สถาปัตยกรรมความปลอดภัย MciPro

เอกสารระบบความปลอดภัยสำหรับพนักงานฉบับสมบูรณ์

☐ ภาพรวม

ระบบความปลอดภัยสำหรับพนักงาน MciPro ใช้กลยุทธ์การป้องกัน 4 ชั้น
เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
ในขณะที่รักษาประสบการณ์การใช้งานที่ราบรื่นสำหรับพนักงานและนักกอล์ฟที่ถูกต้อง

หลักการออกแบบ: - ☐ ไม่มีอุปสรรคสำหรับนักกอล์ฟ (การลงทะเบียน LINE
แบบคลิกเดียวเหมือนเดิม) - ☐ บริการตนเองสำหรับพนักงานส่วนใหญ่
(เข้าถึงทันทีหลังการตรวจสอบ) - ☐ การอนุมัติจากผู้จัดการสำหรับตำแหน่งที่ละเอียดอ่อนเท่านั้น -
☐ การแยกเฉพาะสนามกอล์ฟ (แต่ละสนามกอล์ฟเป็นอิสระ) - ☐ การล็อคหมายเลขโทรศัพท์ LINE
(1 บัญชี = 1 หมายเลขโทรศัพท์) - ☐ ขยายได้ในหลายสนามกอล์ฟ

☐☐ ชั้นความปลอดภัย

ชั้นที่ 1: การเลือกบทบาทก่อน LINE

วัตถุประสงค์: แยกเส้นทางการลงทะเบียนของนักกอล์ฟและพนักงาน

การดำเนินการ: - หน้า Landing page เสนอสองเส้นทาง: - "ฉันเป็นนักกอล์ฟ" → เข้าสู่ระบบ LINE
โดยตรง → สร้างโปรไฟล์แบบคลิกเดียว - "ฉันเป็นพนักงาน/แคดดี้" →
หน้าจอการตรวจสอบพนักงานก่อน

ประโยชน์ด้านความปลอดภัย:
ป้องกันผู้ใช้ทั่วไปจากการเข้าถึงการลงทะเบียนพนักงานโดยไม่ตั้งใจหรือตั้งใจ

ไฟล์: index.html (การกำหนดเส้นทางหน้า landing page)

ชั้นที่ 2: การตรวจสอบรหัสสนามกอล์ฟ

วัตถุประสงค์:
ให้แน่ใจว่าเฉพาะพนักงานที่ได้รับการตรวจสอบพร้อมรหัสเฉพาะสนามเท่านั้นที่สามารถลงทะเบียนได้

วิธีการทำงาน: 1. แต่ละสนามกอล์ฟมีรหัส 4 หลักที่ไม่ซ้ำกัน 2. รหัสเก็บไว้ใน localStorage: golf_course_settings.staffRegistrationCode 3. รหัสแสดงใน Dashboard การจัดการพนักงานของ GM 4. GM สามารถเปลี่ยนรหัสได้ตลอดเวลา (แนะนำ: รายเดือน) 5. พนักงานต้องกรอกรหัสที่ถูกต้องเพื่อผ่านการตรวจสอบ

การจัดการรหัส:

อินเทอร์เฟซ GM: - ตำแหน่ง: แท็บการจัดการพนักงาน → ส่วนบนสุด - การดำเนินการ: - ดูรหัสปัจจุบัน - คลิกปุ่ม "เปลี่ยนรหัส" - ป้อนรหัส 4 หลักใหม่ - บันทึกและแจกจ่ายให้กับพนักงาน

ประโยชน์ด้านความปลอดภัย: - ☐ การแยกเฉพาะสนาม - ☐ ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตข้ามสนาม - ☐ เพิกถอนได้ง่าย (เปลี่ยนรหัสรายเดือน) - ☐ ติดตามได้ (บันทึกประวัติการเปลี่ยนรหัส) - ☐ ง่ายสำหรับพนักงานในการจดจำ

