นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัท โนวา ออร์แกนิค จำกัด (มหาชน)

จัดทำครั้งที่	00
วันที่มีผลบังคับใช้	12/07/2564
จัดเตรียมโดย	..... (นางสาวหฤทัย สิริสินวิบูลย์) เลขานุการบริษัท
อนุมัติโดย	..... (นายประกิจ ตังติสานนท์) ประธานกรรมการบริษัท

สารบัญ

1. หลักการและเหตุผล

บริษัท โนวา ออร์แกนิค จำกัด (มหาชน) ตระหนักถึงความสำคัญของการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการธุรกิจ จึงกำหนดนโยบายฉบับนี้เพื่อให้บริษัทมีกรอบการกำกับดูแลและ บริหารจัดการเทคโนโลยีสารสนเทศระดับบริษัท ที่ดีโดยอ้างอิงหลักการจากหลักเกณฑ์และแนวปฏิบัติในการ จัดให้มี ระบบเทคโนโลยีสารสนเทศ แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ของ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ตลอดจนกฎหมายอื่นที่เกี่ยวข้อง มาปรับใช้ให้ เหมาะสมกับบริบทการดำเนินธุรกิจของบริษัท ซึ่งกำหนดนโยบายการดำเนินการด้านเทคโนโลยีสารสนเทศของ บริษัท ดังนี้

1) นโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ
2) นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
3) นโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

2. วัตถุประสงค์

เพื่อให้บริษัทมีกรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับบริษัท ที่สอดคล้อง กับความต้องการของกิจการ รวมทั้งดูแลให้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการสนับสนุนและพัฒนาการ ดำเนินธุรกิจ การบริหารความเสี่ยง รวมถึงเพื่อให้กิจการสามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของกิจการ โดยมีการใช้ทรัพยากรและการบริหารจัดการความเสี่ยงอย่างเหมาะสมสอดคล้องกับการกำกับดูแลกิจการที่ดี

3. ขอบเขตการบังคับใช้

นโยบายฉบับนี้มีผลบังคับใช้กับ บริษัท โนวา ออร์แกนิค จำกัด (มหาชน) โดยนโยบายหลักเกณฑ์ ระเบียบปฏิบัติและคำสั่งที่ใช้อยู่ก่อนนโยบายฉบับนี้ ให้ยังมีผลใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับนโยบายฉบับนี้

4. คำจำกัดความ

คำศัพท์	คำนิยาม
บริษัท	บริษัท โนวา ออร์แกนิค จำกัด (มหาชน)
ประธานเจ้าหน้าที่สายงาน	ประธานเจ้าหน้าที่สายงานของ บริษัท โนวา ออร์แกนิค จำกัด (มหาชน)
ฝ่ายบริหาร	กรรมการ และ ประธานเจ้าหน้าที่สายงานต่างๆ ของบริษัท
นโยบาย ฯ	นโยบายเทคโนโลยีสารสนเทศ
หน่วยงานเทคโนโลยีสารสนเทศ	หน่วยงานตามโครงสร้างของบริษัทที่มีหน้าที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ
ผู้ใช้งาน	พนักงานประจำ พนักงานตามสัญญาจ้าง ผู้ให้บริการภายนอก คู่ค้าหรือลูกค้า
ผู้ให้บริการภายนอก	บุคคลจากภายนอกบริษัท ซึ่งผู้ประกอบธุรกิจ ว่าจ้างเพื่อใช้บริการที่เกี่ยวข้อง กับระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศ
ระบบเทคโนโลยีสารสนเทศ	ระบบคอมพิวเตอร์ที่หน่วยงานเทคโนโลยีสารสนเทศให้บริการ
บุคลากร	เจ้าหน้าที่หรือพนักงานภายใต้หน่วยงานเทคโนโลยีสารสนเทศ และผู้ให้บริการภายนอก
เครื่องมือ	วิธีดำเนินการจัดการด้านเทคโนโลยีสารสนเทศ
ทรัพยากรด้านเทคโนโลยีสารสนเทศ	1) ระบบเทคโนโลยีสารสนเทศ 2) บุคลากร 3) อุปกรณ์คอมพิวเตอร์
ทรัพย์สินสารสนเทศ	1) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ 2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ 4) ทรัพย์สินสารสนเทศประเภทลิขสิทธิ์ คือ ทรัพย์สินที่เกิดการพัฒนาหรือ สิทธิ์ในการใช้จากเจ้าของผลิตภัณฑ์

