บริษัท ฟลอยด์ จำกัด (มหาชน)

นโยบายรักษาความปลอดภัยสารสนเทศ

Information Security Policy

อนุมัติโดยคณะกรรมการบริษัท ครั้งที่ 4/2568 วันที่ 12 พฤศจิกายน 2568
ประกาศและให้มีผลบังคับใช้ตั้งแต่วันที่ 17 พฤศจิกายน 2568 เป็นต้นไป

https://www.floyd.co.th

บันทึกการเปลี่ยนแปลง

Version No.	วันที่	ผู้ทำการเปลี่ยนแปลง	รายละเอียด	สถานะเอกสาร
Draft V.01	01-09-14	FLOYD	จัดทำร่างนโยบายรักษาความปลอดภัยสารสนเทศ	Draft
Draft V.02	13-10-15	FLOYD	แก้ไขชื่อตำแหน่งตามโครงสร้างองค์กร	Draft
01	01-01-15	FLOYD	นโยบายรักษาความปลอดภัยสารสนเทศ	Cancelled
02	01-04-16	FLOYD	แก้ไขชื่อบริษัท	Cancelled
03	15-05-20	FLOYD	ทบทวนประจำปี 2563 และปรับปรุง/แก้ไข ● คำจำกัดความ - คณะกรรมการบริหาร, - กรรมการผู้จัดการ ● หมวดที่ 1 ข้อกำหนดทั่วไป ข้อ 2 ● หมวดที่ 4 นโยบายการบริหารจัดการรหัสผ่าน ข้อ 11	Cancelled
04	01-03-21	FLOYD	ทบทวนประจำปี 2564 และปรับปรุง/แก้ไข ● หมวดที่ 1 ข้อกำหนดทั่วไป ข้อ 1 หน้าที่ 7 ● หมวดที่ 3 นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ ข้อ 13 หน้าที่ 9	Cancelled
05	15-08-23	FLOYD	ทบทวนประจำปี 2566 และปรับปรุง/แก้ไข ● เพิ่มหมวดที่ 14 นโยบายการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ● เพิ่มหมวดที่ 15 นโยบายการควบคุมการเข้ารหัสข้อมูล (Data Encryption Control)	Cancelled
06	15-11-24	FLOYD	ทบทวนนโยบายรักษาความปลอดภัยสารสนเทศประจำปี 2567	Cancelled
07	17-11-25	FLOYD	ทบทวนนโยบายรักษาความปลอดภัยสารสนเทศประจำปี 2568	Final

ข้อกำหนดและข้อตกลง

ข้อมูลและ/หรือสารสนเทศภายใต้เอกสารฉบับนี้เป็นความลับของบริษัทฯ และเป็นเอกสารสำหรับใช้ภายในองค์กรเท่านั้น ดังนั้น ห้ามเจ้าหน้าที่บริษัทฯ ทำซ้ำหรือเปิดเผยส่วนใดของข้อมูลและ/หรือสารสนเทศภายใต้เอกสารฉบับนี้ให้แก่บุคคลหรือหน่วยงานภายนอก การฝ่าฝืนจะนำไปสู่การลงโทษทางวินัย ซึ่งรวมถึงการให้ออกจากงาน

นโยบายรักษาความปลอดภัยสารสนเทศ

(Information Security Policy)

1. บทนำ

บริษัท ฟลอยด์ จำกัด (มหาชน) ("บริษัทฯ") ได้จัดให้มีการกำหนดนโยบายรักษาความปลอดภัยสารสนเทศเพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทฯ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และ/หรือการถูกคุมคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่บริษัทฯ บริษัทฯ จึงได้จัดทำนโยบายรักษาความปลอดภัยสารสนเทศขึ้นใช้ในบริษัทฯ โดยอ้างอิงมาตรฐาน ISO/IEC 27001 Annex A. และเพื่อใช้เป็นแนวปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

นโยบายรักษาความปลอดภัยสารสนเทศฉบับนี้ ประกอบด้วยหมวดต่าง ๆ ทั้งสิ้น 13 หมวดดังต่อไปนี้

- หมวดที่ 1 ข้อกำหนดทั่วไป
- หมวดที่ 2 นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
- หมวดที่ 3 นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control)
- หมวดที่ 4 นโยบายการบริหารจัดการรหัสผ่าน (Password Control)
- หมวดที่ 5 นโยบายการเข้าถึงระบบเครือข่ายและคอมพิวเตอร์ (Network Access Control)
- หมวดที่ 6 นโยบายการควบคุมการเข้าถึงระบบเครือข่ายชนิดไร้สาย (Wireless Access Control)
- หมวดที่ 7 นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computing)
- หมวดที่ 8 นโยบายการใช้งานอินเตอร์เน็ต (Internet Usage)
- หมวดที่ 9 นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail Usage)
- หมวดที่ 10 นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Malicious Code Protection)
- หมวดที่ 11 นโยบายการสำรองและกู้คืนข้อมูล (Backup System and Recovery)
- หมวดที่ 12 นโยบายการบริหารจัดการการเปลี่ยนแปลงแก้ไขระบบ (Change Management)
- หมวดที่ 13 นโยบายการปฏิบัติตามข้อบังคับ (Regulatory Requirement)
- หมวดที่ 14 นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Personal data protection : PDPA)
- หมวดที่ 15 นโยบายการควบคุมการเข้ารหัสข้อมูล (Data Encryption Control)

2. วัตถุประสงค์

วัตถุประสงค์ของนโยบายรักษาความปลอดภัยสารสนเทศฉบับนี้ มีดังต่อไปนี้

1. เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือ เครือข่ายคอมพิวเตอร์ของบริษัทฯ ทำให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ

2. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในบริษัทฯ ได้รับทราบ และเจ้าหน้าที่บริษัททุกคนต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
3. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่บริษัท เจ้าหน้าที่สารสนเทศ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศสำหรับการดำเนินงาน

3. ขอบเขต

ขอบเขตของนโยบายรักษาความปลอดภัยสารสนเทศครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยของสารสนเทศของบริษัทฯ ทั้งที่อยู่ในสถานที่ปฏิบัติงานของบริษัทฯ หรือภายนอกบริษัทฯ โดยครอบคลุมถึงเจ้าหน้าที่บุคคล และหน่วยงานภายนอกที่ได้รับสิทธิในการเข้าถึงทรัพย์สินที่เกี่ยวข้องกับสารสนเทศของบริษัทฯ

