การตรวจสอบและอนุมัติ (Verification and Approval)

การลงนาม	Signature	Position	Date
จัดทำโดย **Prepared by**	(เจษฎา ไชยวงษา)	Department Head - IT Technical Infrastructure	15 พฤศจิกายน 2566
ตรวจสอบโดย **Verified by**	(ณัฐชมนต์ กวีพิสิทธิ์กุล)	VP - IT	1 ธันวาคม 2566
	(ปวารณ์วดี วิชัยดิษฐ)	SVP - Supply Chain & IT	1 ธันวาคม 2566
อนุมัติโดย **Approved by**	(กฤษชนก ปัทมสัตยาสนธิ)	MD	1 ธันวาคม 2566

บันทึกการแก้ไข (Document History)

ครั้งที่ Revision	รายการที่แก้ไข Revised Topics and Changes	มีผลบังคับใช้ Effective Date
00	เอกสารฉบับสมบูรณ์	1 พฤศจิกายน 2566
01	เพิ่มโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	1 ธันวาคม 2566

บันทึกหน่วยงานผู้รับสำเนาเอกสาร (Document Distribution Record)

☐ ทุกหน่วยงาน ☐ เฉพาะหน่วยงาน/สายงานที่ออกเอกสาร ☐ หน่วยงานที่เกี่ยวข้อง โปรดระบุ....

สำเนา	หน่วยงาน

ขอบเขต (SCOPE)

ครอบคลุมพนักงานประจำของกลุ่มบริษัท อินเด็กซ์ ลิฟวิ่งมอลล์ จำกัด (มหาชน) ตลอดจนบุคคลที่กระทำการในนามของกลุ่มบริษัท อินเด็กซ์ ลิฟวิ่งมอลล์ จำกัด (มหาชน)

บังคับใช้ทั้งบริษัทฯ หมายรวมถึง สำนักงานใหญ่ สาขา เฟอร์นิเจอร์เซ็นเตอร์ ศูนย์กระจายสินค้า (DC) เดอะวอล์ค (The walk) และสำนักงานสาขา หรือหน่วยธุรกิจอื่นใดทั้งที่มีอยู่ในปัจจุบัน หรือในอนาคตของกลุ่มบริษัท อินเด็กซ์ ลิฟวิ่งมอลล์ จำกัด (มหาชน)

วัตถุประสงค์ (OBJECTIVE)

1. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ของกลุ่มบริษัทอินเด็กซ์ ลิฟวิ่งมอลล์ จำกัด (มหาชน) ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
2. เพื่อกำหนดทิศทางและสนับสนุนในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้แก่ผู้บริหารและเป็นบรรทัดฐาน ในการดำเนินการอันเกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร
3. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง
4. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ผู้ดูแลระบบ พนักงานและบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด
5. เพื่อใช้เป็นหลักในการพัฒนาและปรับปรุงคุณภาพด้านความมั่นคงปลอดภัยสารสนเทศ
6. นโยบายและขั้นตอนปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร จะต้องกำหนดและอนุมัติโดยคณะกรรมการอำนวยการ (steering committee) และต้องเผยแพร่ให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องทุกคนได้รับทราบและพนักงานทุกคนจะต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด หลังจากได้รับการอนุมัติแล้ว
7. การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร จะต้องได้รับการสอบทานเป็นประจำทุกปี หรือหากมีการแก้ไขเปลี่ยนแปลงที่เป็นสาระสาคัญ จะต้องได้รับการอนุมัติจากผู้บริหาร

องค์ประกอบของนโยบาย

คำจำกัดความ

ส่วนที่ 1 การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ 2 การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์

ส่วนที่ 3 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 4 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

ส่วนที่ 5 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ 6 การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

ส่วนที่ 7 การควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ 8 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ส่วนที่ 9 การจัดทำระบบสำรองข้อมูลและการเข้ารหัสข้อมูล

ส่วนที่ 10 การตรวจสอบและประเมินความเสี่ยง

ส่วนที่ 11 นโยบายความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต

ส่วนที่ 12 แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์

ส่วนที่ 13 ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์

ส่วนที่ 14 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 15 นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ส่วนที่ 16 การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

จำกัดความ (DEFINITION)