คำศัพท์	คำนิยาม
สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล	อุปกรณ์ ระบบงาน หรือสภาพแวดล้อม ที่จำเป็นหรือมีส่วนช่วยในการประมวลผลข้อมูลเป็นไปอย่างครบถ้วน ถูกต้อง และมีประสิทธิภาพ เช่น

5. บทบาทหน้าที่และความรับผิดชอบ

5.1 คณะกรรมการบริษัท

5.1.1 กำหนดนโยบายเทคโนโลยีสารสนเทศของบริษัท

5.1.2 กำกับดูแลให้ฝ่ายบริหารปฏิบัติตามนโยบายฯ ให้สอดคล้องกับความต้องการของบริษัท รวมทั้ง สนับสนุนและพัฒนาการดำเนินธุรกิจ การบริหารความเสี่ยง เพื่อให้สามารถบรรลุวัตถุประสงค์ และเป้าหมายหลักของบริษัท

5.1.3 ทบทวนหรือปรับปรุงนโยบายฯ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผล กระทบต่อการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ

5.2 ฝ่ายบริหาร

5.2.1 กำหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติที่เกี่ยวข้องกับนโยบาย ฯ

5.2.2 ติดตามควบคุมและกำกับดูแลให้หน่วยงานที่เกี่ยวข้องดำเนินการตามนโยบายฯที่กำหนด

5.3 หน่วยงานเทคโนโลยีสารสนเทศ

5.3.1 ติดตามดูแลให้ผู้ใช้งานปฏิบัติตามนโยบายฯ หลักเกณฑ์ระเบียบปฏิบัติของบริษัทที่เกี่ยวข้อง อย่าง ถูกต้องเหมาะสม และหากมีการปฏิบัติที่ไม่ถูกต้องให้รายงานต่อฝ่ายบริหารทราบ

5.3.2 สื่อสารนโยบายฯ ให้แก่ผู้ใช้งาน ผู้ประกอบธุรกิจที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายดังกล่าวได้อย่างถูกต้อง

หมวดที่ 1

การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศสำหรับบริษัท

1.1 บริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่บริษัท ยอมรับได้ โดยสร้างความร่วมมือจากทุกฝ่ายให้มีความรู้ความเข้าใจในทรัพย์สิน สารสนเทศ เพื่อทำให้ประสิทธิภาพของการดำเนินงานภายใต้ทรัพย์สินสารสนเทศมีค่าสูงสุด

1.2 จัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนิน ธุรกิจ และการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้ตามที่กำหนดไว้ เช่น

1.2.1 ฝ่ายบริหาร มีการวางแผน หรือมีนโยบายในการจัดสรรบุคคลากร

1.2.2 ฝ่ายบุคคล

1) ประกาศ และรับพนักงานตามนโยบาย

2) แจ้งผู้ดูแลระบบ เพื่อจัดเตรียมทรัพย์สินสารสนเทศให้เหมาะสมและเพียงพอตามนโยบาย

1.2.3 ผู้ดูแลระบบ

1) จัดสรร โอนย้าย หรือจัดซื้อทรัพย์สินสารสนเทศตามตำแหน่งความรับผิดชอบ

2) ทำทะเบียนควบคุมทรัพย์สินสารสนเทศ และจัดทำสำเนาเอกสารที่เกี่ยวข้องแยกเก็บเพื่อสะดวกต่อการ ตรวจสอบ เช่น ใบกำกับภาษี สำหรับเครื่องคอมพิวเตอร์ อุปกรณ์ ลิขสิทธิ์ (License) กรณีที่เป็นการโอนย้ายจากสำนักงานใหญ่ไปยังสาขาต้องทำการสำเนาเอกสารดังกล่าวแยกเก็บด้วย

1.2.4 ฝ่ายจัดซื้อ จัดซื้อทรัพย์สินสารสนเทศ (กรณีไม่มีทรัพย์สินสารสนเทศสำรอง)