4. คำจำกัดความ

คำ	คำจำกัดความ
บริษัทฯ	บริษัท ฟลอยด์ จำกัด (มหาชน)
คณะกรรมการบริหาร	คณะกรรมการซึ่งประกอบด้วยผู้บริหารระดับสูงที่ได้รับแต่งตั้งจากคณะกรรมการบริษัท มีอำนาจในการตัดสินใจสูงสุด และมีหน้าที่ในการบริหารงานต่าง ๆ ของบริษัทฯ
กรรมการผู้จัดการ (MD)	ผู้ที่มีหน้าที่ในการบริหารงานต่าง ๆ ของบริษัทฯ ให้เป็นไปตามคู่มืออำนาจดำเนินการที่บริษัทฯ กำหนด รวมถึงตามที่ได้รับมอบหมายจากคณะกรรมการบริษัทและ/หรือคณะกรรมการบริหาร
เจ้าหน้าที่สารสนเทศ (System Administrator)	เจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าสายงานให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
เจ้าหน้าที่บริษัท	เจ้าหน้าที่ของบริษัท รวมถึงบุคคลอื่นที่บริษัทฯ มอบหมายให้ปฏิบัติงานตามสัญญาหรือข้อตกลง
หน่วยงานภายนอก	หน่วยงานภายนอกที่บริษัทฯ อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของบริษัทฯ โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
ผู้ใช้งาน	ผู้บริหาร เจ้าหน้าที่สารสนเทศ เจ้าหน้าที่บริษัท หรือเจ้าหน้าที่จากหน่วยงานภายนอกที่ได้รับอนุญาตในการเข้าถึงข้อมูล และ/หรือ ระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ

คำ	คำจำกัดความ
ระบบคอมพิวเตอร์	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
ระบบเครือข่าย (Network System)	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัทฯ ได้ เช่น ระบบ LAN ระบบ Intranetระบบ Internet เป็นต้น - ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในบริษัทฯ - ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก
เจ้าของข้อมูล	ผู้ได้รับมอบอำนาจจากผู้บริหารให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
สินทรัพย์	ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
ซอฟต์แวร์ (Software)	ซอฟต์แวร์แอพพลิเคชั่น (Application Software) ซอฟต์แวร์ระบบปฏิบัติการคอมพิวเตอร์ (Operating System Software) เครื่องมือในการพัฒนาระบบงาน (Development Tool) และโปรแกรมอรรถประโยชน์ (Utility)
ฮาร์ดแวร์ (Hardware)	เครื่องคอมพิวเตอร์และอุปกรณ์รอบข้างที่สามารถสัมผัสได้ โดยจะประกอบด้วยอุปกรณ์ทางด้านอิเล็กทรอนิกส์ที่ควบคุมการประมวลผลข้อมูล การรับข้อมูลการแสดงผลข้อมูลของเครื่องคอมพิวเตอร์ มีทั้งที่ติดตั้งภายในเครื่องคอมพิวเตอร์และเชื่อมต่อภายนอกเครื่องคอมพิวเตอร์
จดหมายอิเล็กทรอนิกส์ (E-mail)	ระบบที่เจ้าหน้าที่บริษัทใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน
รหัสผ่าน (Password)	ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
ชุดคำสั่งไม่พึงประสงค์	ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
เหตุการณ์ด้านความมั่นคงปลอดภัย	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

5. นโยบายรักษาความปลอดภัยสารสนเทศ

หมวดที่ 1	**ข้อกำหนดทั่วไป**
วัตถุประสงค์	เพื่อกำหนดเป็นมาตรฐานสำหรับนโยบายรักษาความปลอดภัยสารสนเทศ

1. นโยบายรักษาความปลอดภัยสารสนเทศ ประกอบด้วยนโยบายหมวดต่าง ๆ ทั้ง 15 หมวดนี้
   - หมวดที่ 1 ข้อกำหนดทั่วไป
   - หมวดที่ 2 นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
   - หมวดที่ 3 นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control)
   - หมวดที่ 4 นโยบายการบริหารจัดการรหัสผ่าน (Password Control)
   - หมวดที่ 5 นโยบายการเข้าถึงระบบเครือข่ายและคอมพิวเตอร์ (Network Access Control)
   - หมวดที่ 6 นโยบายการควบคุมการเข้าถึงระบบเครือข่ายชนิดไร้สาย (Wireless Access Control)
   - หมวดที่ 7 นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computing)
   - หมวดที่ 8 นโยบายการใช้งานอินเตอร์เน็ต (Internet Usage)
   - หมวดที่ 9 นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail Usage)
   - หมวดที่ 10 นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Malicious Code Protection)
   - หมวดที่ 11 นโยบายการสำรองและกู้คืนข้อมูล (Backup System and Recovery)
   - หมวดที่ 12 นโยบายการบริหารจัดการการเปลี่ยนแปลงแก้ไขระบบ (Change Management)
   - หมวดที่ 13 นโยบายการปฏิบัติตามข้อบังคับ (Regulatory Requirement)
   - หมวดที่ 14 นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection : PDPA)
   - หมวดที่ 15 นโยบายการควบคุมการเข้ารหัสข้อมูล (Data Encryption Control)

ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายฯ ทุกปีอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ที่กระทบต่อนโยบายฉบับนี้

2. นโยบายฯ ฉบับนี้ต้องได้รับความเห็นชอบจาก **คณะกรรมการบริหาร** และได้รับการอนุมัติจาก **คณะกรรมการบริษัท** ก่อนที่จะมีการประกาศใช้ และจะต้องมีการลงลายมือชื่ออย่างเป็นลายลักษณ์อักษร
3. บริษัทฯ ต้องกำหนดให้มี “เจ้าหน้าที่สารสนเทศ” ที่สามารถดูแลรับผิดชอบ แก้ไขปัญหา ติดต่อประสานงานกับหน่วยงานภายนอก เพื่อบริหารจัดการระบบเครือข่ายและคอมพิวเตอร์ที่บริษัทฯ ใช้งานอยู่ได้

หมวดที่ 2	**นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม**
วัตถุประสงค์	เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยของการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเครือข่ายและคอมพิวเตอร์