1. **กลุ่มบริษัท** หมายถึง บริษัท อินเด็กซ์ ลิฟวิ่งมอลล์ จำกัด (มหาชน) และบริษัทย่อย
2. **บริษัทฯ** หมายถึง บริษัทอินเด็กซ์ ลิฟวิ่งมอลล์ จำกัด (มหาชน) โดยให้รวมถึงผู้ซึ่งได้รับมอบอำนาจให้กระทำการแทนบริษัทฯ หรือผู้ได้รับมอบหมายให้ทำงานในนามบริษัทฯ
3. **บริษัทย่อย** หมายถึง บริษัทที่บริษัทฯ ถือหุ้นเกินกว่าร้อยละ 50
4. **ผู้ที่ได้รับมอบหมายอย่างเป็นทางการ** หมายถึง ผู้ที่ผู้บริหารสูงสุดมอบหมายให้ดูแลรับผิดชอบและปฏิบัติงาน
5. **ผู้ใช้ หรือ ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role)
    - ผู้บริหารระดับสูงสุด (Chief Executive Office: CEO) หมายความว่า ผู้บริหารสูงสุดของบริษัทฯ
    - ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Office: CIO) หมายความว่า ผู้บริหารหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ
    - พนักงาน หมายความว่า ลูกจ้างชั่วคราว ลูกจ้างประจำ
    - บุคคลภายนอก หมายความว่า บุคคลที่บริษัทฯ อนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของบริษัทฯ ได้ชั่วคราวเพื่อประโยชน์ในการดำเนินงานของบริษัทฯ ได้แก่ พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดต่อหรือดูแลรักษาระบบให้กับบริษัท หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง
6. **สินทรัพย์** หมายถึง ทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือสิ่งใดก็ตามที่มีคุณค่าต่อบริษัท ประกอบด้วย เครื่องแม่ข่าย (เซิร์ฟเวอร์) โครงสร้างเครือข่ายพื้นฐาน ระบบและซอฟต์แวร์ประยุกต์ ข้อมูล ระบบข้อมูล ตลอดจนระบบย่อยและส่วนประกอบคอมพิวเตอร์อื่นๆ ลูกค้า ที่บริษัทฯ เป็นเจ้าของหรือใช้งานหรืออยู่ภายใต้ความรับผิดชอบของบริษัทฯ นอกจากนี้การใช้ระบบสารสนเทศ หมายรวมถึงการใช้บริการต่างๆ ทั้งหมด ทั้งภายในและภายนอก เช่น การเข้าใช้อินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์ เป็นต้น
7. **การเข้าถึงหรือการควบคุมการเข้าถึง** หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน ในการเข้าถึงหรือใช้งานเครือข่ายหรือระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอกที่เกี่ยวข้องกับการให้บริการและข้อมูลที่จำเป็นต่อการใช้งาน โดยมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากบุคคลทั้งภายในและภายนอก
8. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)
9. **ความมั่นคงปลอดภัยด้านการบริหารจัดการ** หมายถึง การกระทำในระดับบริหารโดยการจัดให้มี นโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ เพื่อนำมาใช้ในกระบวนการคัดเลือก การพัฒนา การนำไปใช้งาน หรือการบำรุงรักษาทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัย
10. **ความมั่นคงปลอดภัยทางด้านกายภาพ** หมายถึง การจัดให้มีนโยบาย มาตรการหลักเกณฑ์ หรือ กระบวนการใดๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจาก การคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

11. **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือ มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
12. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของบริษัทฯ ถูกบุกรุกหรือโจมตี
13. **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานที่บริษัทฯ อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงานโดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
14. **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของ ข้อมูลและระบบเทคโนโลยีสารสนเทศ
15. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
16. **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่ง ข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของบรษัทได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเตอร์เน็ต (Internet)
    - ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ระบบคอมพิวเตอร์ต่างๆ ภายในบริษัทฯ เข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในบริษัทฯ
    - ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่าย คอมพิวเตอร์ต่างๆของบริษัทเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก
17. **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงานของบริษัทที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่บริษัทสามารถนำมาใช้ประโยชน์ในการวางแผนบริหาร สนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร มีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูลและสารสนเทศเป็นต้น
18. **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace)** หมายถึง พื้นที่ที่บริษัทอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น
    - พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล
    - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
    - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
19. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
20. **แผนกเทคโนโลยีสารสนเทศ** หมายถึง หน่วยงานที่ดำเนินการเกี่ยวกับระบบสารสนเทศและระบบงานคอมพิวเตอร์และเป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศของบริษัท โดยมีหน้าที่ศึกษาวิเคราะห์เพื่อพัฒนาระบบสารสนเทศและระบบงานคอมพิวเตอร์ของบริษัท และปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง

21. **จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่อง** คอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

ส่วนที่ 1
การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management)

1. วัตถุประสงค์

เพื่อกำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และกำหนดหน้าที่ผู้รับผิดชอบที่ชัดเจน ในการดูแลระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ ในกรณีที่เกิดการเสียหายหรืออันตรายใดๆ แก่บริษัทฯ, ในการหาแนวทางทบทวนแนวนโยบายและแนวปฏิบัติ เพื่อใช้ในการแก้ปัญหาที่เกิดขึ้นและนำไปสู่การปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้มีคุณภาพต่อไป

2. แนวทางในการบริหารจัดการ

2.1. อินเด็กซ์ ลิฟวิ่งมอลล์ กำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และบทบาทหน้าที่ การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศดังนี้

2.1.1. **ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office: CEO)**

เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นจากการละเลยการควบคุม ความมั่นคงปลอดภัยสารสนเทศกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่บริษัทฯ หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.2. **ผู้บริหารสารสนเทศระดับสูง (CIO)**

เป็นผู้กำกับดูแลรับผิดชอบด้านสารสนเทศของบริษัท กำหนดนโยบาย และแนวทางการใช้งานระบบ การติดตามโครงการลงทุนด้านเทคโนโลยีสารสนเทศและไซเบอร์ให้สอดคล้องกับ กลยุทธ์ทางธุรกิจ

ทั้งนี้ อินเด็กซ์ ลิฟวิ่งมอลล์ จัดให้มีการประชุมคณะกรรมการพัฒนาบริหารจัดการระบบสารสนเทศ โดยผู้บริหารสารสนเทศระดับสูง และผู้บริหารหน่วยงาน เพื่อทำการทบทวนและทราบถึงแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

2.2. ทำความเข้าใจ และให้การสนับสนุนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยจัดให้มีการทำรายงานการประชุมผู้บริหารสารสนเทศและแจ้งเป็นแนวปฏิบัติให้พนักงานที่เกี่ยวข้องรับทราบและปฏิบัติตามอย่างเคร่งครัด

2.3. จัดให้มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงและแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศของบริษัทฯ

2.4. จัดให้มีการประเมินแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ เพื่อนำไปปรับปรุงให้มีประสิทธิภาพในปีถัดไป

2.5. กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศต้องจัดทำเป็นลายลักษณ์อักษรตามวัตถุประสงค์ของขอบเขตงานที่ได้รับการอนุมัติจากผู้บริหารระดับสูงสุด (CEO) หรือผู้บริหารสารสนเทศระดับสูง (CIO) เพื่อประกาศใช้และถือปฏิบัติในบริษัทฯ