1.2.5 ฝ่ายบัญชี/การเงิน ทำการขึ้นทะเบียนทรัพย์สินสารสนเทศ

1.2.6 อื่น ๆ

1.3 การกำกับดูแลระบบสารสนเทศเกี่ยวข้องกับทรัพยากรบุคคล

1.3.1 ก่อนการจ้างงาน

1) บริษัทต้องกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ในคุณสมบัติของบุคลากรตามหน้าที่งานที่ได้รับมอบหมายส่วนบริหารทรัพยากรบุคคลต้องตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นบุคลากรของบริษัท ต้องตรวจสอบประวัติอาชญากรรม หรืออื่นๆ ตามเงื่อนไขที่เกี่ยวข้อง

2) การกำหนดเงื่อนไขการจ้างงาน โดยส่วนบริหารทรัพยกรบุคคลเป็นผู้กำหนดรวมถึงเงื่อนไขและหน้าที่รับผิดชอบต่อความมั่นคงปลอดของสารสนเทศของบริษัท

3) เพื่อให้การบริหารจัดการ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ส่วนบริหารทรัพยากรบุคคล ต้องแจ้งส่วนงานที่รับผิดชอบทราบทันที่เมื่อมีการดำเนินการ ดังต่อไปนี้

- การจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกหรือการสิ้นสุดสภาพการเป็นบุคลากร
- การโอนย้ายส่วนงาน
- การพักงาน การลงโทษทางวินัยหรือระงับการปฏิบัติหน้าที่

1.3.2 ระหว่างการจ้างงาน

1) การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่เจ้าหน้าที่อย่างน้อยปีละ 1 ครั้ง

2) เจ้าหน้าที่ใหม่ของบริษัทต้องได้รับการอบรมเกี่ยวกับนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยจัดเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการบันทึกการอบรมและเก็บรวบรวมไว้ในระบบ

3) ส่วนงานที่รับผิดชอบต้องแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้ายสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท

1.3.3 การเปลี่ยนแปลงตำแหน่งหรือสิ้นสุดการจ้างงาน

1) ส่วนงานที่รับผิดชอบ ด้วยดำเนินการเปลี่ยนแปลงและส่งมอบข้อมูลเพื่อให้แผนกสารสนเทศจัดการกับข้อมูลสิทธิ์ผู้ใช้งานที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศเพื่อให้สอดคล้องกับการเปลี่ยนแปลงของสถานะการว่าจ้าง โดยต้องเก็บข้อมูลเพื่อให้สามารถตรวจสอบประวัติการเปลี่ยนแปลงสิทธิ์ในระบบสารสนเทศที่เกิดขึ้นเหล่านั้นได้

2) เมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน ผู้ใช้งานต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นไปของบริษัท ได้แก่ อุปกรณ์ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก หรืออุปกรณ์ใดๆที่เป็นสินทรัพย์ของบริษัทให้แก่บริษัททันที

1.4 การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศต้องมีความสอดคล้องกันแผน กลยุทธ์บริษัท เพื่อให้บรรลุเป้าหมายตามภารกิจ กลยุทธ์และแผนการดำเนินงานที่กำหนดไว้ โดยมีการปฏิบัติ ดังนี้

1) กำหนดหลักเกณฑ์และปัจจัยในการจัดลำดับความสำคัญของแผนงานด้านเทคโนโลยีสารสนเทศ เช่น ความเหมาะสมสอดคล้องกับแผนกลยุทธ์ของบริษัท ผลกระทบต่อการดำเนินธุรกิจ ความเร่งด่วนใน การใช้งาน เป็นต้น

2) จัดทำและอนุมัติงบประมาณด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับแผนงบประมาณและแผนกลยุทธ์บริษัท

3) จัดให้มีทรัพยากรบุคคลอย่างเพียงพอต่องานด้านเทคโนโลยีสารสนเทศ จัดให้มีหรือการพัฒนาทักษะ ของบุคลากร และจัดจ้างบุคลากรด้านเทคโนโลยีสารสนเทศจากภายนอก

4) จัดการความเสี่ยงในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ ไม่ว่าจะเป็นบุคลากร งบประมาณหรือความต้องการใช้งานเกินกว่าที่กำหนดไว้