1. บริษัทฯ ต้องมีการกำหนดขอบเขตพื้นที่รักษาความปลอดภัย เช่น จัดทำกำแพง บัตรผ่านประตู หรือจัดให้มีเจ้าหน้าที่บริษัทเพื่อทำการต้อนรับ และป้องกันการเข้าถึงบริเวณที่มีระบบอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ
2. บริษัทฯ ต้องจัดให้มีการควบคุมการเข้าถึงทางกายภาพอย่างเหมาะสมสำหรับศูนย์คอมพิวเตอร์ เช่น จัดทำประตูเข้า–ออก และให้มีการล็อคกุญแจทุกครั้งหากไม่มีการใช้งาน
3. บริษัทฯ ต้องกำหนดบุคคลที่ได้รับอนุญาตในการเข้าถึงศูนย์คอมพิวเตอร์ไว้เป็นลายลักษณ์อักษร พร้อมทั้งรายชื่อดังกล่าวต้องได้รับการอนุมัติจากผู้บริหาร อีกทั้งต้องมีการปรับปรุงรายชื่อและทำการอนุมัติใหม่ทุกครั้งที่มีการเปลี่ยนแปลง
4. ระบบและอุปกรณ์สนับสนุนการทำงานหลักที่อยู่ในสภาพแวดล้อมที่ใช้งานจริง (รวมถึง เครื่องแม่ข่ายไฟร์วอลล์ อับเราเตอร์ ระบบจดหมายอิเล็กทรอนิกส์ และอื่น ๆ) ต้องถูกจัดวางภายในศูนย์คอมพิวเตอร์อย่างเหมาะสม
5. บริษัทฯ ต้องจัดให้มีการเก็บบันทึกข้อมูลการเข้าออกศูนย์คอมพิวเตอร์ ทั้งเจ้าหน้าที่สารสนเทศ เจ้าหน้าที่บริษัท และเจ้าหน้าที่จากหน่วยงานภายนอก ลงใน Visitor Log Book โดยจะต้องบันทึกรายละเอียดของผู้เข้าออก และเวลาเข้าออก และให้มีการตรวจสอบอย่างสม่ำเสมอ
6. บริษัทฯ ต้องจัดให้มีการป้องกันความเสียหายสำหรับระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ อย่างเหมาะสม ได้แก่
   - **ระบบไฟฟ้า**
     - บริษัทฯ ต้องจัดให้มีเครื่องสำรองไฟสำหรับระบบคอมพิวเตอร์และเครือข่ายเพื่อให้การดำเนินงานมีความต่อเนื่อง และรวมไปถึงการป้องกันความเสียหายเมื่อมีกระแสไฟไม่คงที่
   - **ระบบป้องกันไฟไหม้**
     - บริษัทฯ ต้องติดตั้งอุปกรณ์เตือนภัยในกรณีที่เกิดไฟไหม้ เช่น เครื่องดักจับควัน เครื่องตรวจจับความร้อน และสัญญาณเตือนภัย เป็นต้น
     - บริษัทฯ ต้องทำการติดตั้งอุปกรณ์ดับเพลิงภายในศูนย์คอมพิวเตอร์
   - **ระบบควบคุมอุณหภูมิและความชื้น**
     - บริษัทฯ ต้องทำการติดตั้งระบบควบคุมอุณหภูมิและความชื้นให้เหมาะกับระบบและอุปกรณ์คอมพิวเตอร์
     - บริษัทฯ ควรตรวจสอบอุณหภูมิและความชื้นในศูนย์คอมพิวเตอร์อย่างสม่ำเสมอ
   - **ระบบป้องกันน้ำรั่วซึม**
     - บริษัทฯ ต้องทำการติดตั้งระบบป้องกันการรั่วซึมของน้ำที่อาจจะเกิดขึ้นจากการใช้งานเครื่องปรับอากาศ หรือฝ้า เพดาน รั่วซึม

หมวดที่ 3	**นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ**
วัตถุประสงค์	เพื่อกำหนดเป็นมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้ไม่ประสงค์ดี หรือโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก

1. เจ้าหน้าที่สารสนเทศ ที่ได้รับมอบหมายจากกรรมการผู้จัดการ ต้องกำหนดสิทธิ์ในการเข้าถึงข้อมูลระบบเครือข่ายและคอมพิวเตอร์ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่บริษัทในการปฏิบัติงาน
2. กรรมการผู้จัดการ เจ้าหน้าที่สารสนเทศ และผู้เป็นเจ้าของข้อมูล ต้องร่วมกันจัดทำตารางสิทธิเพื่อควบคุมการเข้าถึง (Access Control Matrix) โดยแบ่งแยกเป็นกลุ่มของผู้ใช้งานต่าง ๆ และระดับสิทธิ พร้อมทั้งรายละเอียดของสิทธินั้น ๆ ที่สามารถเข้าถึงระบบและข้อมูลในแต่ละระดับ เพื่อเป็นมาตรฐานในการกำหนดสิทธิในการเข้าถึงข้อมูลและระบบงาน และต้องให้มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอและอย่างน้อยปีละ 1 ครั้ง
3. บริษัทฯ ต้องมีการจัดทำขั้นตอนการปฏิบัติงานเพื่อบริหารจัดการบัญชีรายชื่อ รหัสผ่านในการเข้าถึงระบบและข้อมูล โดยต้องปรับปรุงให้มีความเป็นปัจจุบันอยู่เสมอ
4. บริษัทฯ ต้องจัดทำมาตรฐานในการตั้งรหัสผู้ใช้งาน ที่สามารถระบุตัวตนของผู้ใช้งานได้อย่างง่าย และต้องไม่บ่งบอกถึงสิทธิที่ได้รับ
5. ห้ามให้มีการใช้งานรหัสผู้ใช้งานซ้ำกัน และหรือ ร่วมกัน ระหว่างผู้ใช้งาน
6. ผู้ใช้งานมีหน้าที่ความรับผิดชอบต่อรหัสผู้ใช้งานของตน รวมไปถึงกิจกรรมที่เกิดขึ้นต่อระบบและข้อมูลอันเกิดจากรหัสผู้ใช้งานของตน
7. ห้ามเปิดเผยบัญชีผู้ใช้งานให้กับบุคคลภายนอกหรือบุคคลที่ไม่เกี่ยวข้องกับบริษัทฯ
8. ระบบต้องระงับการใช้งาน รหัสผู้ใช้งาน ที่พยายามเข้าสู่ระบบแต่ไม่สำเร็จติดต่อกันเกิน 5 ครั้ง
9. เมื่อผู้ใช้งานโยกย้ายตำแหน่งงานในบริษัท เจ้าหน้าที่สารสนเทศต้องทำการเปลี่ยนแปลงสิทธิของผู้ใช้งานในการเข้าถึงข้อมูลและระบบเครือข่ายและคอมพิวเตอร์ให้มีความเหมาะสม
10. เมื่อผู้ใช้งานลาออกหรือถูกสั่งให้มีการพักงาน หรือถูกให้ออกจากบริษัทฯ เจ้าหน้าที่สารสนเทศต้องทำการระงับการใช้งานรหัสผู้ใช้งานทันที
11. รหัสผู้ใช้งาน สำหรับเจ้าหน้าที่จากหน่วยงานภายนอก ต้องถูกระงับการใช้งานทุกครั้ง เมื่อมีการใช้งานเสร็จสิ้น
12. รหัสผู้ใช้งานสูงสุด (Privilege User Account) ต้องถูกจัดเก็บอย่างปลอดภัย และหากมีความจำเป็นต้องใช้งานรหัสผู้ใช้งานสูงสุดต้องมีการขออนุมัติทุกครั้งเป็นลายลักษณ์อักษร และต้องได้รับการอนุมัติจากกรรมการผู้จัดการ ผู้เป็นเจ้าของข้อมูล หรือเจ้าของระบบเท่านั้น พร้อมทั้งต้องมีการจดบันทึกการใช้งาน ทุกครั้ง
13. บริษัทฯ ต้องมีการทบทวนรหัสผู้ใช้งาน และสิทธิในการเข้าถึงระบบเครือข่ายและคอมพิวเตอร์อยู่เป็นประจำ อย่างน้อยปีละครั้งหรือทุกครั้งเมื่อมีการเปลี่ยนแปลงที่สำคัญ