โดยให้มีผลบังคับใช้กับพนักงานในทุกระดับของบริษัทฯ ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและสินทรัพย์สารสนเทศของบริษัทฯ

2.6. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่พอเพียงต่อการบริหารจัดการด้านความมั่นคงปลอดภัยในแต่ละปีงบประมาณซึ่งรวมถึงแผนความมั่นคงปลอดภัยสารสนเทศที่จะดำเนินการในปีงบประมาณนั้นด้วย

2.7. จัดให้มีการอบรมให้ความรู้ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้กับพนักงาน เพื่อสร้างความตระหนักและความเข้าใจภัยและผลกระทบที่จะเกิดขึ้น จากการใช้ระบบงานสารสนเทศโดยไม่ระมัดระวังหรือไม่เท่าถึงการณ์ อย่างน้อยปีละ 1 ครั้ง

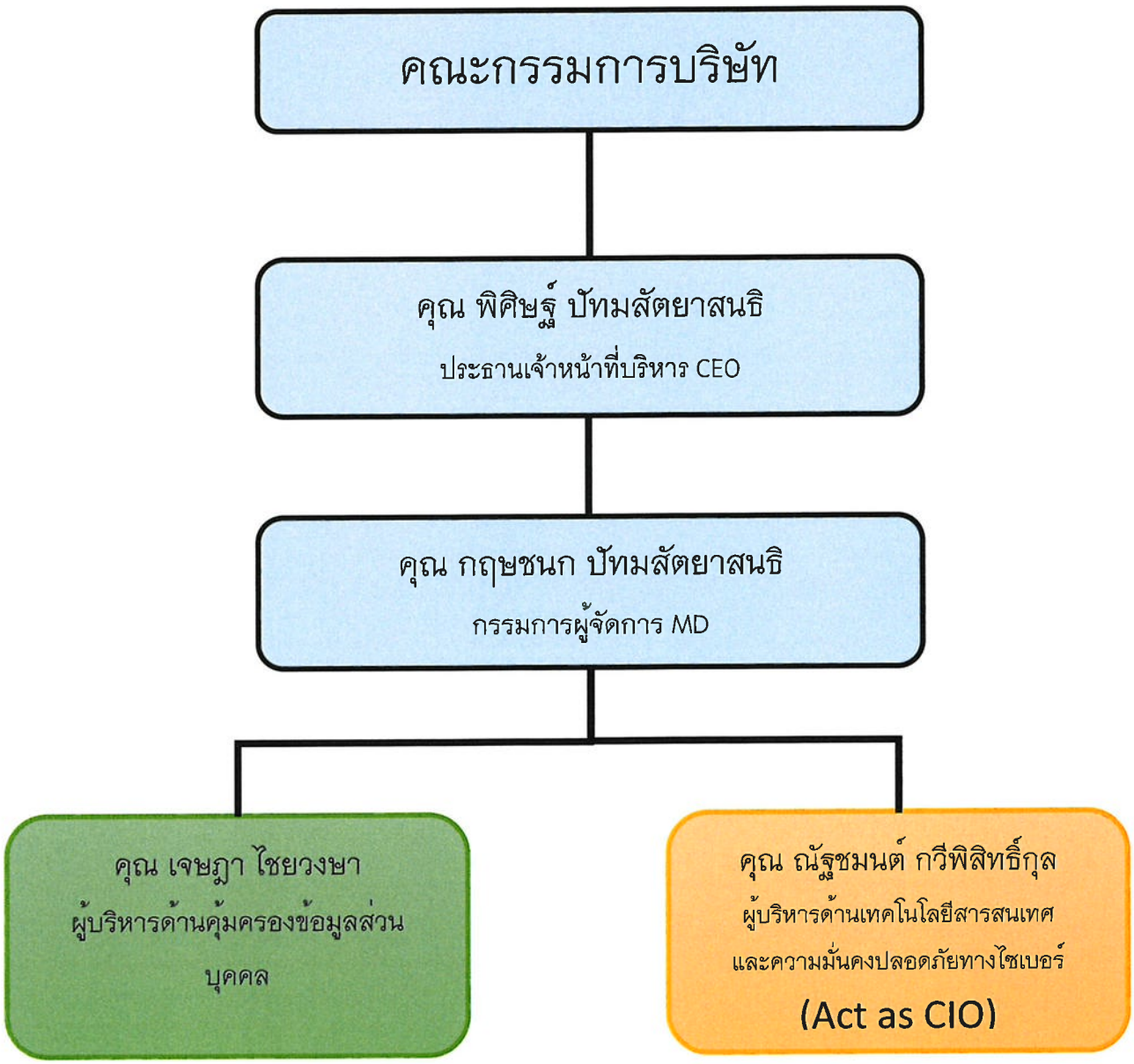
2.8. จัดให้มีการตรวจสอบและประเมินความเสี่ยงในการปฏิบัติปีละ 1 ครั้งและจัดให้มีการทำแผนการปรับปรุง เพื่อทบทวนหรือแก้ไขปัญหาที่พบ

2.9. จัดให้มีการอบรมให้ความรู้และซักซ้อมแผนฉุกเฉินภัยพิบัติ ของระบบเทคโนโลยีสารสนเทศ (IT Disaster recovery plan) อย่างน้อยปีละ 1 ครั้ง

2.10. กำหนดหน้าที่ที่ต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ และกำหนดหน้าที่รับผิดชอบของพนักงานเจ้าหน้าที่ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ และแผนฉุกเฉินภัยพิบัติของระบบเทคโนโลยีสารสนเทศของบริษัท

2.11. ผู้บริหาร ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้ชัดเจน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และ พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

