MciPro Security Architecture

Complete Staff Security System Documentation

■ Overview

The MciPro staff security system implements a **4-layer defense strategy** to prevent unauthorized access while maintaining a seamless experience for legitimate staff and golfers.

Design Principles:
- ✓ Zero-friction for golfers (unchanged one-click LINE registration)
- ✓ Self-service for most staff (instant access after verification)
- ✓ Manager approval for sensitive roles only
- ✓ Course-specific isolation (each golf course independent)
- ✓ LINE phone lock (one account = one phone number)
- ✓ Scalable across multiple golf courses

■■ Security Layers

Layer 1: Pre-LINE Role Selection

Purpose: Separate golfer and staff registration flows

Implementation:
- Landing page offers two paths:
- **"I'm a Golfer"** → Direct LINE login → One-click profile creation
- **"I'm Staff/Caddie"** → Staff verification screen first

Security Benefit: Prevents casual users from accidentally or intentionally accessing staff registration

File: `index.html` (landing page routing)

Layer 2: Golf Course Code Verification

Purpose: Ensure only verified staff with course-specific codes can register

How It Works:
1. Each golf course has unique 4-digit code

2. Code stored in `localStorage`: `golf_course_settings.staffRegistrationCode`
3. Code displayed in GM's Staff Management dashboard
4. GM can change code anytime (recommended: monthly)
5. Staff must enter correct code to pass verification

Code Management:

```
// Location: staff-security.js
getCourseSettings() {
   return JSON.parse(localStorage.getItem('golf_course_settings') ||
       '{"staffRegistrationCode": "0000"}');
}

saveCourseSettings(settings) {
   localStorage.setItem('golf_course_settings', JSON.stringify(settings));
}
```

GM Interface:
- **Location**: Staff Management Tab → Top section
- **Actions**:
- View current code
- Click "Change Code" button
- Enter new 4-digit code
- Save and distribute to staff

Security Benefits:
- ✓ Course-specific isolation
- ✓ Prevents cross-course unauthorized access
- ✓ Easily revoked (change code monthly)
- ✓ Traceable (code change history logged)
- ✓ Simple for staff to remember

Best Practices:
- Change code monthly (1st of each month)
- Change immediately after staff departures (sensitive roles)
- Change if code is compromised
- Never share publicly (internal distribution only)
- Use non-obvious combinations (avoid 1234, 0000, 1111)

Layer 3: Employee ID Validation

Purpose: Ensure staff use proper identification format and prevent duplicates

Employee ID Formats:

```
Department        | Format      | Example
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
Caddies           | PAT-###     | PAT-001 to PAT-999
Pro Shop          | PS-###      | PS-001, PS-012
Restaurant/F&B    | FB-###      | FB-007, FB-023
Maintenance       | MAINT-###   | MAINT-005
Management        | MGR-###     | MGR-001
Accounting        | ACCT-###    | ACCT-001
Reception         | RCP-###     | RCP-003
Security          | SEC-###     | SEC-002
```

Validation Logic:

```
// Location: staff-security.js:112-120
validateEmployeeId(employeeId, department) {
   const formats = this.getEmployeeIdFormat();
   const format = formats[department];
   if (!format) return false;

   const regex = new RegExp(`^${format.prefix}-\\d{${format.length}}$`);
   return regex.test(employeeId);
}
```

Duplicate Prevention:

```
// Location: staff-security.js:284-289
const staff = JSON.parse(localStorage.getItem('staff_members') || '[]');
const exists = staff.find(s => s.employeeId === employeeId);

if (exists) {
   return { success: false, error: 'This Employee ID is already registered' };
}
```

Security Benefits:
- ✓ Prevents random ID entries
- ✓ Department-specific formatting enforces organization
- ✓ Duplicate detection prevents multiple accounts per employee
- ✓ Easy to audit (format instantly shows department)
- ✓ Scalable (add new formats for new departments)

Layer 4: Manager Approval Queue

Purpose: Extra verification for sensitive roles before granting access

Roles Requiring Approval:
- **Management** (MGR-###): Full system access
- **Pro Shop** (PS-###): Financial transactions, inventory
- **Accounting** (ACCT-###): Financial data access

Roles with Instant Access (No Approval):
- Caddies (PAT-###)
- Restaurant/F&B (FB-###)
- Maintenance (MAINT-###)
- Reception (RCP-###)
- Security (SEC-###)

Approval Logic:

```
// Location: staff-security.js:155-161
requiresApproval(department, position) {
   const sensitiveRoles = ['management', 'proshop'];
   const sensitivePositions = ['manager', 'accounting', 'acct', 'pro shop'];

   return sensitiveRoles.includes(department) ||
          sensitivePositions.some(role => position.toLowerCase().includes(role));
}
```