5) กำหนดหน้าที่และความรับผิดชอบของบุคลากรของหน่วยงานเทคโนโลยีสารสนเทศในการจัดสรร และบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศของบริษัท

6) ต้องมีการจัดทำบัญชีสินทรัพย์รวมถึงครุภัณฑ์คอมพิวเตอร์และบัญชีข้อมูลที่เก็บไว้ในส่วนต่างๆ ของบริษัท และแบ่งประเภทชัดเจน เพื่อให้ในการกำหนดมูลค่าสินทรัพย์ โดยระบุผู้เป็นเจ้าของสินทรัพย์แต่ละชนิดต่างที่กำหนดไว้ และต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ตามระยะเวลาที่กำหนดอย่างน้อยปีละ 1 ครั้ง

7) สินทรัพย์ที่เป็นซอฟต์แวร์ที่ใช้สำหรับการดำเนินงานของบริษัทซึ่งไม่มีค่าลิขสิทธิ์ หากส่วนงานใดมีการใช้งานให้ทำทะเบียนไว้ที่ส่วนงาน และให้ส่งสำเนาดังกล่าวที่แผนกสารสนเทศซึ่งเป็นผู้รับผิดชอบในการจัดการข้อมูลและสินทรัพย์ของบริษัท เพื่อประโยชน์ในการค้นหาติดตามและสำรวจช่องโหว่ที่อาจจะมีผลกระทบต่อความมั่นคงปลอดภัยในระบบสารสนเทศ

8) อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ซอฟต์แวร์ หรือระบบงานคอมพิวเตอร์ที่บริษัทเช่ามาใช้งาน ต้องกำหนดให้มีส่วนงานที่รับผิดชอบต้องจัดทำบัญชีรายการของอุปกรณ์ ซอฟต์แวร์ หรือระบบงานคอมพิวเตอร์ที่เช่ามาใช้งาน

9) การใช้งานสินทรัพย์ต้องใช้งานด้วยความระมัดระวัง บำรุงรักษาให้เหมาะสมกับการใช้งาน

10)ควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงข้อมูล และสิ่งอำนวยความสะดวกในการประมวลผลข้อมูล

11)สร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจ หน้าที่เกี่ยวข้องเข้าถึงสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ ซึ่งอาจก่อให้เกิด ความเสียหายต่ออุปกรณ์สารสนเทศหรือมีผลกระทบต่อข้อมูลที่เป็นความลับหรือมีความสำคัญ

หมวดที่ 2
การกำหนดนโยบาย มาตรการ โครงสร้างการบริหารจัดการ เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ การบริหารจัดการทรัพย์สินสารสนเทศ และการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

2.1 การจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2.1.1 การติดตั้งระบบป้องกันการบุกรุก (Firewall)

2.1.2 การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ มัลแวร์ รวมถึงการปรับปรุง Security Patch อยู่ เสมอ

2.1.3 การกำหนดสิทธิ์การเข้าถึง หรือการเข้าใช้ข้อมูลสำหรับเครื่องคอมพิวเตอร์แม่ข่ายของแต่ละผู้ใช้ หรือแต่ละกลุ่ม ของผู้ใช้งาน

2.1.4 การกำหนดสิทธิ์การใช้อุปกรณ์ต่อพ่วงผ่าน USB Port กรณีที่ต้องการใช้ ต้องทำเอกสาร ขออนุมัติผ่านหัวหน้างาน ผู้มีอำนาจ หรือผู้บริหาร พร้อมส่งเอกสารมายังผู้ดูแลระบบเพื่อดำเนินการ

2.1.5 การกำหนดสิทธิ์การใช้งานสื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (อาทิ Thumb-Drive, CD, DVD) ที่มีข้อมูลลับของบริษัทฯ บันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง กรณีที่เป็นอุปกรณ์ ส่วนตัวต้องมีการขึ้นทะเบียน รวมถึงต้องทำเอกสารขออนุมัติผ่านหัวหน้างาน ผู้มีอำนาจ หรือผู้บริหาร พร้อมส่ง เอกสารมายังผู้ดูแลระบบเพื่อดำเนินการก่อนการใช้งานเสมอ