แนวปฏิบัติที่ดีที่สุด: - เปลี่ยนรหัสรายเดือน (วันที่ 1 ของแต่ละเดือน) - เปลี่ยนทันทีหลังจากพนักงานลาออก (ตำแหน่งที่ละเอียดอ่อน) - เปลี่ยนหากรหัสถูกเปิดเผย - ห้ามแชร์สาธารณะ (แจกจ่ายภายในเท่านั้น) - ใช้ชุดตัวเลขที่ไม่ชัดเจน (หลีกเลี่ยง 1234, 0000, 1111)

ชั้นที่ 3: การตรวจสอบรหัสพนักงาน

วัตถุประสงค์: ให้แน่ใจว่าพนักงานใช้รูปแบบการระบุตัวตนที่เหมาะสมและป้องกันการซ้ำซ้อน

รูปแบบรหัสพนักงาน:

```
[redacted]               | [redacted]      | [redacted]
[redacted]
[redacted]               | PAT-###     | PAT-001 [redacted] PAT-999
[redacted]               | PS-###      | PS-001, PS-012
[redacted]/F&B           | FB-###      | FB-007, FB-023
[redacted]               | MAINT-###   | MAINT-005
[redacted]               | MGR-###     | MGR-001
[redacted]               | ACCT-###    | ACCT-001
[redacted]               | RCP-###     | RCP-003
[redacted]               | SEC-###     | SEC-002
```

ตัวตรวจสอบ:

การป้องกันการซ้ำซ้อน:

ประโยชน์ด้านความปลอดภัย: - ☐ ป้องกันการป้อนรหัสแบบสุ่ม - ☐ การจัดรูปแบบเฉพาะแผนกบังคับให้มีองค์กร - ☐ การตรวจจับการซ้ำซ้อนป้องกันหลายบัญชีต่อพนักงาน - ☐ ง่ายต่อการตรวจสอบ (รูปแบบแสดงแผนกทันที) - ☐ ขยายได้ (เพิ่มรูปแบบใหม่สำหรับแผนกใหม่)

ชั้นที 4: คิวการอนุมัติจากผู้จัดการ

วัตถุประสงค์: การตรวจสอบเพิ่มเติมสำหรับบทบาททีละเอียดอ่อนก่อนให้สิทธิ์การเข้าถึง

บทบาททีต้องการการอนุมัติ: - ฝ่ายบริหาร (MGR-###): การเข้าถึงระบบแบบเต็มรูปแบบ - ร้านโปร (PS-###): ธุรกรรมทางการเงิน, สินค้าคงคลัง - บัญชี (ACCT-###): การเข้าถึงข้อมูลทางการเงิน

บทบาททีมีการเข้าถึงทันที (ไม่ต้องอนุมัติ): - แคดดี (PAT-###) - ภัตตาคาร/F&B; (FB-###) - ซ่อมบำรุง (MAINT-###) - แผนกต้อนรับ (RCP-###) - รักษาความปลอดภัย (SEC-###)

ตรรกะการอนุมัติ:

ขั้นตอนการอนุมัติ:

1. พนักงานลงทะเบียน: เสร็จสิ้นการตรวจสอบ (ชั้นที 2 & 3) ยืนยันตัวตนผ่าน LINE สร้างโปรไฟล์ ตั้งสถานะเป็น pending_approval Dashboard แสดงข้อความ "รอการอนุมัติ"
7. ผู้จัดการได้รับแจ้งเตือน: พนักงานทีรอการอนุมัติปรากฏในการจัดการพนักงาน แบนเนอร์แจ้งเตือนสีเหลือง แสดงจำนวน: "รอการอนุมัติ (3)"
11. ผู้จัดการตรวจสอบ: ดูรายละเอียดพนักงาน: ชื่อ รหัสพนักงาน แผนก หมายเลขโทรศัพท์ อีเมล สถานะการตรวจสอบ LINE ☐ ตัดสินใจ: อนุมัติหรือปฏิเสธ
20. การอนุมัติ: คลิกปุ่ม "อนุมัติ" สถานะเปลี่ยนเป็น active พนักงานได้รับการเข้าถึงทันที บันทึกเวลาอนุมัติและผู้อนุมัติ
25. การปฏิเสธ: คลิกปุ่ม "ปฏิเสธ" โปรไฟล์ถูกลบอย่างสมบูรณ์ พนักงานไม่สามารถเข้าสู่ระบบได้ ต้องลงทะเบียนใหม่ด้วยข้อมูลทีถูกต้อง