โครงสร้างการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ



ส่วนที่ 2

การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์

(Computing System Control Room)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการ เข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายและระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้ จะมีผลบังคับใช้กับผู้ใช้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

2. การควบคุมการเข้าออก

2.1 ภายในบริษัทฯ มีการติดตั้งระบบควบคุมการเขาออกอัตโนมัติ (Access Control System) เพื่อควบคุมการเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย เพื่อจุดประสงค์ในการควบคุมการเข้าออกของบุคคลภายนอก โดยใช้เทคโนโลยีระบบ Biometric Finger Scan และ Proximity Card

2.2 ภายในบริษัทฯ มีการติดตั้งระบบกล้องวงจรปิดเพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

2.3 ต้องกำหนดสิทธิให้กับพนักงานให้สามารถมีสิทธิในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย ประกอบด้วย

2.3.1 จัดทำ "ทะเบียนผู้มีสิทธิเข้าออกพื้นที่" เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

2.3.2 กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออก ดังกล่าวโดยจัดทำเป็นเอกสาร "บันทึกการเข้าออกพื้นที่

2.3.3 จัดให้มีพนักงานที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำ และให้มีการปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร ปีละ 1 ครั้ง เป็นอย่างน้อย

2.4 บุคคลภายนอกเข้ามาติดต่อจะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้า-ออกให้ถูกต้อง และจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

2.5 บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

ส่วนที่ 3
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ ได้อย่างถูกต้อง

2. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

2.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศ ที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

2.2 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของพนักงานในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3 ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูล และระบบข้อมูลได้

2.4 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

2.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อ เป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

3. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้นจะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนด ใหมีการลงนามอนุมัติ และเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

3.2 เจ้าของข้อมูลและเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

3.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากพนักงานที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

4. การบริหารจัดการการเข้าถึงของผู้ใช้

4.1 การลงทะเบียนพนักงานใหม่ของบริษัทฯ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปต้องทำภายใน 24 ชั่วโมงหรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน 7 วัน

4.2 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

4.3 ผู้ใช้ต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็น ลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

4.4 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของพนักงาน

4.4.1 ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของพนักงานในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในเอกสาร "การบริหารจัดการการเข้าถึงของผู้ใช้งาน"

4.4.2 การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตาม "การบริหารจัดการการเข้าถึงของผู้ใช้งาน"

4.4.3 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัย ต่อไปนี้ประกอบการพิจารณา

4.4.3.1 ควรได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้นๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ

4.4.3.2 ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

4.4.3.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

4.4.3.4 ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยน รหัสผ่านทุก 3 เดือน เป็นต้น

4.5 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

4.5.1 ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูลวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึง ผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

4.5.2 เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4.5.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

4.5.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

4.5.5 ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร "การบริหารจัดการการเข้าถึงของผู้ใช้งาน"

4.5.6 ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ใน สื่อบันทึกก่อน เป็นต้น

5. การบริหารจัดการการเข้าถึงระบบเครือข่าย

5.1 ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งานกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

5.2 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

5.3 ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

5.4 ผู้ดูแลระบบควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้ กำหนดบุคคลที่รับผิดชอบในการ กำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบ

5.5 ป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและควรทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

5.6 ระบบเครือข่ายทั้งหมดของบริษัทฯ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

5.7 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของบริษัทฯ ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

5.8 การเข้าสู่ระบบงานเครือข่ายภายในบริษัทฯ โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการล็อกอิน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

5.9 IP address ภายในของระบบงานเครือข่ายภายในของบริษัทฯ จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

5.10 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.11 การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

5.12 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยพนักงานกลุ่มเทคโนโลยีสารสนเทศเท่านั้น

6. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย
   6.1 ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือ เปลี่ยนแปลงค่าต่าง ๆของโปรแกรมระบบ (System Software) อย่างชัดเจน
   6.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที
   6.3 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น Telnet ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย
   6.4 ควรดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น web server เป็นต้น
   6.5 ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา
   6.6 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยพนักงานกลุ่มเทคโนโลยีสารสนเทศเท่านั้น
7. การบริหารจัดการการบันทึกและตรวจสอบ
   7.1 ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน
   7.2 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
   7.3 ต้องมีมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆและจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
8. การควบคุมการเข้าใช้งานระบบจากภายนอก ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในบริษัทฯ เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติ ดังนี้
   8.1 การเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายของบริษัทฯ ต้องควบคุมบุคคลที่จะเข้าสู่ระบบของบริษัทฯ จากระยะไกล โดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน
   8.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจากผู้บริหารหน่วยงานเทคโนโลยีสารสนเทศ หรือบริหารหน่วยงานแต่ละหน่วยงานก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของบริษัทฯ ในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด
   8.3 การทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกลผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับบริษัทฯ อย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ
   8.4 ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม
   8.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ เมื่อมีการร้องขอที่จำเป็นเท่านั้น

9. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

9.1 ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของบริษัทฯ ดังนี้

9.1.1 แสดงชื่อผู้ใช้งาน (Username)

9.1.2 ใส่รหัสผ่าน (Password)

ส่วนที่ 4
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ

2. การลงทะเบียนผู้ใช้งาน (User Registration)
   - 2.1 จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบเทคโนโลยีสารสนเทศของบริษัทฯ
   - 2.2 ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยเฉพาะผู้ที่ไม่มีการลงทะเบียนผู้ใช้งานมาก่อน
   - 2.3 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
   - 2.4 ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศรวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว
   - 2.5 ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน
   - 2.6 ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต
3. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)
   - 3.1 ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
   - 3.2 ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ
   - 3.3 ผู้ดูแลระบบต้องมอบหมายสิทธิควรมีความสอดคล้องกับนโยบายควบคุมการเข้าถึง
   - 3.4 ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน
   - 3.5 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ
4. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)
   - 4.1 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ
   - 4.2 ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

