C.7 Documentation**

* Maintained Documents:
  + Source code with comments
  + SOPs for account management
  + Risk assessments
  + Version and patch logs
* All documentation is stored physically in a safe place.
* Updated applications will be applied if necessary.

**C.8 Security Awareness and Training**

* Admins and workers receive:
  + Basic onboarding training (10–15 min) on security.
  + Printed quick start guides with safety tips.
  + All security plans and documentation related to security will be provided.
  + Refresher workshops annually.

**C.9 Incident Response Capability**

* + There is a documentation for this part in DOCUMENTATION

**D. TECHNICAL CONTROLS**

**B.1 Identification and Authentication**

* **Authentication Mechanisms**:  
  The system uses password-based authentication for all users.
* **Password Policy**:
  + **Password length**: Minimum 6 characters, maximum 20 characters
  + **Allowable character set**: all numbers
  + **Password aging**: Passwords expire every 90 days
  + **Reuse policy**: Should not reuse password.
  + **Change process**:
    - Contact Minh Tran to change password
    - Forgotten/lost passwords can be reset by email Minh Tran
  + **Compromise procedure**: If compromise is suspected management will need to report, and developer will help to patch and plan to fix the problem.
* **Access Control Enforcement**:
  + **Application level**: Access to application is role-based (admin vs. worker vs. reception desk)
  + **Operating system-level**: Application runs under standard user privileges; does not require admin OS access
  + **Network-level**: If used in local networks, firewall rules can be applied to restrict device access
* **Accountability and Audit**:
  + Each user has a unique user ID and password
  + Actions are logged with a timestamp and user ID
  + Logs support traceability and accountability for all operations
* **Self-Protection Techniques**:
* **Invalid Access Attempts**:
* **Default Admin Password Policy**:
* **Scripts with Embedded Passwords**:
  + These are **strictly prohibited**
  + No automation tasks in this application require embedded credentials
* **Bypassing Authentication / SSO**:
  + No SSO or bypasses implemented due to application simplicity and offline/local-first architecture
* **Digital Signatures**:
  + Not currently in use
  + If implemented in the future, it will comply with **FIPS 186** and **FIPS 180-1**

**B.2 Logical Access Controls**

* **User Authorization**:
  + Access is granted based on role-based access control (RBAC)
  + Roles: Admin (owner), Worker (staff)
* **Access Control List (ACL)**:
* **Operating System Restrictions**:
  + Application runs as a desktop app and does not allow shell access or access to system files
  + Only essential OS permissions are permitted
* **Unauthorized Transaction Detection**:
* **Inactive Session Handling**:
* **Encryption for Sensitive Files**

**B.3 Public Access Controls**

* **Public Access**:  
  The system is not publicly accessible over the internet. It is a desktop application intended for in-salon use only.

**B.4 Audit Trails**

* **Accountability Support**:
  + All user actions (login, logout, appointment updates, payment logs) are tied to their user ID or username
* **Intrusion Detection**:
* **Log Information:**

## Appendix A

**Authorization to Process SMART SALON APPLICATION Memo**

MEMORANDUM

DATE: 4/15/2025

TO: Senior Information Systems Security Officer (ISSO) FROM: Application/System MINH Owner

SUBJECT: Security Authorization for Application/System SSA

Based on a careful review of the Application System SSA Security Plan, I have confirmed that Application/System SSA meets the requirements of SANS information systems security programs. Therefore,

authorize continued operation of Application/System SSA under the following restrictions:

*[List any restrictions here or write "None."]*

I further authorize the initiation of the following corrective actions, scheduled to be completed by the dates listed below:

*[List any corrective actions here or write "None."]*

Owner of Application/System SSA

[Name] [Title] Signature

Person responsible for security of Application/System SSA

[Name] [Title] Signature