มาตรฐานการควบคุมการเข้าถึงระบบสารสนเทศ

(Access Control Standard)

ประกาศใช้เมื่อ	
ผู้รับผิดชอบ	แผนกเทคโนโลยีสารสนเทศ (MIS Department)

1. วัตถุประสงค์ (Objectives)

เพื่อกำหนดเกณฑ์มาตรฐานขั้นต่ำสำหรับการอนุญาต การจำกัดสิทธิ์ และการจัดการการเข้าถึงระบบสารสนเทศให้มีความปลอดภัย สอดคล้องกับ “นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ” ของบริษัท พีรพัฒน์ เทคโนโลยี จำกัด (มหาชน)

2. มาตรฐานการตั้งรหัสผ่าน (Password Standard)

รหัสผ่านสำหรับเข้าใช้งานระบบสารสนเทศของบริษัท (เช่น Windows AD, Oracle NetSuite) ต้องเป็นไปตามมาตรฐานดังต่อไปนี้ :

1. ความยาวรหัสผ่าน (Minimum Length): ต้องมีไม่น้อยกว่า 8 ตัวอักษร
2. ความซับซ้อน (Complexity): ต้องประกอบด้วย 3 ใน 4 องค์ประกอบดังนี้:
    - ตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ (A-Z)
    - ตัวอักษรภาษาอังกฤษพิมพ์เล็ก (a-z)
    - ตัวเลข (0-9)
    - อักขระพิเศษ (เช่น !, @, #, $, %)
3. อายุรหัสผ่าน (Password Expiry): ต้องมีการบังคับเปลี่ยนรหัสผ่านทุกๆ 90 วัน
4. ประวัติรหัสผ่าน (Password History): ห้ามใช้รหัสผ่านซ้ำกับรหัสผ่านเดิมที่เคยใช้ 5 ครั้งล่าสุด

5. การระงับบัญชีเมื่อเข้าระบบผิด (Account Lockout Threshold): หากใส่รหัสผ่านผิดติดต่อกันครบ 5 ครั้ง บัญชีจะถูกล็อคโดยอัตโนมัติ (Lockout) เป็นเวลาอย่างน้อย 15 นาที หรือจนกว่าจะแจ้งเจ้าหน้าที่แผนกสารสนเทศ ให้ปลดล็อค แผนกสารสนเทศต้องจัดทำรายงานบันทึกประวัติการระงับบัญชีที่ผิดปกติทุกเดือน
6. กรณีมีข้อจำกัดหรือไม่สามารถกำหนดค่าบังคับตามมาตรฐานรหัสผ่านของบริษัทได้ ต้องได้รับการอนุมัติจากผู้จัดการแผนกสารสนเทศ โดยมีการระบุเหตุผลข้อจำกัด

3. มาตรฐานตารางกำหนดสิทธิ์ (User Authorization Matrix - UAM)

1. บริษัท พีรพัฒน์ เทคโนโลยี จำกัด (มหาชน) ต้องจัดทำตารางมาตรฐานกำหนดสิทธิ์ (User Authorization Matrix) สำหรับระบบงานสำคัญ (เช่น Oracle NetSuite)
2. UAM ต้องถูกจัดทำขึ้นโดยหัวหน้าแผนกผู้เป็นเจ้าของกระบวนการทางธุรกิจ (Business Owner)
3. UAM จะเป็นเอกสารอ้างอิงหลักที่แผนกสารสนเทศ ใช้ในการควบคุมให้เป็นไปตามสิทธิ์ (Roles/Permissions)

4. มาตรฐานสิทธิ์ขั้นสูง (High Privilege Access)

1. การจำกัดผู้มีสิทธิ์: สิทธิ์ระดับ Administrator จะสงวนไว้ให้เจ้าหน้าที่แผนกสารสนเทศ ที่มีหน้าที่ดูแลระบบโดยตรงเท่านั้น ห้ามมอบให้บุคคลภายนอก หรือผู้ใช้ทั่วไปถือครองในระยะยาว
2. Vendor / Outsource: หาก Vendor หรือบุคลากรอื่นจำเป็นต้องใช้สิทธิ์ขั้นสูงเพื่อแก้ไขระบบ ต้องทำเรื่องร้องขอชั่วคราว (Time-based access) และเมื่อเสร็จสิ้นงาน แผนกสารสนเทศต้องทำการระงับการทำงาน หรือลดระดับสิทธิ์ลงทันที
3. การตรวจสอบ: บัญชีสิทธิ์ขั้นสูงตามการร้องขอในข้อ 2 เมื่อมีการระงับสิทธิ์การใช้งาน ผู้จัดการแผนกสารสนเทศต้องลงนามรับทราบด้วยทุกครั้ง

5. การเข้าถึงจากระยะไกล (Remote Access Standard)

การเชื่อมต่อเข้าระบบภายในของบริษัทจากภายนอก (Work from Home หรือ Vendor Support) จะต้องเชื่อมต่อผ่าน Virtual Private Network (VPN) ที่บริษัทกำหนดเท่านั้น

ลงชื่อผู้อนุมัติ

.....

(คุณรุ่งทิพย์ มีแม่นวิทย์)

ตำแหน่ง: ประธานฝ่ายเจ้าหน้าที่บริหาร

วันที่: ...../...../.....