หมวดที่ 4	**นโยบายการบริหารจัดการรหัสผ่าน**
วัตถุประสงค์	เพื่อกำหนดมาตรฐานในการใช้งานรหัสผ่าน สำหรับผู้ใช้งานระบบเครือข่ายและคอมพิวเตอร์ในบริษัทฯ เพื่อให้การใช้งานรหัสผ่านเป็นไปอย่างปลอดภัย รัดกุม ยากต่อการคาดเดา

1. รหัสผ่านควรมีความยาวอย่างน้อย 6 ตัวอักษรสำหรับเจ้าหน้าที่บริษัทที่ได้รับสิทธิปกติ (Regular Users)
2. รหัสผ่านควรมีความยาวอย่างน้อย 10 ตัวอักษรสำหรับเจ้าหน้าที่บริษัทที่ได้รับสิทธิพิเศษ (Privileged Users)
3. รหัสผ่านต้องประกอบด้วยตัวอักษร (a-Z) ตัวเลข (0-9) เป็นต้น
4. รหัสผ่านต้องไม่มีตัวอักษรที่ซ้ำ ๆ กัน เช่น “AAABBB” หรือเป็นตัวอักษรที่เรียงต่อกันตามลำดับของ Keyboard เช่น “ASDFGH” เป็นต้น และต้องไม่เรียงตามลำดับตัวอักษร หรือตัวเลข เช่น “ABCDE”, “12345” เป็นต้น
5. รหัสผ่านต้องไม่มีความเกี่ยวข้องกับเจ้าหน้าที่บริษัทงาน เช่น ชื่อ ชื่อเล่น หรือที่อยู่
6. รหัสผ่านต้องไม่ซ้ำบัญชีรายชื่อผู้ใช้ระบบงาน (User ID)
7. รหัสผ่านต้องไม่เป็นคำที่มีอยู่ในพจนานุกรม
8. เมื่อมีการเปลี่ยนแปลงรหัสผ่านต้องไม่ทำการเปลี่ยนรหัสผ่านโดยการใช้รหัสเดิม (Recycle Password)
9. ต้องไม่กำหนดรหัสผ่านเป็นค่าว่าง (Blank Password)
10. เมื่อได้รับรหัสผ่าน ต้องกำหนดให้มีการเปลี่ยนรหัสผ่านเมื่อมีการใช้งานเป็นครั้งแรก
11. ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านทุก 90 วัน
12. ไฟล์ที่เก็บรหัสผ่านต้องทำการเข้ารหัส

หมวดที่ 5	**นโยบายการเข้าถึงระบบเครือข่ายและคอมพิวเตอร์**
วัตถุประสงค์	เพื่อป้องกันการเข้าถึง ระบบเครือข่ายและคอมพิวเตอร์ อย่างไม่ได้รับอนุญาต และเพื่อให้ระบบเครือข่ายมีความปลอดภัย เชื่อถือได้ และมีประสิทธิภาพ ในการให้บริการ