อินเทอร์เฟซ Dashboard ผู้จัดการ:

ประโยชน์ด้านความปลอดภัย: - ☐ การตรวจสอบโดยมนุษย์สำหรับบทบาททีมีสิทธิ์สูง - ☐ ป้องกันการลงทะเบียนจำนวนมากแบบอัตโนมัติ - ☐ ผู้จัดการจดจำพนักงานทีถูกต้อง - ☐ อนุมัติเร็ว (เฉลีย 24 ชัวโมง) - ☐ การติดตามการตรวจสอบ (ใครอนุมัติ, เมือไหร่) - ☐ สามารถปฏิเสธคำขอทีน่าสงสัย

ชั้นที 5: การล็อคหมายเลขโทรศัพท์ LINE (มอยู่แล้ว)

วัตถุประสงค์: ให้แน่ใจว่า 1 คน = 1 บัญชีโดยใช้ความปลอดภัยในตัวของ LINE

วิธีการทำงานของ LINE: - 1 บัญชี LINE = 1 หมายเลขโทรศัพท์ (ตรวจสอบโดย LINE) - หมายเลขโทรศัพท์ตรวจสอบผ่าน SMS โดย LINE - ไม่สามารถสร้างหลายบัญชี LINE ด้วยหมายเลขโทรศัพท์เดียวกัน - ไม่สามารถลงทะเบียนบัญชี LINE เดียวกันสองครั้งใน MciPro

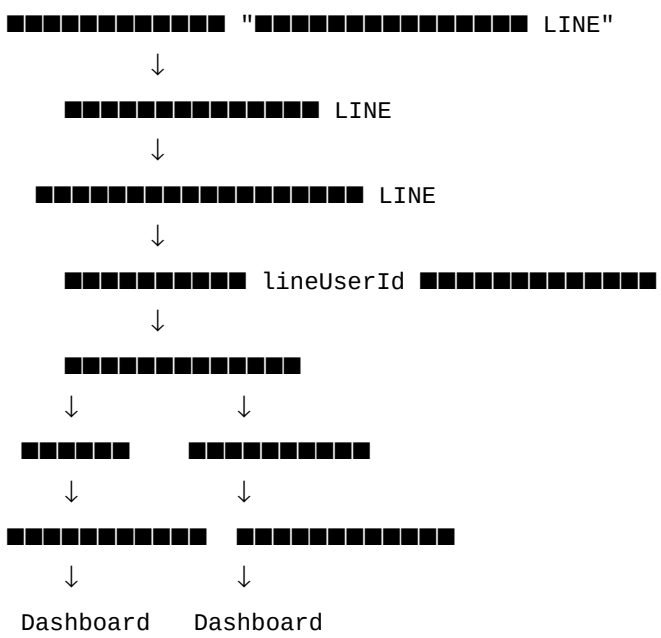
การรวม MciPro:

การป้องกันการซ้ำซ้อน: - ระบบตรวจสอบว่า lineUserId มีอยู่แล้วหรือไม่ - ถ้ามี, โหลดโปรไฟล์ที่มีอยู่ (ผู้ใช้เดิม) - ถ้าใหม่, สร้างโปรไฟล์ใหม่ - 1 LINE ID = 1 โปรไฟล์ MciPro

ประโยชน์ด้านความปลอดภัย: - ☐ ตัวตนตรวจสอบโดย LINE (บุคคลที่สามที่เชื่อถือได้) - ☐ การตรวจสอบหมายเลขโทรศัพท์ผ่าน SMS - ☐ ไม่สามารถสร้างหลายบัญชีด้วยโทรศัพท์เดียวกัน - ☐ ไม่สามารถลงทะเบียนโดยไม่มีสมาร์ทโฟน - ☐ ป้องกันการลงทะเบียนโดยบอท/อัตโนมัติ - ☐ ทำโทรศัพท์หาย = กู้คืน LINE = กู้คืนการเข้าถึง MciPro