2.1.6 ข้อมูลที่เกี่ยวข้องกับการดำเนินงานของบริษัทฯ ทั้งที่มีการเก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือ เครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลโดยผู้ดูแลระบบต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการ กู้คืนข้อมูลเมื่อมีปัญหาเกิดขึ้น

2.1.7 การสำรองข้อมูลควรจัดเก็บอย่างน้อย 2 สถานที่ เช่น สำนักงานใหญ่ และสาขา เป็นต้น

2.1.8 ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ของบริษัทฯ อย่างระมัดระวัง และ ให้การปกป้องเสมือนเป็นสินทรัพย์ของตน กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบอุปกรณ์ คอมพิวเตอร์ของบริษัทฯ ที่ได้รับมอบหมาย

2.1.9 เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งหมดของบริษัทฯ ต้องได้รับการ ปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้ง ควร Log Off คอมพิวเตอร์ทุกครั้งเมื่อไม่ได้ใช้งาน

2.1.10 ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัทฯ ทั้งที่ได้มาจากการ พัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมาต้องได้รับการตรวจสอบ ควบคุม และอนุมัติ อย่างเหมาะสมโดย หน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของบริษัทฯ

2.1.11 ผู้ใช้งานพึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ ไม่ Download/ Upload ข้อมูลหรือ สิ่งอื่นใดที่ ไม่เกี่ยวข้องกับงาน กรณีที่เข้าใช้งานอินเทอร์เน็ตห้ามมิให้ผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป็อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่ไม่มีความเกี่ยวข้องกับงาน เนื่องจากอาจมีโปรแกรมในการโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ ของผู้ใช้งาน หรือใช้ Website ที่ไม่เกี่ยวข้องกับงานหรือกิจการของบริษัทฯ การใช้งานต้องไม่เป็นสาเหตุให้บริษัทฯ และบุคคลอื่นเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำผิดกฎหมาย หรือ พรบ. คอมพิวเตอร์ ทั้งนี้บริษัทฯ สงวนสิทธิ์ในการตรวจสอบ และบันทึกประวัติการใช้คอมพิวเตอร์ของผู้ใช้งานเพื่อตรวจสอบการเข้าใช้งานใน ลักษณะที่ไม่เหมาะสม

2.1.12 จัดอบรมให้ความรู้แก่ผู้ใช้งาน เกี่ยวกับความความสำคัญ แนวปฏิบัติ ขั้นตอนการปฏิบัติงาน และความเสี่ยง เพื่อป้องกัน และสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศ ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับ กฎหมาย ข้อกำหนด นโยบาย และการเปลี่ยนแปลงที่เกี่ยวข้องด้านทรัพย์สินสารสนเทศของบริษัทฯ ด้วย

2.1.13 ทำการปรับปรุงเอกสารทะเบียนควบคุมทรัพย์สินสารสนเทศ อย่างสม่ำเสมอ

2.1.14 ทบทวน และปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง ควรปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับ นโยบายที่มีการเปลี่ยนแปลงด้วย

2.2 การใช้งานอีเมล์ (E-mail)

2.2.1 บัญชีอีเมล์ต้องได้รับการปกป้องด้วยรหัสผ่าน

2.2.2 บัญชีอีเมล์ทั้งหมด และอีเมล์ทุกฉบับ (รวมถึงอีเมล์ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัทฯ ถือเป็นสินทรัพย์ของบริษัทฯ

2.2.3 พื้นที่เก็บอีเมล์บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้เมื่อ ปริมาณของอีเมล์มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ และถ้าหากปริมาณของอีเมล์มากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับ-ส่งอีเมล์ได้ตามปกติอีกต่อไป หาก อีเมล์และไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายแจ้งว่าไม่สามารถส่งอีเมล์ดังกล่าวได้ ผู้ใช้งานต้องลบอีเมล์ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็น การรักษาพื้นที่เก็บอีเมล์ให้เป็นไป ตามขนาดที่บริษัทฯ กำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงานและอีเมล์ ตามที่กฎหมายกำหนดไว้เท่านั้น