4.3 ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีภายหลังจากที่ได้รับหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

4.4 ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและควรกำหนดรหัสผ่านที่แตกต่างกัน

4.5 ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่ง และควรกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

5. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights)

5.1 ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน 1 ครั้งต่อปี เป็นอย่างน้อย

5.2 ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง เช่น สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

5.3 ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

5.4 ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

ส่วนที่ 5
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

1. วัตถุประสงค์

   เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

2. การใช้งานรหัสผ่าน (Password Use)

   ผู้ใช้งานระบบเทคโนโลยีสารสนเทศควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

   2.1 ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

   2.2 ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

   2.3 ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

   2.4 ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

   2.5 ผู้ใช้งานควรตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำกำหนดไว้

   2.6 ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

   2.7 ผู้ใช้งานไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

   2.8 ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น 123 , abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น 111 , aaa เป็นต้น

   2.9 ผู้ใช้งานควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

   2.10 ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

   2.11 ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุกๆ 3 เดือน สำหรับผู้ดูแลและ 6 เดือน สำหรับผู้ใช้งานระบบ

   2.12 ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันที ในครั้งแรกที่ทำการล๊อคอินเข้าสู่ระบบงาน

   2.13 ผู้ใช้งาน ไม่ควร กำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเพื่อทำการล๊อคอินในภายหลัง

   2.14 ผู้ใช้งาน ไม่ควร ใช้รหัสผ่านของตนร่วมกับผู้อื่น

   2.15 ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ใช้งาน

3. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

   3.1 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องโน้ตบุ๊ก

   3.2 ผู้ใช้งานควรล๊อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

   3.3 ผู้ดูแลระบบควรกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

ส่วนที่ 6
การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
(Network Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของบริษัทฯ โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

2. กระบวนการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

2.1 การใช้งานบริการเครือข่าย

2.1.1 ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของบริษัทฯ

2.1.2 บริษัทฯ ไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

2.1.3 ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว บริษัทฯ ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

2.1.4 ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของบริษัทฯ

2.1.5 บริษัทฯ ให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือแจกจ่ายสิทธินี้ให้กับผู้อื่นไม่ได้

2.1.6 บัญชีผู้ใช้งาน (User Account) ที่บริษัทฯ ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

2.2 ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและพนักงาน มีแนวทางปฏิบัติดังนี้

2.2.1 ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุม ระบบเครือข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก "ทะเบียนผู้มีสิทธิเข้าออกพื้นที่" เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

2.2.2 สิทธิในการเข้าออกห้องต่างๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากผู้บริหารหน่วยงานเทคโนโลยีและสารสนเทศ เป็นลายลักษณ์อักษรโดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายห้องควบคุมระบบเครือข่าย

2.2.3 ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย จัดเก็บลายนิ้วมือเจ้าหน้าที่ผ่านเครื่องจัดเก็บลายนิ้วมือ และบันทึกข้อมูลลงคีย์การ์ด เพื่อบันทึกประวัติการเข้า-ออก ห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่

2.2.4 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายต้องทำการติดต่อผู้ดูแลระบบห้องควบคุมระบบเครือข่าย เพื่อเข้าห้องควบคุมระบบเครือข่าย พร้อมทั้งระบุเหตุผลการเข้าห้องควบคุมระบบเครือข่าย

2.2.5 ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการแจ้งเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องหลังจากดำเนินการเสร็จ ให้แจ้งผู้ดูแลระบบห้องควบคุมระบบเครือข่ายเพื่อตรวจสอบความเรียบร้อยและความถูกต้อง

2.3 ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติ ดังนี้

2.3.1 ผู้ติดต่อจากหน่วยงานภายนอกต้องทำการติดต่อผู้ดูแลระบบห้องควบคุมระบบเครือข่าย เพื่อเข้าห้องควบคุมระบบเครือข่าย พร้อมทั้งระบุเหตุผลการเข้าห้องควบคุมระบบเครือข่าย

2.3.2 ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการแจ้งผู้ติดต่อจากหน่วยงานภายนอก หลังจากดำเนินการเสร็จให้แจ้งผู้ดูแลระบบห้องควบคุมระบบเครือข่ายเพื่อตรวจสอบความเรียบร้อยและความถูกต้อง

ส่วนที่ 7
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

1. วัตถุประสงค์

   เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทฯ ให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย
   - 2.1 ผู้ใช้งานควรกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
   - 2.2 ผู้ใช้งานควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่ รหัสผ่าน (Password) เพื่อเข้าใช้งาน
   - 2.3 ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง
   - 2.4 ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของบริษัทฯ ร่วมกัน
   - 2.5 ผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)
   - 3.1 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข
   - 3.2 ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
   - 3.3 ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือแจกจ่ายให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
   - 3.4 ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

ส่วนที่ 8
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
(Application Information Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาต เข้าถึงระบบสารสนเทศของบริษัทฯ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ ได้อย่างถูกต้อง

2. การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

2.1 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนพนักงานใหม่ของบริษัทฯ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

2.2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

2.3 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของพนักงาน ดังต่อไปนี้

2.3.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

2.3.2 ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

2.3.3 กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

2.3.4 กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

2.3.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

2.3.6 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

2.4 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

2.4.1 ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

2.4.2 ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

2.4.3 กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

2.4.4 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

2.4.5 กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

2.4.6 กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัทฯ เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ส่วนที่ 9
การจัดทำระบบสำรองข้อมูล

1. วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและกู้คืนระบบ เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

2. แนวปฏิบัติงานการสำรองข้อมูลและระบบคอมพิวเตอร์

2.1 ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามนโยบายการสำรองข้อมูลของบริษัทฯ