1. บริษัทฯ ต้องจัดแบ่งเครือข่ายภายใน และเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบเครือข่ายและคอมพิวเตอร์ และต้องทำการติดตั้ง Firewall เพื่อป้องกันการเข้าถึงเครือข่ายจากผู้ไม่ประสงค์ดี
2. จัดทำแผนผังการเชื่อมต่อระบบเครือข่าย (Network Diagram) ซึ่งระบุถึงรายละเอียดของเครือข่ายภายในบริษัทฯ และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
3. การเข้าถึง หรือ การเชื่อมต่ออุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และอุปกรณ์สื่อสารใด ๆ รวมไปถึงการเปลี่ยนแปลงใด ๆ ก็ตามที่มีผลกระทบต่อระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ ต้องได้รับอนุมัติอย่างเป็นทางการจากกรรมการผู้จัดการ หรือผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบระบบเครือข่ายและคอมพิวเตอร์ก่อนที่สามารถดำเนินการได้ในทุกกรณี
4. สำหรับผู้ใช้งานที่อยู่ภายในบริษัทฯ การเชื่อมต่อเครือข่ายภายในบริษัทฯ ต้องเชื่อมต่อผ่านทางช่องทางที่บริษัทฯ จัดหาให้เท่านั้น
5. การเชื่อมต่อทางเครือข่าย และการกำหนดเส้นทางจราจรบนระบบเครือข่าย ต้องสามารถควบคุมได้ ได้แก่ การควบคุมผ่าน IP-Routing หรือ Firewall Policy
6. ห้ามเปิดเผยข้อมูลเกี่ยวกับค่าติดตั้งหรือช่องโหว่ของระบบเครือข่าย รวมถึงข้อมูลที่มีความสำคัญของระบบเครือข่ายแก่บุคคลที่ไม่เกี่ยวข้องกับบริษัทฯ
7. การส่งรับข้อมูลที่มีความสำคัญหรือเป็นความลับผ่านระบบเครือข่ายและคอมพิวเตอร์ ควรได้รับการเข้ารหัสที่เป็นมาตรฐานสากล
8. การเชื่อมต่อใด ๆ ที่ไม่ได้ใช้งาน หรือไม่มีความจำเป็นต้องถูกระงับ หรือปิดการใช้งาน
9. บริษัทฯ ต้องจัดเก็บข้อมูลจราจรของอุปกรณ์ที่ใช้งานบนระบบเครือข่ายและคอมพิวเตอร์อย่างต่อเนื่องไม่น้อยกว่า 90 วัน
10. การเข้าถึงระบบจัดเก็บข้อมูลจราจรบนระบบเครือข่ายต้องเป็นไปอย่างรัดกุม ปลอดภัย และเข้าถึงได้เฉพาะผู้มีสิทธิเท่านั้น
11. การเข้าถึงหรือเชื่อมต่อระบบเครือข่ายและคอมพิวเตอร์ของบริษัทฯ จากบริเวณที่อนุญาตการเข้าถึงจากระยะไกล (Remote Access) ต้องต่อผ่านอุปกรณ์ Firewall เท่านั้น และการเชื่อมต่อนั้นต้องมีการเข้ารหัส เช่น มาตรฐาน SSL หรือมาตรฐาน IPSec VPN และต้องจัดให้มีการจัดเก็บการใช้งานทุกครั้ง
12. การใช้เครื่องมือในการดักจับข้อมูลบนระบบเครือข่ายและคอมพิวเตอร์ และ/หรือ เครื่องมือเพื่อประเมินช่องโหว่ และตรวจสอบระบบเครือข่าย ต้องได้รับความเห็นชอบอย่างเป็นทางการจากกรรมการผู้จัดการของบริษัทฯ เท่านั้น
13. เครื่องแม่ข่ายที่ใช้สำหรับระบบงานสำคัญของบริษัทฯ ต้องทำการปิดการเชื่อมต่อที่ไม่ได้ใช้งาน (Disable Port) และควรทำการ Hardening OS หากเป็นไปได้ รวมถึงต้องมีการปรับปรุง Patch สำหรับระบบปฏิบัติการให้เป็นปัจจุบันอยู่เสมอ
14. บริษัทฯ ควรทำการแยกระบบสำหรับการปฏิบัติงานจริง และระบบที่ใช้ในการทดสอบออกจากกัน

หมวดที่ 6	**นโยบายการควบคุมการเข้าถึงระบบเครือข่ายชนิดไร้สาย**
วัตถุประสงค์	เพื่อกำหนดมาตรฐานในการใช้งาน และติดตั้งระบบเครือข่ายชนิดไร้สายสำหรับเชื่อมต่อกับเครือข่ายภายในบริษัทฯ

1. การติดตั้งระบบเครือข่ายแบบไร้สาย เพื่อใช้งานในบริษัทฯ ต้องผ่านการเห็นชอบ และอนุมัติจากกรรมการผู้จัดการเท่านั้น อีกทั้งการติดตั้งระบบต้องดำเนินการโดยเจ้าหน้าที่บริษัทที่มีความรู้ ความสามารถในการติดตั้งระบบเท่านั้น
2. ควรติดตั้งระบบเครือข่ายแบบไร้สาย หลังอุปกรณ์ Firewall เพื่อป้องกันการโจมตีจากบุคคล หรือโปรแกรมที่ไม่ประสงค์ดี
3. ห้ามเจ้าหน้าที่บริษัททำการติดตั้งเครือข่ายแบบไร้สาย ซึ่งหมายรวมถึงทั้ง Wireless Router, Access Point ด้วยตนเอง หรือเปิดใช้งานเครือข่ายแบบไร้สายที่โทรศัพท์ หากมีการปฏิบัติงานอยู่ในบริษัทฯ
4. เจ้าหน้าที่สารสนเทศ ต้องทำการบันทึก หมายเลขประจำเครื่อง (MAC Address) ไว้ที่อุปกรณ์เครือข่ายไร้สาย เพื่อเป็นการกำหนดให้เฉพาะเครื่องคอมพิวเตอร์ที่ได้รับอนุญาตเท่านั้นที่สามารถใช้งานเครือข่ายไร้สายได้
5. การเข้าถึงระบบเครือข่ายไร้สาย หรือใช้งานระบบเครือข่ายไร้สาย ต้องผ่านการพิสูจน์ตัวตนเสมอ
6. การกำหนดชื่อเครื่องสำหรับอุปกรณ์เครือข่ายไร้สาย (SSID) ไม่ควรกำหนดให้สามารถระบุถึงตำแหน่งที่ตั้ง หรือบริการที่เปิดใช้งานได้ อีกทั้งไม่ควรใช้งาน SSID ที่มาพร้อมกับอุปกรณ์ไร้สาย
7. ต้องกำหนดให้มีมาตรฐานการเข้ารหัส (เช่น WEP, WPA2, AES เป็นต้น) ระหว่างอุปกรณ์ไร้สาย และอุปกรณ์เชื่อมต่อให้มีความปลอดภัยสูงสุดตามที่อุปกรณ์นั้น ๆ สามารถรองรับได้ และต้องมีการปรับปรุงให้เป็นปัจจุบัน

หมวดที่ 7	**นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล**
วัตถุประสงค์	เพื่อกำหนดมาตรฐานในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลสำหรับบริษัทฯ ซึ่งหมายรวมถึงคอมพิวเตอร์ส่วนบุคคลแบบตั้งโต๊ะ และคอมพิวเตอร์ส่วนบุคคลแบบพกพา ให้เจ้าหน้าที่บริษัทได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเจ้าหน้าที่บริษัทควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด

1. เครื่องคอมพิวเตอร์ที่บริษัทฯ อนุญาตให้เจ้าหน้าที่บริษัทใช้งานเป็นทรัพย์สินของบริษัทฯ ดังนั้น เจ้าหน้าที่บริษัทจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของบริษัทฯ
2. ข้อมูลสารสนเทศ หรือโปรแกรมอื่นใดที่เจ้าหน้าที่บริษัทได้จัดทำหรือพัฒนาขึ้นระหว่างการจ้างงานถือเป็นทรัพย์สินของบริษัทฯ
3. ซอฟต์แวร์ที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัทฯ เป็นซอฟต์แวร์ที่บริษัทฯ ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามเจ้าหน้าที่บริษัทคัดลอกซอฟต์แวร์ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
4. ไม่อนุญาตให้เจ้าหน้าที่บริษัททำการติดตั้งและแก้ไขเปลี่ยนแปลงซอฟต์แวร์ในเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัทฯ
5. การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่สารสนเทศเท่านั้น
6. ในการเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล จะต้องมีการกำหนดชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password)
7. เจ้าหน้าที่บริษัทไม่ควรอนุญาตให้บุคคลอื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน
8. เจ้าหน้าที่บริษัทต้องทำการล็อคหน้าจอทุกครั้ง ในกรณีที่เจ้าหน้าที่บริษัทไม่ได้ปฏิบัติงานอยู่หน้าเครื่องคอมพิวเตอร์ และต้องมีการใส่รหัสผ่านทุกครั้งเมื่อต้องการกลับเข้าสู่หน้าจอ
9. เจ้าหน้าที่บริษัทที่ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องทำการสำรองข้อมูลที่สำคัญของบริษัทฯ จากเครื่องคอมพิวเตอร์ส่วนบุคคลไปยังสื่อบันทึก หรือเครื่องแม่ข่ายที่บริษัทฯ กำหนดให้เท่านั้น
10. การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่สารสนเทศ หรือได้รับการอนุมัติจากเจ้าหน้าที่สารสนเทศ และ/หรือ กรรมการผู้จัดการ เท่านั้น
11. ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
12. ไม่อนุญาตให้มีการนำเครื่องคอมพิวเตอร์ส่วนตัวของเจ้าหน้าที่บริษัทเข้ามาใช้เพื่อทำงานของบริษัทฯ หรือเชื่อมต่อไปยังระบบเครือข่ายและระบบงานหลักของบริษัทฯ

หมวดที่ 8	**นโยบายการใช้งานอินเตอร์เน็ต**
วัตถุประสงค์	เพื่อให้เจ้าหน้าที่บริษัทรับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเตอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคล ซึ่งส่งผลให้ให้ระบบคอมพิวเตอร์ของบริษัทฯ ถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทางานตามปกติได้

1. เจ้าหน้าที่สารสนเทศควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy Firewall IPS/IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-Up Modem หรือเชื่อมต่อผ่านเครือข่ายโทรศัพท์ของเจ้าหน้าที่บริษัท
2. ในการรับ-ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับ-ส่งข้อมูลทุกครั้ง
3. เจ้าหน้าที่บริษัทต้องไม่ใช้เครือข่ายอินเตอร์เน็ตของบริษัทฯ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการ เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
4. เจ้าหน้าที่บริษัทต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับบริษัทฯ
5. ห้ามเจ้าหน้าที่บริษัทเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเตอร์เน็ต
6. เจ้าหน้าที่บริษัทต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเตอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
7. ในการเสนอความคิดเห็นผ่านเว็บบอร์ด (Web board) เจ้าหน้าที่บริษัทต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของบริษัทฯ และต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัทฯ

หมวดที่ 9	**นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์**
วัตถุประสงค์	เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัทฯ ซึ่งเจ้าหน้าที่บริษัทจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่อาจจะเกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเตอร์เน็ต เจ้าหน้าที่บริษัทจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่เจ้าหน้าที่สารสนเทศได้กำหนดไว้ และจะต้องปฏิบัติตามคำแนะนำของเจ้าหน้าที่สารสนเทศนั้นอย่างเคร่งครัด

1. เจ้าหน้าที่สารสนเทศต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ ให้เหมาะสมกับการเข้าใช้บริการของเจ้าหน้าที่บริษัทและหน้าที่ความรับผิดชอบของเจ้าหน้าที่บริษัท รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น
2. เจ้าหน้าที่สารสนเทศต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร
3. สำหรับเจ้าหน้าที่ใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที
4. การกำหนดรหัสผ่านที่ดี (Good Password) ต้องเป็นไปตามนโยบายการบริหารจัดการรหัสผ่าน
5. เจ้าหน้าที่บริษัทไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
6. เจ้าหน้าที่บริษัทควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3 - 6 เดือน
7. เจ้าหน้าที่บริษัทควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร
8. เจ้าหน้าที่บริษัทควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานของบริษัทฯ เท่านั้น
9. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบ ทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
10. เจ้าหน้าที่บริษัทควรทำการตรวจสอบไวรัสบนเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดทุกครั้ง
11. เจ้าหน้าที่บริษัทไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

หมวดที่ 10	**นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี**
วัตถุประสงค์	เพื่อควบคุมและป้องกันระบบเครือข่าย เครื่องแม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัทฯ จากซอฟต์แวร์อันตรายหรือไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดี

1. เจ้าหน้าที่สารสนเทศต้องจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัสเวอร์ชั่นล่าสุดในระดับระบบปฏิบัติการบน เครื่องคอมพิวเตอร์และเครื่องแม่ข่ายที่สำคัญของบริษัทฯ
2. เจ้าหน้าที่สารสนเทศต้องกำหนดให้มีการปรับปรุง Antivirus Engine และAntivirus Pattern ให้เป็นปัจจุบันอยู่เสมอ โดยอ้างอิงจากเว็บไซต์ของเจ้าของผลิตภัณฑ์
3. เจ้าหน้าที่สารสนเทศต้องกำหนดให้โปรแกรมป้องกันไวรัสทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะที่มีการใช้ระบบด้วย
4. เจ้าหน้าที่สารสนเทศต้องกำหนดให้โปรแกรมป้องกันไวรัสทำการสแกนเครื่องแม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคลเพื่อตรวจหาไวรัสเป็นประจำทุกอาทิตย์ (Weekly Schedule Scan)
5. เจ้าหน้าที่สารสนเทศต้องกำหนดให้เจ้าหน้าที่บริษัทไม่สามารถปิดการทำงานของโปรแกรมป้องกันไวรัสบนเครื่องแม่ข่ายหรือเครื่องคอมพิวเตอร์ส่วนบุคคลได้
6. ข้อมูลสารสนเทศและซอฟต์แวร์อื่นใดที่ดาวน์โหลดจาก Internet หรือได้รับผ่านทางจดหมายอิเล็กทรอนิกส์ ต้องทำการตรวจสอบไวรัสก่อนทำการดาวน์โหลดลงสู่เครื่องคอมพิวเตอร์ของบริษัทฯ ทุกครั้ง
7. ห้ามมิให้เจ้าหน้าที่บริษัทหรือเจ้าหน้าที่สารสนเทศ ดำเนินการใด ๆ ที่เกี่ยวกับการพัฒนาไวรัสหรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ
8. ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกบริษัทฯ มาใช้ ผู้ใช้งานสื่อบันทึกข้อมูลนั้นต้องตรวจสอบไวรัสคอมพิวเตอร์ก่อนใช้งานทุกครั้ง

หมวดที่ 11	**นโยบายการการสำรองและกู้คืนข้อมูล**
วัตถุประสงค์	เพื่อจัดทำมาตรฐานในการสำรองข้อมูลและการกู้คืนข้อมูลเมื่อเกิดเหตุใด ๆ ที่ไม่สามารถเข้าถึงข้อมูลของบริษัทฯ ได้ด้วยวิธีการปกติ และให้แน่ใจว่าระบบสารสนเทศและข้อมูลของบริษัทฯ สามารถกู้คืนกลับมาใช้ งานได้ในช่วงเวลาที่กำหนด รวมถึงมีการจัดเก็บการสำรองข้อมูลในสภาพแวดล้อมที่มีการควบคุมอย่างเหมาะสม และทำการจัดเก็บการสำรองข้อมูลอย่างสม่ำเสมอ รวมทั้งมีการจัดทำการทดสอบการกู้คืนข้อมูลเพื่อให้สามารถแน่ใจในกระบวนการสำรองข้อมูล

1. บริษัทฯ ต้องกำหนดให้เจ้าหน้าที่สารสนเทศทำการสำรองข้อมูลจากเครื่องแม่ข่าย อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีความสำคัญ หรือจำเป็นต่อการปฏิบัติงานให้ครบถ้วน
2. บริษัทฯ ต้องกำหนดให้ เจ้าหน้าที่สารสนเทศ ต้องจัดทำคู่มือการปฏิบัติการในการสำรองข้อมูล โดยประกอบด้วยข้อมูลดังต่อไปนี้
   - รายละเอียดข้อมูลที่ทำการสำรอง
   - ความถี่ในการสำรองข้อมูล
   - ประเภทของสื่อบันทึก (Backup Media)
   - ขั้นตอนและวิธีการสำรองโดยละเอียด
   - สถานที่และวิธีการเก็บรักษาสื่อบันทึก
   - ระยะเวลาในการจัดเก็บตามประเภทของข้อมูล (เนื่องด้วยข้อมูลบางประเภทต้องจัดเก็บเป็นระยะเวลาตามที่กฎหมายกำหนด
3. บริษัทฯ ต้องจัดเก็บสื่อบันทึกที่ใช้สำรองข้อมูล ชุดโปรแกรมสำรอง ระบบปฏิบัติการสำรอง ระบบฐานข้อมูลสำรองค่าติดตั้งเครื่องแม่ข่ายและอุปกรณ์ บัญชีผู้ใช้ ข้อมูลจราจร พร้อมทั้งสำเนานโยบาย มาตรฐาน และขั้นตอนปฏิบัติงาน และสิ่งที่จำเป็นสำหรับการทำธุรกรรมอย่างต่อเนื่องไว้ในสถานที่ที่ปลอดภัย ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และพร้อมใช้ในกรณีที่สถานที่ทำงานปัจจุบันไม่สามารถเข้าใช้งานได้
4. สื่อบันทึกที่ใช้สำรองข้อมูล ต้องมีป้ายกำกับให้ชัดเจน เพื่อบอกถึงสิ่งที่ถูกสำรองไว้ภายในสื่อบันทึก ขนาด วันที่เก็บ ระยะเวลาในการเก็บ และ ผู้จัดเก็บ เป็นอย่างน้อย
5. การเข้าถึงสื่อบันทึกข้อมูล การทำสำเนาข้อมูลในสื่อบันทึกข้อมูล หรือการถ่ายรูป เพื่อการบันทึกรายละเอียดที่เกี่ยวข้องกับสื่อบันทึกข้อมูล ต้องได้รับอนุญาตจากกรรมการผู้จัดการของบริษัทฯ เท่านั้น และห้ามให้บุคคลที่ไม่ได้รับอนุญาตหรือบุคคลภายนอกทำการสำเนาใด ๆ ก็ตามที่เกี่ยวข้องกับสื่อบันทึกข้อมูลทั้งหมด
6. บริษัทฯ ต้องกำหนดให้มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของบริษัทฯ พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง พร้อมทั้งให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง
7. บริษัทฯ ต้องกำหนดให้มีการทดสอบการกู้คืนข้อมูลจากข้อมูลหรือหรือระบบที่ได้มีการสำรองไว้แล้วอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูล หรือระบบที่สำรองไว้มีความถูกต้องครบถ้วน และมีความพร้อมใช้งาน

หมวดที่ 12	**นโยบายการบริหารจัดการการเปลี่ยนแปลงแก้ไขระบบ**
วัตถุประสงค์	เพื่อให้มีการควบคุมที่ดีในการเปลี่ยนแปลงแก้ไขระบบเครือข่ายและคอมพิวเตอร์ที่มีการใช้งานอยู่ในบริษัทฯ เพื่อให้สามารถตรวจสอบการเปลี่ยนแปลงแก้ไขระบบที่เกิดขึ้น เพื่อให้มีการบันทึกการเปลี่ยนแปลงแก้ไขระบบและเพื่อให้สามารถป้องกันผลกระทบที่อาจจะเกิดขึ้นจากการเปลี่ยนแปลงแก้ไขระบบได้