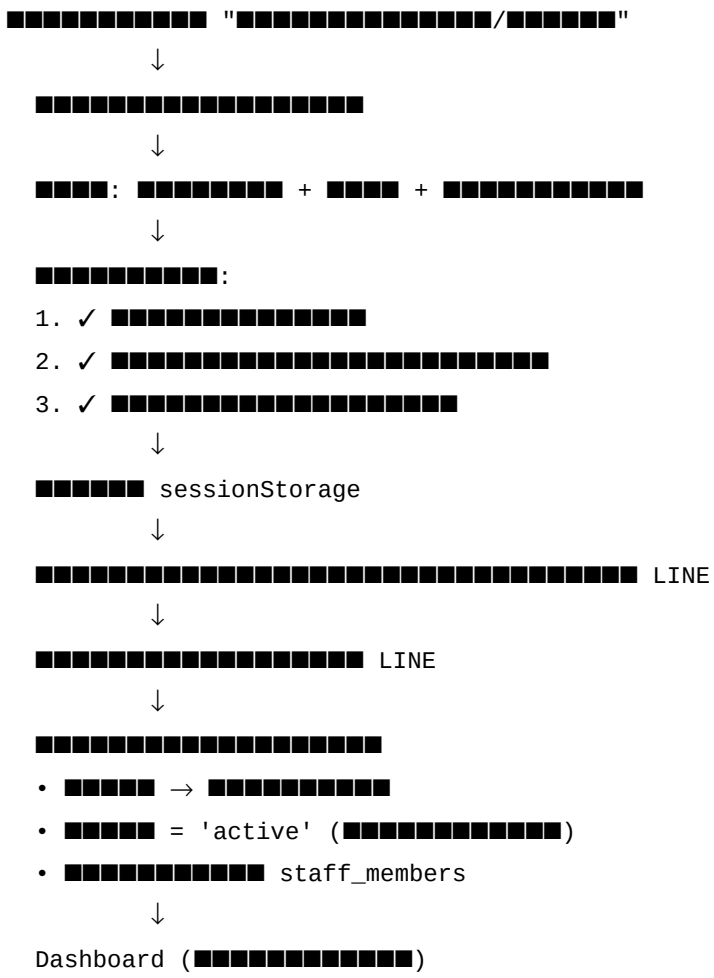
☐ แผนภาพการไหลของข้อมูล

ขั้นตอนการลงทะเบียนนักกอล์ฟ



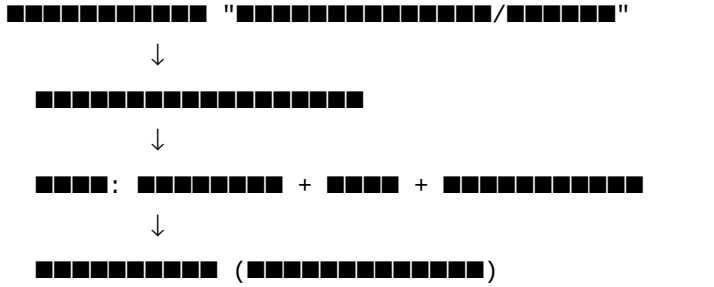
เวลา: ~30 วินาที การดำเนินการของผู้ใช้: 2 คลิก การตรวจสอบความปลอดภัย: 1 (การตรวจสอบโทรศัพท์ LINE)

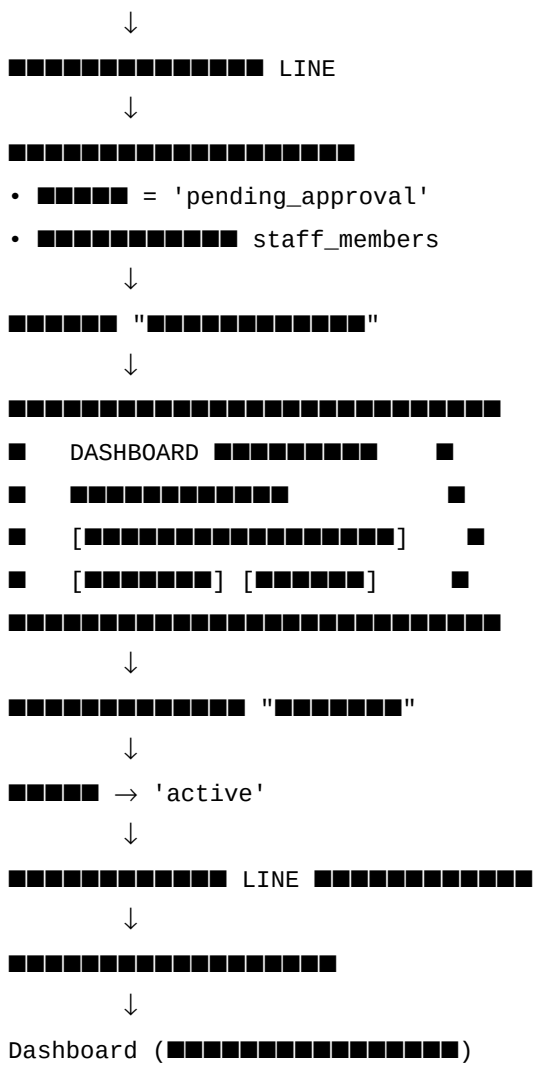
ขั้นตอนการลงทะเบียนพนักงาน (ไม่ละเอียดอ่อน)



เวลา: ~2-3 นาที การดำเนินการของผู้ใช้: 7 ข้อมูลนำเข้า, 3 คลิก การตรวจสอบความปลอดภัย: 4 (รหัส, รูปแบบ, การซ้ำ, LINE)

ขั้นตอนการลงทะเบียนพนักงาน (บทบาททีละเอียดอ่อน)





เวลา: 2-3 นาที (การลงทะเบียน) + รอการอนุมัติ เวลารอ: เฉลีย 1-24 ชัวโมง
การตรวจสอบความปลอดภัย: 5 (รหัส, รูปแบบ, การซ้ำ, LINE, การตรวจสอบโดยมนุษย์)

□□ การจัดเก็บข้อมูล

คีย์ localStorage

1. golf_course_settings

วัตถุประสงค์: จัดเก็บการกำหนดค่าเฉพาะสนาม ความปลอดภัย: จัดเก็บฝังไคลเอนต์, เฉพาะสนาม
การเข้าถึง: GM สามารถแก้ไขผ่าน Dashboard การจัดการพนักงาน

2. staff_members

วัตถุประสงค์: จัดเก็บโปรไฟล์พนักงานทั้งหมด ความปลอดภัย: ฟิลด์สถานะควบคุมการเข้าถึง การเข้าถึง: GM สามารถดู/แก้ไข, พนักงานสามารถดูโปรไฟล์ของตนเอง

3. mcipro_user_profiles (โปรไฟล์แบบรวม)

วัตถุประสงค์: การจัดเก็บโปรไฟล์แบบรวม (นักกอล์ฟ + พนักงาน) ความปลอดภัย: ฟิลด์บทบาทกำหนดการเข้าถึง Dashboard การเข้าถึง: ใช้สำหรับการยืนยันตัวตนและการโหลดโปรไฟล์

คีย์ sessionStorage

staff_verification (ชั่วคราว)

วัตถุประสงค์: การจัดเก็บชั่วคราวระหว่างการลงทะเบียน ความปลอดภัย: ถูกล้างหลังจากการลงทะเบียนเสร็จสิ้น อายุการใช้งาน: เซสชันเท่านั้น (ปิดด้วยแท็บเบราว์เซอร์)

☐ แนวปฏิบัติด้านความปลอดภัยที่ดีที่สุด

สำหรับฝ่ายจัดการสนามกอล์ฟ

1. การจัดการรหัสการลงทะเบียน: - ☐ เปลี่ยนรหัสรายเดือนในวันที่ 1 ของเดือน - ☐ ใช้ตัวเลขที่ไม่ต่อเนื่อง (หลีกเลี่ยง 1234, 0000) - ☐ แจกจ่ายรหัสอย่างปลอดภัย (ตัวต่อตัว, ข้อความส่วนตัว) - ☐ บันทึกการเปลี่ยนรหัสพร้อมวันที่ - ☐ เปลี่ยนทันทีหากถูกเปิดเผย - ☐ ใช้รหัสที่แตกต่างกันสำหรับการดำเนินงานหลายสนาม

2. การตรวจสอบคิวการอนุมัติ: - ☐ ตรวจสอบการอนุมัติที่รอดำเนินการทุกวัน - ☐ ตรวจสอบความถูกต้องของพนักงานก่อนอนุมัติ - ☐ สืบสวนการลงทะเบียนที่น่าสงสัย - ☐ ปฏิเสธความพยายามที่ไม่รู้จัก/ไม่ได้รับอนุญาต - ☐ บันทึกการอนุมัติ/การปฏิเสธทั้งหมด - ☐ เวลาตอบสนอง: ภายใน 24 ชั่วโมง

3. การตรวจสอบรายชื่อพนักงาน: - ☐ รายสัปดาห์: ตรวจสอบรายชื่อพนักงานที่ใช้งานอยู่ - ☐ รายเดือน: การตรวจสอบรายชื่อเต็มรูปแบบ - ☐ รายไตรมาส: ตรวจสอบรหัสพนักงานทั้งหมด - ☐ ปิดการใช้งานพนักงานที่ออกทันที - ☐ ตรวจสอบบัญชีที่ซ้ำกัน - ☐ ตรวจสอบการมอบหมายแผนก

4. การควบคุมการเข้าถึง: - ☐ ปิดการใช้งานพนักงานเมื่อเลิกจ้าง (วันเดียวกัน) - ☐ ตรวจสอบบันทึกการเข้าถึงของพนักงานเป็นระยะ - ☐ ตรวจสอบรูปแบบกิจกรรมที่ผิดปกติ - ☐

สืบสวนความพยายามเข้าสู่ระบบทีล้มเหลว - ☐ รายงานเหตุการณ์ด้านความปลอดภัยทันที

สำหรับพนักงาน

1. ความปลอดภัยในการลงทะเบียน: - ☐ เก็บรหัสสนามเป็นความลับ - ☐ ห้ามแชร์รหัสพนักงาน - ☐ ใช้โทรศัพท์ทีปลอดภัยพร้อมหน้าจอล็อค - ☐ เก็บแอป LINE ให้อัปเดต - ☐ รายงานการทำโทรศัพท์หายทันที

2. ความปลอดภัยของบัญชี: - ☐ รหัสผ่าน LINE ทีปลอดภัย - ☐ เปิดใช้งานการยืนยันตัวตนสองขั้นตอน LINE - ☐ ออกจากระบบบนอุปกรณ์ทีใช้ร่วมกัน - ☐ ห้ามแชร์ข้อมูลรับรองการเข้าสู่ระบบ - ☐ รายงานกิจกรรมทีน่าสงสัย

3. การปกป้องข้อมูล: - ☐ ห้ามแชร์ข้อมูลลูกค้า - ☐ ห้ามถ่ายภาพหน้าจอข้อมูลทีละเอียดอ่อน - ☐ ปฏิบัติตามนโยบายความเป็นส่วนตัวของข้อมูล - ☐ รายงานการละเมิดข้อมูลทันที

☐ การตอบสนองต่อเหตุการณ์ด้านความปลอดภัย

ความพยายามเข้าถึงโดยไม่ได้รับอนุญาต

ตัวบ่งชี: - ความพยายามใช้รหัสทีล้มเหลวหลายครัง - รหัสพนักงานทีน่าสงสัย - ความพยายามลงทะเบียนซ้ำ ๆ - ชือทีไม่รู้จักในการอนุมัติทีรอดำเนินการ

ขันตอนการตอบสนอง: 1. ทันที: ปฏิเสธการอนุมัติทีรอดำเนินการ 2. ทันที: เปลียนรหัสการลงทะเบียนพนักงาน 3. ภายใน 1 ชัวโมง: แจ้งหัวหน้าแผนกทังหมด 4. ภายใน 4 ชัวโมง: แจกจ่ายรหัสใหม่อย่างปลอดภัย 5. ภายใน 24 ชัวโมง: การตรวจสอบรายชือพนักงานเต็มรูปแบบ 6. ภายใน 48 ชัวโมง: ตรวจสอบบันทึกความปลอดภัย 7. เอกสาร: รายงานเหตุการณ์ทีสมบูรณ์

การเปิดเผยรหัส

ตัวบ่งชี: - รหัสถูกแชร์สาธารณะ (โซเชียลมีเดีย, ฯลฯ) - การลงทะเบียนพนักงานทีไม่รู้จัก - พนักงานเดิมยังมีรหัส

ขันตอนการตอบสนอง: 1. ทันที: เปลียนรหัส 2. ทันที: ตรวจสอบการลงทะเบียนล่าสุด 3. ภายใน 1 ชัวโมง: แจ้งผู้จัดการ 4. ภายใน 4 ชัวโมง: แจกจ่ายรหัสใหม่ 5. ภายใน 24 ชัวโมง:

ปิดการใช้งานบัญชีที่น่าสงสัย 6. ภายใน 48 ชั่วโมง: การตรวจสอบความปลอดภัย

การบุกรุกบัญชีพนักงาน

ตัวบ่งชี้: - พนักงานรายงานการเข้าถึงโดยไม่ได้รับอนุญาต - กิจกรรมผิดปกติในบัญชี - การเข้าสู่ระบบจากตำแหน่งที่ไม่คาดคิด - บัญชี LINE ถูกบุกรุก

ขั้นตอนการตอบสนอง: 1. ทันที: ปิดการใช้งานบัญชีพนักงาน 2. ทันที: แจ้งทีม IT/ความปลอดภัย 3. ภายใน 1 ชั่วโมง: พนักงานเปลี่ยนรหัสผ่าน LINE 4. ภายใน 4 ชั่วโมง: ตรวจสอบกิจกรรมบัญชี 5. ภายใน 24 ชั่วโมง: เปิดใช้งานอีกครั้งหากปลอดภัย 6. เอกสาร: รายงานเหตุการณ์

☐ การตรวจสอบและการตรวจสอบความปลอดภัย

การแจ้งเตือนอัตโนมัติ

การตรวจสอบระบบ: - ความพยายามใช้รหัสที่ล้มเหลว (3+ ใน 10 นาที) - ความพยายามใช้รหัสพนักงานซ้ำ - การอนุมัติที่รอดำเนินการมากกว่า 48 ชั่วโมง - ความล้มเหลวในการเข้าสู่ระบบบัญชีพนักงาน (5+) - รูปแบบการเข้าถึงที่ผิดปกติ

ผู้รับการแจ้งเตือน: - ผู้จัดการทั่วไป - ทีม IT/ความปลอดภัย - ผู้ดูแลระบบ

บันทึกการตรวจสอบ

สิ่งที่ถูกบันทึก:

```
[redacted]        | [redacted]
[redacted]
[redacted]  | [redacted], [redacted], [redacted], IP
[redacted]       | [redacted], [redacted], [redacted], [redacted]
[redacted]/[redacted]    | [redacted], [redacted], [redacted], [redacted]
[redacted]         | [redacted], LINE User ID, [redacted]/[redacted]
[redacted]    | [redacted], [redacted], [redacted]/[redacted]
```

การเก็บรักษาบันทึก: อย่างน้อย 12 เดือน

การเข้าถึง: ผู้จัดการทั่วไป, ทีม IT/ความปลอดภัย

การตรวจสอบความปลอดภัยเป็นประจำ

รายสัปดาห์: - สถานะการอนุมัติที่รอดำเนินการ - การตรวจสอบการลงทะเบียนล่าสุด - ความพยายามเข้าถึงที่ล้มเหลว - การเปลี่ยนแปลงรายชื่อพนักงาน

รายเดือน: - การตรวจสอบรายชื่อพนักงานเต็มรูปแบบ - การเปลี่ยนรหัส (แนะนำ) - การตรวจสอบบันทึกความปลอดภัย - การวิเคราะห์รูปแบบการเข้าถึง - สรุปเหตุการณ์

