

บริษัท พิชแอนด์สฟว์ จำกัด (มหาชน)	เลขที่ :	PM-IT-001
	ครั้งที่ :	02
ระเบียบการปฏิบัติงาน เรื่อง นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ	วันที่เริ่มใช้ :	1 ก.ค. 2568
	หน้า :	1 / 4

ข้อมูลการเปลี่ยนแปลง

ครั้งที่	ผู้จัดทำ	วันที่	ข้อมูลที่แก้ไข/เปลี่ยนแปลง	ผู้อนุมัติ
1	นายพิทยา เอ็นนาน	1 ต.ค. 2561	ประกาศใช้ครั้งแรก	ประธานเจ้าหน้าที่บริหาร
2	นายสิริวิชญ์ อินทรวงศ์	1 ก.ค. 2568	แก้ไขรายละเอียด	

1. วัตถุประสงค์

1.1 เพื่อใช้เป็นแนวทางกำหนดมาตรการ วิธีการปฏิบัติงาน และระบบการควบคุมภายในเพื่อควบคุมการปฏิบัติงาน และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

1.2 เพื่อเป็นแนวทางปฏิบัติให้การสนับสนุนการดำเนินการด้านรักษาความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศของบริษัท เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.3 เพื่อสนับสนุนการบริหารจัดการความเสี่ยงด้านสารสนเทศ รวมถึงการป้องกัน ตรวจสอบ และตอบสนองต่อเหตุการณ์ด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

2. คำนิยาม

“บริษัท”	หมายถึง	บริษัท พิชแอนด์สฟว์ จำกัด (มหาชน)
“ระบบเทคโนโลยีสารสนเทศ”	หมายถึง	อุปกรณ์ (Hardware) หรือโปรแกรม (Software) หรือระบบ
“ฝ่ายบริหารและการจัดการ”	หมายถึง	หน่วยงานที่รับผิดชอบดูแลระบบเทคโนโลยีสารสนเทศของบริษัท และให้หมายความรวมถึงสายที่ปฏิบัติงานของเจ้าหน้าที่เทคโนโลยีสารสนเทศ
“พนักงาน”	หมายถึง	พนักงานของบริษัท ทั้งพนักงานประจำ ลูกจ้างชั่วคราว หรือพนักงานฝึกงาน และให้หมายความรวมถึงบุคคลอื่นที่บริษัทแต่งตั้งให้ปฏิบัติงานในฝ่ายบริหารและการจัดการ
“เจ้าหน้าที่เทคโนโลยีสารสนเทศ”	หมายถึง	พนักงานของบริษัทที่ปฏิบัติงานในฝ่ายบริหารและการจัดการ หรือมีหน้าที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ
“บุคคลภายนอก”	หมายถึง	บุคคลที่ไม่ใช่พนักงานของบริษัท เช่น ผู้ให้บริการ, ลูกค้า, ผู้ขายสินค้า เป็นต้น
“ผู้ให้บริการ”	หมายถึง	บุคคลภายนอกที่ให้บริการด้านเทคโนโลยีสารสนเทศ เช่น ผู้พัฒนาระบบ, ผู้ดูแลระบบ, ผู้ให้บริการระบบคลาวด์ (Cloud Provider), ผู้ให้บริการจัดการระบบ (Managed Service Provider: MSP)
“ข้อมูล”	หมายถึง	สิ่งที่สื่อความหมายให้รับรู้เรื่องราว ข้อเท็จจริง หรือเนื้อหาต่าง ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยคำพูด การเขียน หรือวิธีการอื่นใด
“หน่วยงานธุรกิจเจ้าของข้อมูล”	หมายถึง	หน่วยงานที่ก่อให้เกิดข้อมูลขึ้นในบริษัท มีความรับผิดชอบในความถูกต้องของข้อมูล และจัดเก็บข้อมูลให้เป็นปัจจุบันอยู่เสมอ จัดหาพื้นที่ดูแล และควบคุมไม่ให้เกิดการทำลายหรือเปิดเผยที่ไม่เหมาะสม รวมถึงเป็นผู้พิจารณาอนุมัติการนำข้อมูลไปใช้งาน การเก็บ และการทำลายข้อมูล ที่ตนเป็นเจ้าของ
“ผู้ดูแลระบบเทคโนโลยีสารสนเทศ”	หมายถึง	พนักงานที่ได้รับมอบหมายจากผู้บริหารสูงสุดของบริษัทให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครื่องคอมพิวเตอร์ ระบบฐานข้อมูล และทรัพยากรเทคโนโลยีสารสนเทศของบริษัท