1. บริษัทฯ ต้องจัดทำเอกสารคู่มือการติดตั้งระบบเครือข่ายและคอมพิวเตอร์ การติดตั้งเครื่องแม่ข่ายพร้อมทั้งมีการปรับปรุงให้เป็นปัจจุบันเสมอ
2. บริษัทฯ ต้องกำหนดให้ “เจ้าหน้าที่สารสนเทศ” เป็นผู้รับผิดชอบ หรือคอยประสานงานกับหน่วยงานภายนอก เพื่อทำการเปลี่ยนแปลงแก้ไขระบบงานตามที่มีผู้ใช้งานร้องขอ
3. บริษัทฯ ต้องกำหนดขั้นตอนการปฏิบัติงานเพื่อควบคุมและบริหารจัดการการเปลี่ยนแปลงแก้ไขระบบ และปรับปรุงให้เป็นปัจจุบันเสมอ ซึ่งอาจจะประกอบไปด้วยเนื้อหาดังต่อไปนี้
   3.1. ขั้นตอนปฏิบัติงานในการร้องขอ
   3.2. การระบุรายการต้องการเปลี่ยนแปลงแก้ไข วันเวลาที่ต้องการเปลี่ยนแปลงแก้ไข
   3.3. การประเมินผลกระทบของการเปลี่ยนแปลงแก้ไข
   3.4. ขั้นตอนการขออนุมัติการเปลี่ยนแปลงแก้ไข รวมถึงขั้นตอนการขออนุมัติการเปลี่ยนแปลงแก้ไขในกรณีฉุกเฉิน
   3.5. ขั้นตอนการปฏิบัติงานในการนำระบบกลับสู่สภาวะปกติ หากการเปลี่ยนแปลงแก้ไขที่ร้องขอไม่สำเร็จ
   3.6. การทดสอบระบบที่ได้รับการเปลี่ยนแปลงแก้ไข
   3.7. การรายงานกรรมการผู้จัดการถึงผลลัพธ์ของการเปลี่ยนแปลงแก้ไข
   3.8. การติดตามผลหลังการเปลี่ยนแปลงแก้ไข
4. การร้องขอให้มีการเปลี่ยนแปลงระบบ ต้องทำเป็นลายลักษณ์อักษร และต้องได้รับอนุมัติอย่างเป็นทางการจากเจ้าของข้อมูลและระบบงาน และกรรมการผู้จัดการเท่านั้น
5. ต้องจัดเก็บข้อมูลรายละเอียดการเปลี่ยนแปลง รายละเอียดค่าติดตั้งต่าง ๆ เกี่ยวกับระบบงาน และชุดโปรแกรมที่ใช้อยู่ให้เป็นปัจจุบัน
6. ห้ามใช้ข้อมูลจริงในการทดสอบระบบก่อนที่จะมีการเปลี่ยนแปลงแก้ไขระบบงานจริง
7. ต้องทำการสำรองข้อมูลและระบบก่อนทำการเปลี่ยนแปลงแก้ไขระบบงานทุกครั้ง

หมวดที่ 13	**นโยบายการปฏิบัติตามข้อบังคับ**
วัตถุประสงค์	เพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมายที่เกี่ยวข้องกับการดำเนินงานของบริษัทฯ

1. บริษัทฯ ต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยอย่างเคร่งครัด และไม่กระทำความผิด ดังนั้น หากผู้ใช้งานคอมพิวเตอร์กระทำผิดโดยอ้างอิงจากกฎหมายดังกล่าว บริษัทฯ ถือว่าเป็นความผิดส่วนบุคคล
2. ห้ามมิให้ผู้ใช้งานทุกคนในบริษัทฯ กระทำการที่เป็นการละเมิดลิขสิทธิ์ซอฟต์แวร์เป็นอันขาด

หมวดที่ 14	**นโยบายการคุ้มครองข้อมูลส่วนบุคคล** (PDPA)
วัตถุประสงค์	เพื่อปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

1. บริษัทฯ ได้มีการจัดทำนโยบายการใช้คุกกี้ (Cookies Policy) ในการเข้าชมเว็บไซต์ของ บริษัทฯ อาจมีการวางคุกกี้ไว้ในอุปกรณ์ของผู้เข้าชม และมีการเก็บรวบรวมข้อมูลโดยอัตโนมัติ คุกกี้บางส่วนมีความจำเป็น เพื่อให้เว็บไซต์สามารถทำงานได้อย่างเหมาะสม และบางส่วนเป็นคุกกี้ที่มีไว้เพื่ออำนวยความสะดวกแก่ผู้เข้าชมเว็บไซต์
2. บริษัทฯ ได้มีการติดตั้งกล้องวงจรปิดบริเวณภายในอาคาร และภายนอกอาคาร เพื่อตรวจสอบความเคลื่อนไหวที่เกิดขึ้น หากมีเหตุการณ์ที่น่าสงสัย และอาจเกิดอันตรายต่อผู้ที่มีส่วนได้ส่วนเสียของบริษัทฯ ทั้งนี้บริษัทฯ ได้มีการบันทึกภาพ และวิดีโอ เก็บไว้เพื่อเป็นหลักฐานในกรณีเกิดเหตุการณ์ต่าง ๆ ขึ้น

หมวดที่ 15	**นโยบายการควบคุมการเข้ารหัสข้อมูล** (Data Encryption Control)
วัตถุประสงค์	เพื่อสร้างความน่าเชื่อถือในความมั่นคงปลอดภัยของข้อมูลในระบบต่อผู้เกี่ยวข้องกับบริษัทฯ

1. บริษัทฯ มีนโยบายการควบคุมการเข้ารหัสข้อมูล โดยมีการบริหารจัดการข้อมูล และมีการจัดลำดับชั้นความลับ มีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนดวิธีบริหารจัดการกับข้อมูลแต่ละประเภท รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการยกเลิกหรือการนำกลับมาใช้ใหม่
   1.1 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL (Secure Socket Layer) การใช้ VPN (Virtual Private Network) เป็นต้น
   1.2 มีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน
   1.3 มีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม เป็นต้น หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน