เรื่อง การอนุมัติยกเว้นการปฏิบัติตามนโยบายด้าน IT Policy หัวข้อเรื่องการกำหนดรหัสผ่าน

เรียน คุณมัณฑนา อัศวเมธา

เนื่องด้วยข้อกำหนดวิธีการกำหนดรหัสผ่าน ซึ่งถูกกำหนดไว้ในนโยบายการควบคุมความปลอดภัยทางเทคโนโลยีสารสนเทศ เลขที่เอกสาร QP-IT-001 ที่เริ่มมีผลบังคับใช้ตั้งแต่วันที่ 14 กันยายน 2563 แต่มีบางระบบที่ไม่สามารถปฏิบัติตามข้อกำหนดได้ทั้งหมด ซึ่งได้ระบุไว้ในตารางด้านล่างนี้

ระบบ	Application Level ของระบบ AdaPos
ข้อกำหนดที่ขอยกเว้น	• รหัสผ่านควรประกอบด้วย ตัวอักษรภาษาอังกฤษ ตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ อักขระพิเศษและตัวเลข (0-9) • รหัสผ่านต้องมีความยาวขั้นต่ำอย่างน้อย 8 ตัวอักษร • รหัสผ่านต้องเปลี่ยนทุก ๆ 90 วัน • ระงับการใช้งานเมื่อมีการกรอกรหัสผ่านผิดจำนวน 5 ครั้ง • รหัสผ่านไม่สามารถใช้ซ้ำกับรหัสผ่านเดิม 5 ครั้ง • ในกรณีที่ไม่มีการปฏิบัติงานที่อยู่หน้าเครื่องคอมพิวเตอร์ ซึ่งมีการระยะเวลาสิ้นสุดการใช้งานของระบบเมื่อไม่มีกิจกรรม (Idle Timeout) หรือ ระยะเวลาในการเชื่อมต่อระบบ (Session Timeout) ที่ 15 นาที
เหตุผล	เป็นข้อจำกัดของระบบ AdaPos ไม่มีพารามิเตอร์ให้กำหนดรหัสผ่านตามข้อกำหนด
มาตรการชดเชยเพื่อลดความเสี่ยง	• มีการควบคุมโดยมีกระบวนการปิดการขายประจำวัน ซึ่งจะมีการกระทบยอดขาย ซึ่ง Cashier จะสรุปผลการกระทบยอดระหว่างใบปิดการขายในระบบกับบันทึกสรุปยอดเงินและเอกสารประกอบว่าจำนวนยอดขาย โดยผู้จัดการ / หัวหน้าสาขาตรวจสอบความถูกต้องพร้อมเซ็นชื่อกำกับ

ระบบ	Database level ของระบบ ISCode
ข้อกำหนดที่ขอยกเว้น	• รหัสผ่านต้องเปลี่ยนทุก ๆ 90 วัน • ระงับการใช้งานเมื่อมีการกรอกรหัสผ่านผิดจำนวน 5 ครั้ง • รหัสผ่านไม่สามารถใช้ซ้ำกับรหัสผ่านเดิม 5 ครั้ง • ในกรณีที่ไม่มีการปฏิบัติงานที่อยู่หน้าเครื่องคอมพิวเตอร์ ซึ่งมีการระยะเวลาสิ้นสุดการใช้งานของระบบเมื่อไม่มีกิจกรรม (Idle Timeout) หรือ ระยะเวลาในการเชื่อมต่อระบบ (Session Timeout) ที่ 15 นาที
เหตุผล	เป็นข้อจำกัดของระบบ ISCode ไม่มีพารามิเตอร์ให้กำหนดรหัสผ่านตามข้อกำหนด

มาตรการชดเชยเพื่อลดความเสี่ยง	• จำกัดการเข้าถึงระบบฐานข้อมูลเฉพาะผู้ให้บริการเท่านั้น โดยผู้ให้บริการจะสามารถเข้าถึงฐานข้อมูลผ่านระบบ VPN (Remote Access) ซึ่งต้องได้รับอนุญาต จึงจะเข้าถึงระบบฐานข้อมูลได้ • มีการควบคุมผู้ใช้งานที่มีสิทธิสูงอย่างเหมาะสม

ระบบ	Database level ของระบบ SAP S/4 HANA
ข้อกำหนดที่ขอยกเว้น	• รหัสผ่านต้องเปลี่ยนทุก ๆ 90 วัน • รหัสผ่านควรประกอบด้วย ตัวอักษรภาษาอังกฤษ ตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ อักขระพิเศษและตัวเลข (0-9)
เหตุผล	1. SYS 2. SYSTEM 3. _SYS_STATISTICS 4. XSSQLCC_AUTO_USER_3094F258A8978F7A7558E080D94C8500B0772804AA2663AF6058A40D719CA72D 5. XSSQLCC_AUTO_USER_D5D3B0C4F06A79377BE0D4198763EC5EDEBC14E80D1BB1BBABA9D3B5F3C4AD1A 6. XSSQLCC_AUTO_USER_5E2492DBCDEDAE8BF85A0EA2741D2302882088A51A3ED5634ABEB402AE579A39 7. SAPDBCTRL 8. DBACOCKPIT 9. SAPHANADB • User ดังกล่าว ไม่สามารถ Setting Parameter ค่า LIFETIME_CHECK _ENABLED เป็น TRUE เนื่องจากหากมีการ Setting ให้ Password Expire ในกรณีที่ต้องการเข้าใช้งาน User ดังกล่าวจะต้องมี Plan Downtime เกิดขึ้นเพื่อ Reset Password ซึ่งจะกระทบกับ Operation ระหว่างวัน • ไม่สามารถ Setting Parameter ค่า Password_layout ให้มีอักขระพิเศษได้ เนื่องจากหากมีการ Setting ระบบจะบังคับให้ Change Password ทุก User ซึ่งจะส่งผลกระทบต่อระบบ
มาตรการชดเชยเพื่อลดความเสี่ยง	• จำกัดการเข้าถึงระบบฐานข้อมูลเฉพาะผู้ให้บริการเท่านั้น โดยผู้ให้บริการจะสามารถเข้าถึงฐานข้อมูลผ่านระบบ VPN (Remote Access) ซึ่งต้องได้รับอนุญาต จึงจะเข้าถึงระบบฐานข้อมูลได้ • มีการควบคุมผู้ใช้งานที่มีสิทธิสูงอย่างเหมาะสม

ระบบ	Database level ของระบบ AdaPos
ข้อกำหนดที่ขอยกเว้น	• รหัสผ่านต้องเปลี่ยนทุก ๆ 90 วัน
เหตุผล	User sa และ User distributor_admin ไม่สามารถ Setting Parameter ค่า is_expiration_checked = 1 เนื่องจากระบบมีการ Config Password ไว้หลายๆ ที่ หากมีการ Setting ให้ Password Expire ต้องมีการ Downtime ซึ่งจะกระทบกับ Operation ระหว่างวัน
มาตรการชดเชยเพื่อลดความเสี่ยง	• จำกัดการเข้าถึงระบบฐานข้อมูลเฉพาะผู้ให้บริการเท่านั้น โดยผู้ให้บริการจะสามารถเข้าถึงฐานข้อมูลผ่านระบบ VPN (Remote Access) ซึ่งต้องได้รับอนุญาต จึงจะเข้าถึงระบบฐานข้อมูลได้ • มีการควบคุมผู้ใช้งานที่มีสิทธิสูงอย่างเหมาะสม

ผู้จัดทำ ..... (นางสาวปิยะวรรณ แก้วเมือง) SMGR-IT	ผู้สอบทาน..... (นางสาวศุภรดา โชจินวัฒนะ) CFO	ผู้อนุมัติ ..... (นางสาวมัณฑนา อัศวเมธา) Deputy CEO

ประกาศใช้ ณ วันที่ 04 มกราคม 2566
ฉบับแก้ไขครั้งที่ 02