บริษัท พีชแอนด์สืฟวี่ จำกัด (มหาชน)	เลขที่ :	PM-IT-001
	ครั้งที่ :	02
ระเบียบการปฏิบัติงาน เรื่อง นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ	วันที่เริ่มใช้ :	1 ก.ค. 2568
	หน้า :	2 / 4

2. คำนิยาม (ต่อ)

“ผู้ดูแลงาน”	หมายถึง	พนักงานของบริษัทที่ปฏิบัติงานในฝ่ายบริหารและการจัดการ และได้รับมอบหมายให้ดูแลงานบางงาน หรือโปรแกรมต่าง ๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัท
“บริการคลาวด์ (Cloud Services)”	หมายถึง	บริการด้านเทคโนโลยีสารสนเทศที่ให้โดยผู้ให้บริการผ่านอินเทอร์เน็ต เช่น บริการจัดเก็บข้อมูล (Cloud Storage), ระบบอีเมล (Cloud - Email), ระบบ ERP หรือซอฟต์แวร์อื่นในรูปแบบ SaaS
“ความมั่นคงปลอดภัยของข้อมูล”	หมายถึง	การคุ้มครองข้อมูลเพื่อให้คงไว้ซึ่ง ความลับ, ความถูกต้อง, และความพร้อมใช้งาน

3. ขอบข่าย

นโยบายฉบับนี้ให้บังคับใช้กับพนักงาน ผู้บริหารทุกระดับ ผู้ให้บริการ ที่ปรึกษา และบุคคล/นิติบุคคลที่ปฏิบัติงานที่จำเป็นซึ่งจ้างงาน ที่ได้ใช้ทรัพยากร และระบบเทคโนโลยีสารสนเทศของบริษัท ให้มีผลครอบคลุมถึง ข้อมูล และระบบเทคโนโลยีสารสนเทศทั้งปวงของบริษัท ไม่ว่าจะเป็นระบบที่ตั้งอยู่ภายในองค์กร หรืออยู่ในระบบคลาวด์ (Cloud) ของผู้ให้บริการภายนอก ทั้งนี้ ไม่รวมถึงข้อมูลทดสอบ และระบบเครื่องคอมพิวเตอร์อื่นที่ไม่ได้เชื่อมโยงกับระบบเทคโนโลยีสารสนเทศของบริษัท

4. นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security Policy)

4.1 การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

ฝ่ายบริหารและการจัดการ ต้องกำหนดโครงสร้างการบริหารจัดการระบบเทคโนโลยีสารสนเทศ โดยแยกหน้าที่ที่เกี่ยวข้องกับการพัฒนา การปฏิบัติการ และการควบคุมระบบอย่างชัดเจน พร้อมจัดให้มีระบบสอบทานและตรวจสอบความถูกต้อง เพื่อป้องกันไม่ให้เกิดความผิดพลาดหรือการกระทำใดๆ ได้โดยลำพังตลอดกระบวนการที่อาจส่งผลกระทบต่อระบบหรือข้อมูลสารสนเทศ

แนวทางปฏิบัติ

- จัดตั้งคณะทำงานรักษาความปลอดภัยข้อมูลสารสนเทศ มีหน้าที่ทบทวนนโยบาย อนุมัติกระบวนการสำคัญ และเป็นศูนย์กลางประสานงานกับหน่วยงานภายในและภายนอก
- แบ่งแยกหน้าที่ของผู้พัฒนา ผู้ใช้งาน ผู้ดูแลระบบ และผู้ตรวจสอบ เพื่อป้องกันผลประโยชน์ทับซ้อน
- กำหนดมาตรการตรวจสอบ เช่น การจัดเก็บ log และการตรวจสอบเป็นระยะ