2.2 การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

2.3 การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

2.4 ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

2.5 ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บริหารหน่วยงานเทคโนโลยีสารสนเทศ

2.6 ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

2.7 การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สาคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

2.8 นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ (Backup Procedure) โดยเคร่งครัด

3. การกู้คืนระบบ

3.1 ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบ เครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้บริหารหน่วยงานเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้บริหารหน่วยงานเทคโนโลยีสารสนเทศทราบ

3.2 ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

3.3 หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

4. การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Disaster Recovery Plan)

นโยบายเกี่ยวกับการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Disaster Recovery Plan) ต้องมอบหมายให้หน่วยงานที่เกี่ยวข้องดำเนินการ ดังต่อไปนี้

4.1 กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

4.2 กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

4.3 ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

4.4 จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

4.5 ทดสอบ/ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง อย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 10
การตรวจสอบและประเมินความเสี่ยง

1. วัตถุประสงค์

   เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

2. แนวปฏิบัติการประเมินความเสี่ยง

   2.1 ระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของบริษัทฯ เพื่อการประเมินความเสี่ยงนั้น ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย เนื่องจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error), ไวรัสคอมพิวเตอร์ (Computer Virus), ระบบไฟฟ้าขัดข้อง, ความเสียหายจากเพลิงไหม้ , โจรกรรม และการขโมยอุปกรณ์คอมพิวเตอร์

   2.2 กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

   2.3 การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

   2.3.1 ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

   2.3.2 ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

   2.3.3 จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

   2.4 กำหนดมาตรการจัดการความเสี่ยง

   2.4.1 ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ (IT Disaster Recovery Plan)

   2.4.2 จัดทำหลักเกณฑ์นโยบายกฎระเบียบในการใช้เครื่องคอมพิวเตอร์และเครือข่ายของบริษัทฯ

ส่วนที่ 11
นโยบายความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต
(Internet Security Policy)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความคำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของบริษัทฯ ถูกระงับชะลอขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

2.1 ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่บริษัทฯ จัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากหน่วยงานเทคโนโลยีและสารสนเทศเป็นลายลักษณ์อักษร

2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

2.3 ผู้ใช้หมั่น Update Patch และ Hotfix อย่างสม่ำเสมอ โดยสามารถ Download patch และ Hotfix ต่างๆ จาก Microsoft web site เพื่อแก้ปัญหาช่องโหว่

2.4 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

2.5 ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัทฯ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

2.6 ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัทฯ

2.7 ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับบริษัทฯ

2.8 ห้ามผู้ใช้ เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการ ผ่านอินเทอร์เน็ต

2.9 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอาย

2.10 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ 12
แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

1. วัตถุประสงค์
   1.1 เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของบริษัทฯ สามารถสนับสนุนการปฏิบัติงานและการบริหารงานของบริษัทฯ เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ และประสิทธิผล
   1.2 เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สำหรับพนักงานและหน่วยงาน เป็นมาตรฐานอยู่ในกรอบของกฎหมาย
2. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์
   2.1 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น
   2.2 ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ
   2.3 สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (default password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที
   2.4 รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น 'x' หรือ 'o' ในการพิมพ์แต่ละตัวอักษร
   2.5 ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง
   2.6 ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการล็อกเอ้าท์ออกจากหน้าจอ ตัดการใช้งานผู้ใช้ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง
   2.7 ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์
   2.8 ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน
   2.9 ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัทฯ หรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมายหรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่น แสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัทฯ
   2.10 ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านรับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน
   2.11 ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของบริษัทฯ เพื่อการทำงานของบริษัทฯ เท่านั้น
   2.12 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ เสร็จสิ้นควรทำการล็อกเอ้าท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
   2.13 ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

2.14 ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

2.15 ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของบริษัท ฯ ทำให้เกิดความแตกแยก ผ่านทางจดหมายอิเล็กทรอนิกส์

2.16 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

2.17 ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยเท่าที่จำเป็น

2.18 ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ 13
ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์
(Terms of Use and Disclaimer)

1. วัตถุประสงค์
   1.1 เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของบริษัทฯ สามารถสนับสนุนการปฏิบัติงานและการบริหารงานของบริษัทฯ เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ และประสิทธิผล
   1.2 เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สำหรับพนักงานและหน่วยงาน เป็นมาตรฐานอยู่ในกรอบของกฎหมาย
2. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัทฯ
   2.1 ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ จะต้องไม่กระทำการอันละเมิดต่อกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำอย่างน้อย ดังต่อไปนี้
      2.1.1 พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
      2.1.2 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
      2.1.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัทฯ
   3.1 หน่วยงาน/บุคคล ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัทฯ จะต้องใช้จดหมายอิเล็กทรอนิกส์ของบริษัทฯ เพื่อผลประโยชน์ของบริษัทฯ เท่านั้น
   3.2 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ เพื่อการประกอบธุรกิจหรือแสวงหาผลประโยชน์ส่วนตน
   3.3 ห้ามใช้บริการนี้ไปในการเผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใดๆ ที่ก่อให้เกิดความเสียหายต่อสถาบันชาติ ศาสนา และ พระมหากษัตริย์
   3.4 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ ในการประกอบอาชญากรรมทางคอมพิวเตอร์หรือการกระทำการใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับของบริษัทฯ
   3.5 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ เพื่อการเผยแพร่ข้อมูลข่าวสาร หรือภาพ เสียง ข้อความ ที่ไม่เหมาะสมหรือสร้างความเสื่อมเสียให้กับผู้อื่น
   3.6 ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบ หรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือองค์กร
   3.7 ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (Impersonation)
   3.8 ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น
      3.8.1 การสร้างจดหมายลูกโซ่ (Chain mail)
      3.8.2 การส่งจดหมายจำนวนมาก (Spam mail)
      3.8.3 การส่งจดหมายต่อเนื่อง (Letter bomb)
      3.8.4 การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