Approval Workflow:

Staff Registers:
- Completes verification (Layer 2 & 3)
- Authenticates via LINE
- Creates profile
- Status set to `pending_approval`
- Dashboard shows "Pending Approval" message

Manager Notified:
- Pending staff appears in Staff Management
- Yellow notification banner
- Count displayed: "Pending Approvals (3)"

Manager Reviews:
- Views staff details:

- Name
- Employee ID
- Department
- Phone number
- Email
- LINE verification status ✓
- Decides: Approve or Reject

Approval:
- Click "Approve" button
- Status changes to `active`
- Staff gets immediate access
- Approval timestamp and approver recorded

Rejection:
- Click "Reject" button
- Profile completely removed
- Staff cannot log in
- Must re-register with correct information

Manager Dashboard Interface:

```
// Location: staff-security.js:196-263
renderPendingApprovalsUI() {
   const pending = this.getPendingApprovals();
   // Renders yellow notification box with:
   // - Staff name and position
   // - Employee ID
   // - Contact information
   // - LINE verification status
   // - Approve/Reject buttons
}
```

Security Benefits:
- ✓ Human verification for high-privilege roles
- ✓ Prevents automated mass registrations
- ✓ Manager recognizes legitimate employees
- ✓ Quick to approve (24-hour average)
- ✓ Audit trail (who approved, when)
- ✓ Can reject suspicious requests

Layer 5: LINE Phone Lock (Existing)

Purpose: Ensure one person = one account using LINE's built-in security

How LINE Works:
- 1 LINE account = 1 phone number (verified by LINE)
- Phone number verified via SMS by LINE
- Cannot create multiple LINE accounts with same phone number
- Cannot register same LINE account twice in MciPro

MciPro Integration:

```
// Each profile linked to lineUserId (unique identifier)
const profile = {
   lineUserId: 'U1234567890abcdef...',  // Unique LINE ID
   // ... other profile data
};
```

Duplicate Prevention:
- System checks if `lineUserId` already exists
- If exists, loads existing profile (returning user)
- If new, creates new profile
- One LINE ID = one MciPro profile

Security Benefits:
- ✓ Identity verified by LINE (trusted third party)
- ✓ Phone number verification by SMS
- ✓ Cannot create multiple accounts with same phone
- ✓ Cannot register without smartphone
- ✓ Prevents bot/automated registrations
- ✓ Lost phone = recover LINE = recover MciPro access

■ Data Flow Diagrams

Golfer Registration Flow

```
Golfer Clicks "Log in with LINE"
          ↓
   LINE Authentication
```

```
        ↓
 Return with LINE Profile
        ↓
   Check if lineUserId exists
        ↓
   ■■■■■■■■■■■■■■
   ↓           ↓
EXISTS      NEW USER
   ↓           ↓
Load Profile  Create Profile
   ↓           ↓
Dashboard   Dashboard
```

Time: ~30 seconds
User Actions: 2 clicks
Security Checks: 1 (LINE phone verification)

Staff Registration Flow (Non-Sensitive)

```
Staff Clicks "I'm Staff/Caddie"
        ↓
 Staff Verification Page
        ↓
 Enter: Course Code + Department + Employee ID
        ↓
 Validation:
 1. ✓ Course Code matches
 2. ✓ Employee ID format correct
 3. ✓ No duplicate Employee ID
        ↓
 Store in sessionStorage
        ↓
 Redirect to LINE Authentication
        ↓
 Return with LINE Profile
        ↓
 Create Staff Profile
 • Role → Department mapping
 • Status = 'active' (instant access)
 • Save to staff_members
```

```
        ↓
Dashboard (Immediate Access)
```

Time: ~2-3 minutes
User Actions: 7 inputs, 3 clicks
Security Checks: 4 (code, format, duplicate, LINE)

Staff Registration Flow (Sensitive Roles)

```
Staff Clicks "I'm Staff/Caddie"
        ↓
Staff Verification Page
        ↓
Enter: Course Code + Department + Employee ID
        ↓
Validation (same as above)
        ↓
LINE Authentication
        ↓
Create Staff Profile
• Status = 'pending_approval'
• Save to staff_members
        ↓
"Pending Approval" Screen
        ↓
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■   MANAGER DASHBOARD      ■
■   Pending Approvals      ■
■   [Staff Details]        ■
■   [Approve] [Reject]     ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
        ↓
Manager Clicks "Approve"
        ↓
Status → 'active'
        ↓
LINE Notification to Staff
        ↓
Staff Logs In
        ↓
```

```
Dashboard (Now Has Access)
```

Time: 2-3 minutes (registration) + wait for approval
Wait Time: 1-24 hours average
Security Checks: 5 (code, format, duplicate, LINE, human verification)

■■ Data Storage

---

localStorage Keys

1. golf_course_settings

```
{
 "staffRegistrationCode": "1234",
 "courseName": "Greenview Golf Club",
 "lastCodeUpdate": "2025-10-07T10:30:00.000Z",
 "courseId": "GVC-001",
 "managerName": "John Manager"
}
```

Purpose: Store course-specific configuration
Security: Stored client-side, course-specific
Access: GM can modify via Staff Management dashboard

---

2. staff_members

```
[
 {
   "id": "STAFF-1728284930123",
   "firstName": "John",
   "lastName": "Smith",
   "employeeId": "PAT-023",
   "department": "caddy",
   "position": "Caddie",
   "phone": "+66 12 345 6789",
   "email": "john.smith@email.com",
   "status": "active",
   "hireDate": "2025-10-01",
```

```
    "lineUserId": "U1234567890abcdef",
    "caddyLicense": "PAT-023",
    "experienceLevel": "Expert",
    "gpsTrackerId": "GPS-PAT-023",
    "languages": "English, Thai",
    "workingStatus": "off-duty",
    "currentLocation": null,
    "rating": 4.8,
    "totalAssignments": 247,
    "totalTips": 125400,
    "approvedAt": "2025-10-01T09:15:00.000Z",
    "approvedBy": "Jane Manager"
  },
  {
    "id": "STAFF-1728285930456",
    "firstName": "Sarah",
    "lastName": "Johnson",
    "employeeId": "PS-001",
    "department": "proshop",
    "position": "Pro Shop Manager",
    "phone": "+66 87 654 3210",
    "email": "sarah.johnson@email.com",
    "status": "pending_approval",
    "hireDate": "2025-10-07",
    "lineUserId": "U0987654321fedcba",
    "approvedAt": null,
    "approvedBy": null
  }
]
```


Purpose: Store all staff profiles

Security: Status field controls access

Access: GMs can view/edit, staff can view own profile

---

3. mcipro_user_profiles (Unified Profiles)


```
[
  {
    "id": "USER-1728284930123",
    "lineUserId": "U1234567890abcdef",
```

```
  "firstName": "John",
  "lastName": "Smith",
  "phone": "+66 12 345 6789",
  "email": "john.smith@email.com",
  "role": "caddie",
  "roleSpecific": {
    "caddyNumber": "PAT-023",
    "experience": "Expert",
    "languages": ["English", "Thai"]
  }
 }
]
```

Purpose: Unified profile storage (golfers + staff)
Security: Role field determines dashboard access
Access: Used for authentication and profile loading

---

sessionStorage Keys

staff_verification (Temporary)

```
{
 "verified": true,
 "courseCode": "1234",
 "department": "caddy",
 "employeeId": "PAT-023",
 "timestamp": 1728284930123
}
```

Purpose: Temporary storage during registration
Security: Cleared after registration completes
Lifetime: Session only (closes with browser tab)

■ Security Best Practices

For Golf Course Management

1. Registration Code Management:
- ✓ Change codes monthly on 1st of month

- ✓ Use non-sequential numbers (avoid 1234, 0000)
- ✓ Distribute codes securely (in-person, private messages)
- ✓ Log code changes with dates
- ✓ Change immediately if compromised
- ✓ Use different codes for multi-course operations

2. Approval Queue Monitoring:
- ✓ Check pending approvals daily
- ✓ Verify employee legitimacy before approving
- ✓ Investigate suspicious registrations
- ✓ Reject unknown/unauthorized attempts
- ✓ Document all approvals/rejections
- ✓ Response time: Within 24 hours

3. Staff Roster Audits:
- ✓ Weekly: Review active staff list
- ✓ Monthly: Full roster audit
- ✓ Quarterly: Verify all employee IDs
- ✓ Deactivate departed staff immediately
- ✓ Check for duplicate accounts
- ✓ Verify department assignments

4. Access Control:
- ✓ Deactivate staff upon termination (same day)
- ✓ Review staff access logs periodically
- ✓ Monitor unusual activity patterns
- ✓ Investigate failed login attempts
- ✓ Report security incidents immediately

For Staff

1. Registration Security:
- ✓ Keep course code confidential
- ✓ Never share employee ID
- ✓ Use secure phone with lock screen
- ✓ Keep LINE app updated
- ✓ Report lost phone immediately

2. Account Security:
- ✓ Secure LINE password
- ✓ Enable LINE two-factor authentication
- ✓ Log out on shared devices
- ✓ Don't share login credentials

- ✓ Report suspicious activity

3. Data Protection:
- ✓ Don't share customer data
- ✓ Don't screenshot sensitive info
- ✓ Follow data privacy policies
- ✓ Report data breaches immediately

■ Security Incident Response

Unauthorized Access Attempt

Indicators:
- Multiple failed code attempts
- Suspicious employee IDs
- Repeated registration attempts
- Unknown names in pending approvals

Response Protocol:
1. **Immediate**: Reject pending approval
2. **Immediate**: Change staff registration code
3. **Within 1 hour**: Notify all department heads
4. **Within 4 hours**: Distribute new code securely
5. **Within 24 hours**: Full staff roster audit
6. **Within 48 hours**: Review security logs
7. **Document**: Complete incident report

Code Compromise

Indicators:
- Code shared publicly (social media, etc.)
- Unknown staff registrations
- Former employee still has code

Response Protocol:
1. **Immediate**: Change code
2. **Immediate**: Review recent registrations
3. **Within 1 hour**: Notify managers
4. **Within 4 hours**: Distribute new code
5. **Within 24 hours**: Deactivate suspicious accounts
6. **Within 48 hours**: Security review

Staff Account Compromise

Indicators:
- Staff reports unauthorized access
- Unusual activity on account
- Login from unexpected location
- LINE account compromised

Response Protocol:
1. **Immediate**: Deactivate staff account
2. **Immediate**: Notify IT/Security team
3. **Within 1 hour**: Staff changes LINE password
4. **Within 4 hours**: Review account activity
5. **Within 24 hours**: Reactivate if safe
6. **Document**: Incident report

■ Security Monitoring & Auditing

Automated Alerts

System Monitors:
- Failed code attempts (3+ in 10 minutes)
- Duplicate employee ID attempts
- Pending approvals over 48 hours old
- Staff account login failures (5+)
- Unusual access patterns

Alert Recipients:
- General Manager
- IT/Security team
- System administrator

Audit Logs

What's Logged:

```
Event Type          | Data Recorded
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
Staff Registration  | Time, Employee ID, Department, IP
```

```
Code Change          | Time, Old Code, New Code, Changed By
Approval/Rejection   | Time, Staff ID, Decision, Manager
Login                | Time, LINE User ID, Success/Fail
Profile Updates      | Time, Field Changed, Old/New Value
```

Log Retention: 12 months minimum

Access: General Manager, IT/Security team

Regular Security Reviews

Weekly:
- Pending approvals status
- Recent registrations review
- Failed access attempts
- Staff roster changes

Monthly:
- Full staff roster audit
- Code change (recommended)
- Security log review
- Access pattern analysis
- Incident summary

Quarterly:
- Comprehensive security audit
- Policy review
- Staff security training
- System vulnerability assessment
- Compliance check

Annually:
- Full system security review
- Penetration testing
- Policy updates
- Staff security certification
- Third-party audit (if applicable)

■ Compliance & Privacy

Data Privacy (PDPA Compliance)

Personal Data Collected:
- Name
- Phone number
- Email address (optional)
- LINE User ID
- Employee ID
- Department
- Employment history

Data Usage:
- Staff management
- Access control
- Performance tracking
- Communication
- Payroll (if integrated)

Data Protection:
- Stored locally (client-side)
- No cloud storage without consent
- Encrypted transmission (HTTPS)
- Access restricted by role
- Audit trail maintained

Data Rights:
- Staff can view own data
- Staff can request corrections
- Staff can request deletion (with employment termination)
- Staff can export own data

Access Control Policy

Role-Based Access:

General Manager:
- ✓ Full system access
- ✓ View all staff
- ✓ Approve/reject registrations
- ✓ Change registration codes
- ✓ View all reports
- ✓ Export data

Department Manager:
- ✓ View department staff
- ✓ Edit department staff
- ✓ View department reports
- ✗ Cannot approve staff
- ✗ Cannot change codes

Staff:
- ✓ View own profile
- ✓ Edit own contact info
- ✓ View own schedule
- ✓ View own performance
- ✗ Cannot view other staff
- ✗ Cannot access admin functions

■ Related Documentation

- General Manager Guide
- Staff Registration Guide
- Troubleshooting
- Technical Implementation

■ Security Contacts

Report Security Issues:
- Email: security@mcipro.com
- Phone: [Emergency security line]
- In-Person: General Manager office

For Technical Issues:
- Email: support@mcipro.com
- Phone: [IT support line]

Last Updated: October 7, 2025
Version: 1.0
Next Review: November 7, 2025
Classification: Internal Use Only