รายไตรมาส: - การตรวจสอบความปลอดภัยที่ครอบคลุม - การตรวจสอบนโยบาย - การฝึกอบรมความปลอดภัยของพนักงาน - การประเมินช่องโหว่ของระบบ - การตรวจสอบการปฏิบัติตาม

รายปี: - การตรวจสอบความปลอดภัยระบบเต็มรูปแบบ - การทดสอบการเจาะระบบ - การอัปเดตนโยบาย - การรับรองความปลอดภัยของพนักงาน - การตรวจสอบโดยบุคคลที่สาม (ถ้าเกี่ยวข้อง)

☐ การปฏิบัติตามและความเป็นส่วนตัว

ความเป็นส่วนตัวของข้อมูล (การปฏิบัติตาม PDPA)

ข้อมูลส่วนบุคคลที่เก็บรวบรวม: - ชื่อ - หมายเลขโทรศัพท์ - ที่อยู่อีเมล (ไม่บังคับ) - LINE User ID - รหัสพนักงาน - แผนก - ประวัติการจ้างงาน

การใช้ข้อมูล: - การจัดการพนักงาน - การควบคุมการเข้าถึง - การติดตามประสิทธิภาพ - การสื่อสาร - เงินเดือน (ถ้ารวม)

การปกป้องข้อมูล: - จัดเก็บภายใน (ผ้งไคลเอนต์) - ไม่มีการจัดเก็บบนคลาวด์โดยไม่มีความยินยอม - การส่งที่เข้ารหัส (HTTPS) - การเข้าถึงถูกจำกัดตามบทบาท - การติดตามการตรวจสอบถูกรักษา

สิทธิ์ข้อมูล: - พนักงานสามารถดูข้อมูลของตนเอง - พนักงานสามารถขอการแก้ไข - พนักงานสามารถขอลบ (เมื่อเลิกจ้าง) - พนักงานสามารถส่งออกข้อมูลของตนเอง

นโยบายการควบคุมการเข้าถึง

การเข้าถึงตามบทบาท:

ผู้จัดการทั่วไป: - ☐ การเข้าถึงระบบเต็มรูปแบบ - ☐ ดูพนักงานทั้งหมด - ☐ อนุมัติ/ปฏิเสธการลงทะเบียน - ☐ เปลี่ยนรหัสการลงทะเบียน - ☐ ดูรายงานทั้งหมด - ☐ ส่งออกข้อมูล

ผู้จัดการแผนก: - ☐ ดูพนักงานแผนก - ☐ แก้ไขพนักงานแผนก - ☐ ดูรายงานแผนก - ☐ ไม่สามารถอนุมัติพนักงาน - ☐ ไม่สามารถเปลี่ยนรหัส

พนักงาน: - ☐ ดูโปรไฟล์ของตนเอง - ☐ แก้ไขข้อมูลติดต่อของตนเอง - ☐ ดูตารางเวลาของตนเอง - ☐ ดูประสิทธิภาพของตนเอง - ☐ ไม่สามารถดูพนักงานอื่น - ☐ ไม่สามารถเข้าถึงฟังก์ชันผู้ดูแลระบบ

☐ เอกสารที่เกี่ยวข้อง

- **คู่มือผู้จัดการทั่วไป**
- **คู่มือการลงทะเบียนพนักงาน**
- **การแก้ไขปัญหา**
- **การใช้งานทางเทคนิค**

☐ ผู้ติดต่อด้านความปลอดภัย

รายงานปัญหาด้านความปลอดภัย: - อีเมล: security@mcipro.com - โทรศัพท์: [สายด่วนความปลอดภัยฉุกเฉิน] - ตัวต่อตัว: สำนักงานผู้จัดการทั่วไป

สำหรับปัญหาทางเทคนิค: - อีเมล: support@mcipro.com - โทรศัพท์: [สาย IT support]

อัปเดตล่าสุด: 7 ตุลาคม 2025 เวอร์ชัน: 1.0 การตรวจสอบครั้งถัดไป: 7 พฤศจิกายน 2025 การจำแนก: ใช้ภายในเท่านั้น