MciPro 安全架构

完整员工安全系统文档

概述

MciPro 员工安全系统实施4层防御策略,以防止未经授权的访问,同时为合法员工和高尔夫球手保持无缝体验。

设计原则:

- 球手零摩擦(保持一键式 LINE 注册不变)
- 大多数员工自助服务(验证后立即访问)
- 仅敏感角色需要管理者批准
- 球场特定隔离(每个高尔夫球场独立)
- LINE 手机锁定(一个账户 = 一个手机号码)
- 可跨多个高尔夫球场扩展

安全层级

第1层:LINE 前角色选择

目的:分离球手和员工注册流程

实施方式:

- 登录页面提供两个路径:
- "我是球手" → 直接 LINE 登录 → 一键创建个人资料
- "我是员工/球童" → 先进入员工验证屏幕

安全优势:防止普通用户意外或故意访问员工注册

文件: index.html (登录页面路由)

第2层:高尔夫球场代码验证

目的:确保只有拥有球场特定代码的已验证员工才能注册

工作原理:

1. 每个高尔夫球场拥有独特的4位数字代码
2. 代码存储在 localStorage: golf_course_settings.staffRegistrationCode
3. 代码显示在总经理的员工管理仪表板中
4. 总经理可以随时更改代码(建议:每月)
5. 员工必须输入正确的代码才能通过验证

代码管理:

```
getCourseSettings() { return JSON.parse(localStorage.getItem('golf_course_settings') || '{"staffRegistrationCode": "0000"}'); }
```

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

总经理界面:

- 位置:员工管理选项卡 → 顶部部分
- 操作:
- 查看当前代码
- 点击"更改代码"按钮
- 输入新的4位数字代码
- 保存并分发给员工

安全优势:

- 球场特定隔离
- 防止跨球场未经授权的访问
- 易于撤销(每月更改代码)
- 可追溯(记录代码更改历史)
- 员工易于记忆

最佳实践:

- 每月更改代码(每月1日)
- 员工离职后立即更改(敏感角色)
- 代码被泄露时立即更改

- 绝不公开分享(仅内部分发)
- 使用非明显的组合(避免 1234、0000、1111)

第3层:员工ID验证

目的:确保员工使用适当的识别格式并防止重复

员工ID格式:

```
————————————————————————————————┼————————————————————————————————— 球童 | PAT-### | PAT-001 至 PAT-999 专业店 | PS-### | PS-001, PS-012 餐厅/餐饮 | FB-### | FB-007, FB-023 维护 | MAINT-### | MAINT-005 管理 | MGR-### | MGR-001 会计 | ACCT-### | ACCT-001 接待 | RCP-### | RCP-003 安保 | SEC-### | SEC-002
```

验证逻辑:

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); }
```

防止重复:

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' }; }
```

安全优势:

- 防止随机ID输入
- 部门特定格式强制执行组织
- 重复检测防止每位员工拥有多个账户
- 易于审计(格式立即显示部门)
- 可扩展(为新部门添加新格式)

第4层:管理者批准队列

目的:在授予访问权限之前对敏感角色进行额外验证

需要批准的角色:

- 管理 (MGR-###):完整系统访问权限

- 专业店 (PS-###):财务交易、库存
- 会计 (ACCT-###):财务数据访问

具有即时访问权限的角色(无需批准):

- 球童 (PAT-###)
- 餐厅/餐饮 (FB-###)
- 维护 (MAINT-###)
- 接待 (RCP-###)
- 安保 (SEC-###)

批准逻辑:

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)); }
```

批准工作流程:

员工注册:

- 完成验证(第2层和第3层)
- 通过 LINE 进行身份验证
- 创建个人资料
- 状态设置为 pending_approval
- 仪表板显示"等待批准"消息

管理者收到通知:

- 待批准的员工出现在员工管理中
- 黄色通知横幅
- 显示计数:"待批准 (3)"

管理者审核:

- 姓名
- 员工ID
- 部门
- 电话号码
- 电子邮件
- LINE 验证状态

- 决定:批准或拒绝

批准:

- 点击"批准"按钮
- 状态更改为 active
- 员工获得即时访问权限
- 记录批准时间戳和批准者

拒绝:

- 点击"拒绝"按钮
- 完全删除个人资料
- 员工无法登录
- 必须使用正确信息重新注册

管理者仪表板界面:

```
renderPendingApprovalsUI() { const pending = this.getPendingApprovals(); // 渲染黄色通知框,包含: // - 员工姓名和职位 // - 员工ID // - 联系信息 // - LINE 验证状态 // - 批准/拒绝按钮 }
```

安全优势:

- 对高权限角色进行人工验证
- 防止自动化批量注册
- 管理者识别合法员工
- 快速批准(平均24小时内)
- 审计跟踪(谁批准了、何时批准)
- 可以拒绝可疑请求

第5层:LINE 手机锁定(现有)

目的:使用 LINE 的内置安全性确保一个人 = 一个账户

LINE 工作原理:

- 1个 LINE 账户 = 1个手机号码(由 LINE 验证)
- 手机号码通过 LINE 的短信验证
- 无法使用同一手机号码创建多个 LINE 账户
- 无法在 MciPro 中重复注册同一 LINE 账户

MciPro 集成:

```
const profile = { lineUserId: 'U1234567890abcdef...', // 唯一 LINE ID // ... 其他个人资料数据 };
```

防止重复:

- 系统检查 lineUserId 是否已存在
- 如果存在,加载现有个人资料(回访用户)
- 如果是新用户,创建新个人资料
- 一个 LINE ID = 一个 MciPro 个人资料

安全优势:

- 由 LINE 验证身份(可信第三方)
- 通过短信验证手机号码
- 无法使用同一手机创建多个账户
- 没有智能手机无法注册
- 防止机器人/自动注册
- 手机丢失 = 恢复 LINE = 恢复 MciPro 访问

数据流程图

球手注册流程

```
↓ LINE 身份验证 ↓ 返回 LINE 个人资料 ↓ 检查 lineUserId 是否存在 ↓ ┌──────────┴──────────┐ ↓
↓ 存在 新用户 ↓ ↓ 加载个人资料 创建个人资料 ↓ ↓ 仪表板 仪表板
```

时间:约30秒

用户操作:2次点击

安全检查:1次(LINE 手机验证)

员工注册流程(非敏感)

```
↓ 员工验证页面 ↓ 输入:球场代码 + 部门 + 员工ID ↓ 验证: 1. 球场代码匹配 2. 员工ID格式正确 3.
无重复员工ID ↓ 存储在 sessionStorage 中 ↓ 重定向到 LINE 身份验证 ↓ 返回 LINE 个人资料 ↓
创建员工个人资料 • 角色 → 部门映射 • 状态 = 'active'(即时访问) • 保存到 staff_members ↓
仪表板(立即访问)
```

时间:约2-3分钟

用户操作:7次输入,3次点击

安全检查:4次(代码、格式、重复、LINE)

员工注册流程(敏感角色)

```
↓ 员工验证页面 ↓ 输入:球场代码 + 部门 + 员工ID ↓ 验证(与上述相同) ↓ LINE 身份验证 ↓
创建员工个人资料 • 状态 = 'pending_approval' • 保存到 staff_members ↓ "等待批准"屏幕 ↓
┌──────────────────────────────────────────────┐ | 管理者仪表板 | | 待批准 | |
[员工详细信息] | | [批准][拒绝] | └──────────────────────────────────────────────┘ ↓
管理者点击"批准" ↓ 状态 → 'active' ↓ 向员工发送 LINE 通知 ↓ 员工登录 ↓ 仪表板(现在拥有访问权限)
```

时间:2-3分钟(注册) + 等待批准

等待时间:平均1-24小时

安全检查:5次(代码、格式、重复、LINE、人工验证)

数据存储

localStorage 键

1. golfcoursesettings


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


目的:存储球场特定配置

安全性:客户端存储,球场特定

访问:总经理可通过员工管理仪表板修改

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 } ]
```


目的:存储所有员工个人资料

安全性:状态字段控制访问

访问:总经理可以查看/编辑,员工可以查看自己的个人资料

3. mciprouserprofiles(统一个人资料)

{ "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"] } }]

目的:统一个人资料存储(球手 + 员工)

安全性:角色字段确定仪表板访问

访问:用于身份验证和个人资料加载

sessionStorage 键

staff_verification(临时)

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

目的:注册期间的临时存储

安全性:注册完成后清除

生命周期:仅会话(关闭浏览器选项卡时结束)

安全最佳实践

高尔夫球场管理

1. 注册代码管理:
- 每月1日更改代码
- 使用非连续数字(避免 1234、0000)
- 安全分发代码(亲自交付、私人消息)
- 记录代码更改及日期
- 如果被泄露,立即更改
- 多球场运营使用不同代码

2. 批准队列监控:
- 每日检查待批准项
- 批准前验证员工合法性

- 调查可疑注册
- 拒绝未知/未经授权的尝试
- 记录所有批准/拒绝
- 响应时间:24小时内

3. 员工名册审计:
- 每周:审查活跃员工列表
- 每月:完整名册审计
- 每季度:验证所有员工ID
- 离职员工立即停用
- 检查重复账户
- 验证部门分配

4. 访问控制:
- 员工离职当天停用账户
- 定期审查员工访问日志
- 监控异常活动模式
- 调查失败的登录尝试
- 立即报告安全事件

员工

1. 注册安全:
- 保持球场代码机密
- 绝不分享员工ID
- 使用带锁屏的安全手机
- 保持 LINE 应用更新
- 手机丢失立即报告

2. 账户安全:
- 保护 LINE 密码
- 启用 LINE 双因素身份验证
- 在共享设备上注销
- 不共享登录凭据

- 报告可疑活动

3. 数据保护:

- 不共享客户数据
- 不截屏敏感信息
- 遵守数据隐私政策
- 立即报告数据泄露

安全事件响应

未经授权的访问尝试

指标:

- 多次失败的代码尝试
- 可疑的员工ID
- 重复注册尝试
- 待批准中的未知姓名

响应协议:

1. 立即:拒绝待批准
2. 立即:更改员工注册代码
3. 1小时内:通知所有部门主管
4. 4小时内:安全分发新代码
5. 24小时内:完整员工名册审计
6. 48小时内:审查安全日志
7. 记录:完整事件报告

代码泄露

指标:

- 代码公开分享(社交媒体等)
- 未知员工注册
- 前员工仍持有代码

响应协议:

1. 立即:更改代码
2. 立即:审查最近的注册
3. 1小时内:通知管理者
4. 4小时内:分发新代码
5. 24小时内:停用可疑账户
6. 48小时内:安全审查

员工账户泄露

指标:

- 员工报告未经授权的访问
- 账户上的异常活动
- 从意外位置登录
- LINE 账户泄露

响应协议:

1. 立即:停用员工账户
2. 立即:通知 IT/安全团队
3. 1小时内:员工更改 LINE 密码
4. 4小时内:审查账户活动
5. 24小时内:如果安全,重新激活
6. 记录:事件报告

安全监控与审计

自动化警报

系统监控:

- 失败的代码尝试(10分钟内3次以上)
- 重复员工ID尝试
- 超过48小时的待批准项

- 员工账户登录失败(5次以上)
- 异常访问模式

警报接收者:

- 总经理
- IT/安全团队
- 系统管理员

审计日志

记录内容:

```
──────────────────────────────────┼──────────────────────────────────────────────
──────── 员工注册 | 时间、员工ID、部门、IP 代码更改 | 时间、旧代码、新代码、更改者 批准/拒绝 |
时间、员工ID、决定、管理者 登录 | 时间、LINE 用户ID、成功/失败 个人资料更新 |
时间、更改的字段、旧/新值
```

日志保留:最少12个月

访问:总经理、IT/安全团队

定期安全审查

每周:

- 待批准状态
- 最近注册审查
- 失败的访问尝试
- 员工名册变更

每月:

- 完整员工名册审计
- 代码更改(建议)
- 安全日志审查
- 访问模式分析
- 事件摘要

每季度:

- 全面安全审计

- 政策审查
- 员工安全培训
- 系统漏洞评估
- 合规检查

每年:
- 完整系统安全审查
- 渗透测试
- 政策更新
- 员工安全认证
- 第三方审计(如适用)

合规与隐私

数据隐私(PDPA 合规)

收集的个人数据:
- 姓名
- 电话号码
- 电子邮件地址(可选)
- LINE 用户ID
- 员工ID
- 部门
- 就业历史

数据使用:
- 员工管理
- 访问控制
- 绩效跟踪
- 沟通
- 薪资(如果集成)

数据保护:
- 本地存储(客户端)

- 未经同意不进行云存储
- 加密传输(HTTPS)
- 按角色限制访问
- 维护审计跟踪

数据权利:
- 员工可以查看自己的数据
- 员工可以请求更正
- 员工可以请求删除(随就业终止)
- 员工可以导出自己的数据

访问控制政策

基于角色的访问:

总经理:
- 完整系统访问权限
- 查看所有员工
- 批准/拒绝注册
- 更改注册代码
- 查看所有报告
- 导出数据

部门经理:
- 查看部门员工
- 编辑部门员工
- 查看部门报告
- 不能批准员工
- 不能更改代码

员工:
- 查看自己的个人资料
- 编辑自己的联系信息
- 查看自己的日程安排
- 查看自己的绩效

- 不能查看其他员工
- 不能访问管理功能

相关文档

- 总经理指南
- 员工注册指南
- 故障排除
- 技术实施

安全联系方式

报告安全问题:

- 电子邮件: security@mcipro.com
- 电话:[紧急安全热线]
- 现场:总经理办公室

技术问题:

- 电子邮件: support@mcipro.com
- 电话:[IT 支持热线]

最后更新:2025年10月7日

版本: 1.0

下次审查:2025年11月7日

分类:仅限内部使用