3.9 ห้ามผู้ใช้บริการกระทำการใดๆ ที่อาจจะนำมาซึ่งความเสื่อมเสีย หรือก่อให้เกิดความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของบริษัทฯ

3.10 ผู้ใช้ต้องรักษารหัสผ่าน (Password) ส่วนบุคคลหรือหน่วยงานของจดหมายอิเล็กทรอนิกส์ ไว้เป็นความลับ

3.11 ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทฯ ให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับกิจการของบริษัทฯ

3.12 การส่งข้อมูลข่าวสารที่เป็นความลับของบริษัทฯ ให้กับบุคคลหรือหน่วยงานนอกบริษัทฯ จะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่บริษัทฯ กำหนด

3.13 ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail address) และรหัสผ่าน (Password) ของหน่วยงานหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับ หากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)

3.14 ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัทฯ หรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์จะต้องศึกษาคู่มือการใช้งานระเบียบปฏิบัติคำแนะนำและข้อตกลงเงื่อนไข ให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของบริษัทฯ ได้อย่างถูกต้อง

3.15 กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยข้อบังคับ กฎหมาย ขอสงวนสิทธิ์ที่จะทำการ ยกเลิก หรือระงับบริการแก่ผู้ใช้บริการนั้นๆ เป็นการชั่วคราวเพื่อทำการสอบสวน และตรวจสอบหาสาเหตุของมูลเหตุนั้นๆ

3.16 การกระทำใดๆ ที่เกี่ยวกับการเผยแพร่ ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์และ/หรือโฮมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการ แผนกเทคโนโลยีและสารสนเทศ ไม่มีส่วนเกี่ยวข้องใดๆ

ส่วนที่ 14
การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
(Third party access control)

1. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้องและการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ ให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือกควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบการใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

2. แนวทางปฏิบัติ

2.1 ผู้บริหารหน่วยงานเทคโนโลยีและสารสนเทศ ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

2.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหนวยงานภายนอก

2.2.1 บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้บริหารหน่วยงานเทคโนโลยีและสารสนเทศ หรือผู้มีอำนาจ

2.2.2 จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

- เหตุผลในการขอใช้
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
- การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
- การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

2.2.3 หน่วยงานภายนอกที่ทำงานให้กับบริษัทฯ ทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในบริษัทฯ หรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของบริษัทฯ โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

2.2.4 บริษัทฯ ควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่เข้าไปปฏิบัติงาน

2.2.5 เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

2.2.6 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของบริษัทฯ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และ การรักษาความพร้อมที่จะให้บริการ (Availability)

2.2.7 บริษัทฯ มีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจได้ว่าบริษัทฯ สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

2.2.8 ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ 15
นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย
(Wireless Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. แนวทางปฏิบัติ

1. ผู้ดูแลระบบเครือข่ายไร้สายมีหน้าที่ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

1.1 เครือข่ายของบริษัทฯ เป็นสมบัติของบริษัทฯ ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้าม ต้องได้รับโทษจากทางบริษัทฯ และรับโทษตามกฎหมาย

1.2 ผู้ดูแลระบบต้องวางตัวกระจายสัญญาณไร้สาย (Access Point) ในตำแหน่งที่เหมาะสม โดยไม่ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายของบริษัทฯ

1.3 การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องติดตั้งโดยการแยกเครือข่ายไร้สายออกจากระบบเครือข่ายภายใน LAN เพื่อป้องกันการเข้าถึงจากบุคคลภายนอก

1.4 การกำหนดการเข้าถึงระบบเครือข่ายไร้สาย ต้องแบ่งแยกการใช้งานให้แตกต่างกันตามความจำเป็นของผู้ใช้งาน และกำหนดรหัสการเข้าใช้งานตามวัตถุประสงค์ของการใช้งาน

1.5 ให้กำหนดรายการที่สามารถเข้าใช้ระบบเครือข่ายได้ เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และ รหัสผ่าน (Password) ที่กำหนดไว้เท่านั้น

1.6 ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่ามาจากโรงงานผู้ผลิตให้เป็นอย่างอื่น

1.7 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

1.8 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้น ในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแล ระบบรายงานให้ผู้บริหารหน่วยงานทราบทันที

2. ผู้ใช้งานระบบเครือข่ายไร้สายของบริษัทฯ มีหน้าที่ความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

2.1 ห้ามผู้ใช้งานนำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในบริษัทฯ ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

2.2 บริษัทฯ ให้บัญชีผู้ใช้งานเป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน จำหน่าย หรือแจกจ่ายสิทธินี้ให้กับผู้อื่นไม่ได้

2.3 บัญชีผู้ใช้งานที่บริษัทฯ ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งานนั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

2.4 ห้ามผู้ใช้งานปฏิบัติการใดๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของบริษัทฯ

2.5 บริษัทฯ ไม่อนุญาตให้ผู้ใช้งานทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไร ผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

2.6 ผู้ใช้งานจะต้องไม่อ่าน, เขียน, ลบ, เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user account) ของผู้อื่น หรือพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัย รวมไปถึงเข้าสู่เครื่องคอมพิวเตอร์ของหน่วยงานอื่นๆ ของบริษัทฯ การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว บริษัทฯ ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

2.7 ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไข ในการรับทราบกฎระเบียบ หรือนโยบายต่างๆ ที่บริษัทฯ กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบ หรือนโยบายของบริษัทฯ มิได้

2.8 บริษัทฯ ทรงไว้ซึ่งสิทธิที่จะปฏิเสธการเชื่อมต่อและ/หรือการใช้งาน และทรงไว้ซึ่งสิทธิที่จะยกเลิกหรือระงับการเชื่อมต่อและ/หรือการใช้งานใดๆ ของผู้ใช้งานที่ละเมิดหรือพยายามจะละเมิดกฎระเบียบนี้ของบริษัทฯ โดยไม่มีการแจ้งให้ทราบก่อนล่วงหน้า

ส่วนที่ 16
การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

1. ระบบป้องกันผู้บุกรุก
   แผนดำเนินการรายวัน
   ดำเนินการตรวจสอบไฟล์ล็อกหรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบ ดังต่อไปนี้
   1.1 การโจมตีเกิดขึ้นมากน้อยเพียงใด การโจมตีประเภทใดเกิดขึ้นเป็นจำนวนมาก
   1.2 ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
   1.3 ระดับความรุนแรงมากน้อยเพียงใด
   1.4 หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี
2. ระบบไฟร์วอลล์
   2.1 ดำเนินการตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุกอย่างน้อยเดือนละ 1 ครั้ง
   2.2 ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของไฟล์วอลล์ สิ่งที่ต้องตรวจสอบ มีดังต่อไปนี้
      2.2.1 Packet ที่ไฟล์วอลล์ได้ทำการ Block
      2.2.2 ลักษณะของ Packet ที่ถูก Block
      2.2.3 Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก
   2.3 กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งผู้บริหารหน่วยงานเทคโนโลยีสารสนเทศ เพื่อตัดสินใจดำเนินการแก้ไขปัญหา
3. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต
   ภัยคุกคามทางอินเตอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเตอร์เน็ต โทรจัน รวมถึงสปายแวร์
   แผนดำเนินการรายวัน/รายสัปดาห์/รายเดือน
   3.1 ดำเนินการตรวจสอบไฟล์ล็อกและรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต สิ่งที่ควรตรวจสอบมีดังนี้
      3.1.1 มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
      3.1.2 มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
      3.1.3 มีการส่งมัลแวร์จากเครือข่ายภายในบริษัทฯ ไปยังภายนอกหรือไม่
   3.2 ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของบริษัทฯ
   3.3 ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ควรระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

การบังคับ

เจ้าหน้าที่ของ บริษัทอินเด็กซ์ ลิฟวิ่งมอลล์ จำกัด (ต่อจากนี้เรียกว่า "บริษัทฯ") ทุกท่าน และหมายรวมถึง บุคคลภายนอก ไม่ว่าจะเป็นคู่ค้า ผู้รับจ้างช่วง ผู้มีส่วนเกี่ยวข้อง ซึ่งได้รับอนุญาตให้ใช้งานระบบคอมพิวเตอร์ ระบบข้อมูลสารสนเทศของบริษัทฯ ทั้งหมด ต่อจากนี้เรียกว่า "ผู้ใช้งาน"

"ผู้ใช้งาน" มีหน้าที่ในการปฏิบัติตามนโยบาย และระเบียบปฏิบัติงานอื่นๆ ที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์ ระบบข้อมูลสารสนเทศตามที่องค์กรได้กำหนดไว้อย่างเคร่งครัด หากตรวจสอบพบว่า "ผู้ใช้งาน" ได้ใช้งานระบบคอมพิวเตอร์ และ/หรือระบบข้อมูลสารสนเทศของบริษัทฯ มีการกระทำอันหนึ่งอันใดเป็นการละเมิด หรือขัดแย้งต่อนโยบาย และระเบียบปฏิบัติอื่นๆ ตามที่ได้กล่าวมาในข้างต้นนั้น บริษัทฯ ขอสงวนสิทธิในการดำเนินการทางวินัยตามระเบียบข้อบังคับในการปฏิบัติงานของบริษัทฯ ถึงขั้นสูงสุด และจะพิจารณาเพื่อดำเนินคดีตามกฎหมายที่เกี่ยวข้องทันที

การพ้นสภาพของพนักงาน

ข้อมูลความลับ สูตร กรรมวิธีการทำงาน ข้อมูลภายในของบริษัทฯ ข้อมูลอื่นใดอันจัดเป็นทรัพย์สินทางปัญญาของบริษัทฯ รวมทั้งข้อมูลอื่นๆที่สื่อสารผ่านระบบคอมพิวเตอร์ หรือระบบข้อมูลสารสนเทศ ซึ่ง "ผู้ใช้งาน" อาจได้รับ และ/หรืออาจมีสิทธิเข้าถึงผ่านระบบคอมพิวเตอร์ ระบบข้อมูลสารสนเทศของบริษัทฯ ตามนโยบาย และระเบียบปฏิบัติต่างๆที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์ ระบบข้อมูลสารสนเทศนั้น "ผู้ใช้งาน" มีข้อผูกพันในการห้ามเผยแพร่ข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 3 ปี โดยนับตั้งแต่วันที่ "ผู้ใช้งาน" พ้นสภาพจากการเป็น "ผู้ใช้งาน" ของบริษัทฯ (หรือห้ามเผยแพร่ข้อมูลดังกล่าวตามเงื่อนไข และระยะเวลาตามที่บริษัทฯ ได้กำหนดไว้ในระเบียบปฏิบัติ หรือสัญญาฉบับอื่นๆที่บริษัทฯ ได้ทำไว้กับ "ผู้ใช้งาน" โดยให้บังคับใช้สัญญาฉบับที่มีเงื่อนไข และระยะเวลาที่เข้มงวดที่สุด)

เอกสารอ้างอิง (REFERENCE) และแบบฟอร์ม (FORM)

ลำดับที่	รหัส-ชื่อเอกสาร	คำอธิบายการใช้

ตาราง เอกสารอ้างอิง (REFERENCE) และแบบฟอร์ม (FORM)