นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

Information Security Policy

ประกาศใช้เมื่อ	
ผู้รับผิดชอบ	แผนกเทคโนโลยีสารสนเทศ (MIS Department)

1. วัตถุประสงค์ (Objectives)

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท พีรพัฒน์ เทคโนโลยี จำกัด (มหาชน) เพื่อให้มั่นใจว่าข้อมูลและระบบสารสนเทศที่สำคัญ (เช่น Oracle NetSuite และระบบอื่นๆ) ได้รับการปกป้องอย่างเหมาะสม รักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) สอดคล้องกับมาตรฐาน และการดำเนินงานในปัจจุบัน

รักษาความลับ (Confidentiality)	ความถูกต้องครบถ้วน (Integrity)	ความพร้อมใช้งาน (Availability)

2. ขอบเขต (Scope)

นโยบายนี้มีผลบังคับใช้กับบุคคลทุกกลุ่มที่มีสิทธิ์เข้าถึงข้อมูลและระบบสารสนเทศของบริษัท พีรพัฒน์ เทคโนโลยี จำกัด (มหาชน) ได้แก่

- พนักงานและผู้บริหารทุกระดับ
- ผู้รับจ้างและผู้ให้บริการภายนอก (Vendors / Contractors)
- นักศึกษาฝึกงานและบุคคลภายนอกที่ได้รับสิทธิ์เข้าถึงระบบ

3. นโยบายการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control Policy)

อยู่บนพื้นฐานหลักการ Least Privilege (ให้สิทธิ์เท่าที่จำเป็น) โดยมีรายละเอียดดังนี้

3.1 การขอเข้าใช้งานระบบ

- ผู้ใช้งานต้องได้รับการอนุมัติอย่างเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาแผนกต้นสังกัด หรือในกรณีพนักงานใหม่ แผนกทรัพยากรบุคคล (HR) สามารถเป็นผู้แจ้งรายชื่อพนักงานเพื่อให้แผนกสารสนเทศดำเนินการสร้างบัญชีผู้ใช้งานได้เพื่อให้เกิดความรวดเร็วในการปฏิบัติงาน
- ต้องผ่านช่องทางการร้องขออย่างเป็นทางการ ได้แก่
  - เปิด Ticket ผ่านระบบ IT Helpdesk
  - กรอกฟอร์มเอกสาร หรือแบบฟอร์มอิเล็กทรอนิกส์ที่กำหนด
  - ส่งอีเมลที่ระบุรายละเอียดอย่างชัดเจน

3.2 การจัดการสิทธิ์ขั้นสูง (High Privilege User Control)

- บัญชี Administrator / Super User มอบให้เฉพาะบุคลากรแผนกสารสนเทศที่ได้รับอนุมัติเท่านั้น
- ห้ามผู้ให้บริการภายนอก (Vendors) ถือครองสิทธิ์สูงสุดเป็นการถาวร
  - หากจำเป็นต้องใช้ชั่วคราว ให้สร้างบัญชีแบบ Time-based Account
  - ระงับการทำงานทันทีเมื่องานแล้วเสร็จ

3.3 การเข้าถึงจากระยะไกล (Remote Access Control)

- การเข้าถึงจากภายนอกเครือข่ายต้องผ่านช่องทางที่ปลอดภัย เช่น VPN (Virtual Private Network)
- ต้องได้รับการอนุมัติตามระดับความสำคัญของข้อมูล

3.4 ความปลอดภัยของรหัสผ่าน

- รหัสผ่านต้องมีความซับซ้อนตาม “มาตรฐานการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control Standard)”
- ระบบต้องกำหนด Account Lockout Policy เพื่อป้องกันการสุ่มเดารหัสผ่าน
- จำนวนครั้งที่ผิดพลาดและระยะเวลาระงับบัญชีให้ปรับใช้ตาม System Capability

4. นโยบายการตรวจสอบและทบทวนสิทธิ์ (Monitoring and Review Policy)

- **การสอบทานบัญชีผู้ใช้งาน (User Profile Review):** แผนกสารสนเทศและผู้จัดการแต่ละหน่วยงานต้องร่วมตรวจสอบสถานะบัญชี ความเหมาะสมของสิทธิ์และการแบ่งแยกหน้าที่ (Segregation of Duties) อย่างน้อยปีละ 1 ครั้ง

- **การเฝ้าระวังการเข้าถึง (Abnormal Access Monitoring):** แผนกสารสนเทศต้องมีกลไกตรวจสอบและจัดเก็บ Log การเข้าถึงที่ผิดปกติ (เช่น Login ล้มเหลวซ้ำหรือการเข้าถึงข้อมูลนอกเหนือสิทธิ์) และรายงานต่อผู้จัดการแผนกสารสนเทศ

- **การจัดการพนักงานพ้นสภาพ:** แผนก HR ต้องแจ้งแผนกสารสนเทศล่วงหน้าหรือทันทีเมื่อพนักงานลาออก/ถูกเลิกจ้าง และแผนกสารสนเทศต้องระงับสิทธิ์การเข้าถึงทั้งหมดอย่างทันท่วงที

5. นโยบายการจัดการการเปลี่ยนแปลง (Change Management Policy)

การเปลี่ยนแปลงระบบสารสนเทศหลัก (เช่น Oracle NetSuite) การนำโปรแกรมใหม่ขึ้นระบบจริง (Production Environment) หรือการปรับปรุงฐานข้อมูล ต้องปฏิบัติตามหลักเกณฑ์ดังนี้

- ต้องมีการร้องขอและอนุมัติเป็นลายลักษณ์อักษร หรือผ่านช่องทางอิเล็กทรอนิกส์ที่ตรวจสอบย้อนหลังได้
  - เปิด Ticket ผ่าน IT Helpdesk หรืออนุมัติทางอีเมลที่ระบุรายละเอียดอย่างชัดเจน
- ต้องมีการทดสอบใน UAT (User Acceptance Test) พร้อมหลักฐาน ก่อนนำขึ้นระบบจริง
- ต้องได้รับอนุมัติจากผู้มีอำนาจก่อนนำการเปลี่ยนแปลงขึ้นสู่ระบบจริงทุกครั้ง
- ต้องมีการสอบทานทุกครั้ง โดยผู้ร้องขอ หลังจากขึ้นใช้งานระบบจริง

6. นโยบายการสำรองข้อมูลและการกู้คืนข้อมูล (Backup and Recovery Policy)

- แผนกสารสนเทศ ต้องดำเนินการสำรองข้อมูลสำคัญขององค์กรตามกำหนดเวลาที่กำหนดไว้
- ต้องมีแผนการกู้คืนข้อมูล (Disaster Recovery Plan) และทดสอบการกู้คืนอย่างน้อยปีละ 1 ครั้ง

7. บทลงโทษ (Disciplinary Actions)

ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายฉบับนี้ อาจถูกพิจารณาลงโทษทางวินัยตามระเบียบของบริษัท และอาจถูกดำเนินคดีตามกฎหมายที่เกี่ยวข้อง หากการกระทำดังกล่าวสร้างความเสียหายแก่บริษัท พีรพัฒน์ เทคโนโลยี จำกัด (มหาชน)

ลงชื่อผู้อนุมัติ

.....

(คุณรุ่งทิพย์ มีแม่นวิทย์)

ตำแหน่ง: ประธานฝ่ายเจ้าหน้าที่บริหาร

วันที่: ...../...../.....