อ้างอิงมาตรฐาน ISO/IEC 27001:2022

- 6.1.1, 6.1.2, 6.1.8, 10.1.3, 10.6.1, 14.1.1

4.2 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และการป้องกันความเสียหาย (Physical Security)

ต้องจัดให้มีระบบรักษาความปลอดภัยทางกายภาพและอุปกรณ์ต่างๆ เพื่อควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ ป้องกันการบุกรุก และภัยพิบัติจากภายนอก เช่น อัคคีภัย หรือไฟฟ้าขัดข้อง

แนวทางปฏิบัติ

- จำกัดสิทธิ์การเข้าถึงเฉพาะผู้มีอำนาจ พร้อมบันทึกการเข้าออก
- ติดตั้งอุปกรณ์ป้องกัน เช่น สัญญาณเตือนภัย เครื่องตรวจจับควัน และระบบ UPS

อ้างอิง ISO/IEC 27001:2022

- 9.1.1, 9.1.5, 9.2.1, 9.2.2

4.3 การรักษาความปลอดภัยของระบบงานและเครือข่าย (Information System and Network Security)

ต้องมีมาตรการควบคุมการเข้าถึงระบบและข้อมูลเฉพาะสำหรับผู้มีหน้าที่ รวมถึงการป้องกันจากภัยคุกคามภายนอก เช่น มัลแวร์ หรือการเจาะระบบ

บริษัท พิชแอนด์สฟว์ จำกัด (มหาชน)	เลขที่ :	PM-IT-001
	ครั้งที่ :	02
ระเบียบการปฏิบัติงาน เรื่อง นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ	วันที่เริ่มใช้ :	1 ก.ค. 2568
	หน้า :	3 / 4

แนวทางปฏิบัติ

- แยกหน้าที่ของผู้ดูแลระบบ ผู้ใช้งาน และผู้บันทึกข้อมูล
- ใช้ระบบบัญชีผู้ใช้เฉพาะบุคคล พร้อมการจัดสิทธิ์ตามบทบาทงาน
- ติดตั้ง Firewall และควบคุมการเชื่อมต่อระบบภายนอก

อ้างอิง ISO/IEC 27001:2022

- 10.1.3, 11.1.1, 11.2.1, 11.3.1, 11.4.1, 11.4.2, 12.2.3, 11.6.1, 11.6.2

4.4 การควบคุมการพัฒนาและเปลี่ยนแปลงระบบงาน (Development and Change Management)

การพัฒนาหรือปรับปรุงระบบงานต้องอยู่ภายใต้กระบวนการควบคุมที่เหมาะสม มีการตรวจสอบความถูกต้อง และการอนุมัติก่อนนำไปใช้งานจริง

แนวทางปฏิบัติ

- คัดเลือกผู้พัฒนาโดยคำนึงถึงความปลอดภัยและความเชี่ยวชาญ
- มีเอกสารคู่มือ ทดสอบระบบ และการฝึกอบรมผู้ใช้
- มีการควบคุมเวอร์ชันของโปรแกรม และเก็บรักษา Source Code อย่างปลอดภัย

อ้างอิง ISO/IEC 27001:2022

- 10.1.4, 10.3.2, 12.1.1, 12.2.1, 12.2.2, 12.4.1, 12.4.3, 12.5.1, 12.5.3

4.5 การสำรองข้อมูลและการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity)

ระบบต้องมีการสำรองข้อมูลอย่างสม่ำเสมอ และมีแผนรองรับกรณีเกิดเหตุการณ์ไม่คาดคิด เช่น ไฟฟ้าดับ ระบบล่ม หรือภัยพิบัติ

แนวทางปฏิบัติ:

- สำรองข้อมูลตามรอบระยะเวลา พร้อมตรวจสอบการกู้คืนข้อมูลปีละอย่างน้อย 1 ครั้ง
- จัดทำคู่มือและแผนฉุกเฉิน โดยระบุขั้นตอนกู้ระบบกลับมาใช้งานได้

อ้างอิง ISO/IEC 27001:2022

- 10.5.1, 14.1.3, 14.1.4

4.6 การควบคุมการปฏิบัติงานด้าน IT (Computer Operation Control)

การปฏิบัติงานประจำวันด้าน IT ต้องมีแนวทางการดำเนินการที่ชัดเจน พร้อมบันทึกขั้นตอน และวิธีการแก้ไขปัญหา เพื่อให้การประมวลผลข้อมูลมีความถูกต้องและต่อเนื่อง

แนวทางปฏิบัติ

- จัดทำคู่มือปฏิบัติงาน เช่น Operation Manual และวิธีการจัดการเหตุผิดปกติ

อ้างอิง ISO/IEC 27001:2022

- 10.1.1, 12.2.2

4.7 การควบคุมผู้ให้บริการภายนอก (IT Outsourcing)

การใช้บริการจากผู้ให้บริการภายนอกต้องอยู่ภายใต้สัญญาและการควบคุมที่รัดกุม เพื่อให้แน่ใจว่างานที่ดำเนินการมีความมั่นคงปลอดภัย

แนวทางปฏิบัติ

- ตรวจสอบคุณสมบัติของผู้ให้บริการให้รอบคอบก่อนเลือกใช้
- กำหนดสิทธิ์เข้าถึงเฉพาะในระบบที่จำเป็น และอยู่ภายใต้การควบคุมอย่างใกล้ชิด

อ้างอิง ISO/IEC 27001:2022

- 10.1.4

4.8 การปฏิบัติตามกฎหมายและข้อกำหนด (Compliance)

ระบบและการดำเนินการด้าน IT ต้องไม่ขัดต่อกฎหมาย ข้อบังคับ หรือสัญญาที่เกี่ยวข้อง

แนวทางปฏิบัติ

- ปฏิบัติตาม พ.ร.บ. คอมพิวเตอร์ฯ, พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และข้อบังคับภายในบริษัท

บริษัท พีชแอนด์สฟว์ จำกัด (มหาชน)	เลขที่ :	PM-IT-001
	ครั้งที่ :	02
ระเบียบการปฏิบัติงาน เรื่อง นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ	วันที่เริ่มใช้ :	1 ก.ค. 2568
	หน้า :	4 / 4

4.9 การรักษาความปลอดภัยด้านบุคลากร (Personnel Security)

พนักงานต้องได้รับการอบรม ให้ความรู้ และมีความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง
แนวทางปฏิบัติ

- อบรมพนักงานใหม่ และอบรมประจำปีด้าน IT Security
- มีกระบวนการตรวจสอบการกระทำผิด และบทลงโทษหากฝ่าฝืนนโยบาย

อ้างอิง ISO/IEC 27001:2022

- 8.1.1, 8.1.3, 8.2.2, 8.2.3, 15.1.5

5. บทลงโทษ

การกระทำใดๆ ที่เข้าข่ายละเมิด ฝ่าฝืน หรือละเว้นไม่ปฏิบัติตามนโยบายฉบับนี้ รวมถึงขั้นตอนหรือวิธีปฏิบัติที่จัดทำขึ้น
เพื่อรองรับนโยบายฉบับนี้ ถือว่ามีความผิดทางวินัย และจะถูกลงโทษตามระเบียบของบริษัท

6. บันทึกคุณภาพ

- SOP-IT-001: การขอรับบริการงานเทคโนโลยีสารสนเทศ
- SOP-IT-005: แผนการตรวจสอบระบบทำงานของระบบเทคโนโลยีสารสนเทศ
- SOP-IT-006: แผนการทดสอบและทวนสอบข้อมูลระบบเทคโนโลยีสารสนเทศ
- SOP-IT-011: รายงานระบบสารสนเทศประจำปี