2.2.4 ห้ามใช้บัญชีอีเมล์ของบริษัทฯ เพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย พรบ. ข้อกำหนด และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือนโยบาย ต่าง ๆ ที่บริษัทฯ ได้ประกาศไว้ หากพบว่ามีการส่งข้อมูลที่ผิดต่อพระราชบัญญัติวาด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือผิดต่อกฎระเบียบของ บริษัทให้แจ้งต่อผู้บังคับบัญชาโดยตรงหรือเจ้าหน้าที่หน่วยงานคอมพิวเตอร์

2.2.5 ซอฟต์แวร์สำหรับใช้งานอีเมล์ต้องได้รับการตั้งค่าให้อีเมล์ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้น ต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงาน ชื่อบริษัท และเบอร์โทรศัพท์ติดต่ออีเมล์บริษัทฯ ทุกฉบับต้อง มีข้อความแสดงเจตจำนง/ ข้อยกเว้นความรับผิดชอบของบริษัทฯ แนบท้าย กรณีที่เป็นอีเมล์ติดต่อลูกค้าให้กำกับ ข้อมูลการชำระเงิน เช่น เลขบัญชี ชื่อบัญชี ประเภทบัญชีสำหรับรับชำระเงิน ว่าไม่มีการเปลี่ยนแปลงใด ๆ เพื่อ ป้องกันการปลอมแปลงโจรกรรมข้อมูล การหลอกลวงทางอินเทอร์เน็ต (Phishing Mail) เพื่อให้ได้ข้อมูล หรือ หลอกลวงให้ลูกค้าชำระเงินด้วยช่องทางอื่น ๆ

2.2.6 ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง ให้ใช้ข้อความสุภาพในการส่งจดหมายอิเล็คทรอนิกส์ การสนทนา หรือการสื่อสารทางอิเล็คทรอนิกส์อื่นๆโดยคำนึงอยู่เสมอว่าอีเมล์ที่ส่งออกนั้นกระทำในนาม ตัวแทนของบริษัทฯ ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหาหรือรูปภาพที่ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศหรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรมหรือ ศาสนา รวมถึงอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบัน พระมหากษัตริย์โดยเด็ดขาด หรือไฟล์อื่นใดที่ ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อบริษัทฯ

2.2.7 ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบ นั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)

2.2.8 เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์มีไวรัส ผู้ใช้งานต้องระงับ การส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

2.2.9 ในการติดต่อสื่อสารทางอิเล็คทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็คทรอนิกส์ การสนทนา หรือการติดต่อสื่อสารใดๆ ให้ถือเสมือนหนึ่งการส่งจดหมายแบบเป็นทางการโดยจะต้องปฏิบัติตามกฎการรับ-ส่งหนังสือหรือจดหมายของ บริษัท ได้แก่

1) การรักษาความลับของเอกสารด้วยการกำหนดมาตรฐานของการส่งอีเมล์หรือไฟล์ มีการใส่คำเฉพาะเพื่อไม่ให้เอกสารถูกส่งออกด้านนอก

2) ห้ามส่งเอกสารความลับโดยจดหมายอิเล็คทรอนิกส์ยกเว้นได้รับการเข้ารหัสโดยได้รับการยืนยันจากหน่วยงานคอมพิวเตอร์

2.2.10 ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อบริษัท หรือบุคคลอื่นๆ

2.2.11 จดหมายอิเล็คทรอนิกส์หรือการสื่อสารทางอิเล็คทรอนิกส์ใดๆ โดยไม่ระบุชื่อผู้ส่ง (SPAM e-mail)

2.2.12 ไม่อนุญาตให้พนักงานใช้อีเมล (e-mail) อื่นใดที่ บริษัท ไม่ได้กำหนดให้ใช้

2.2.13 กำหนดมาตรฐานในการตั้งชื่อไฟล์การทำงานให้เป็นรูปแบบเดียวกัน เพื่อความเข้าใจง่ายและเป็นระเบียบปลอดภัย ตามประกาศภายในของบริษัท

2.3 นโยบายการบริหารความเสี่ยง

2.3.1 หน่วยงานเทคโนโลยีสารสนเทศระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT- related risk)

2.3.2 ประเมินความเสี่ยงซึ่งครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และความมีนัยสำคัญหรือ ผลกระทบที่จะเกิดขึ้น

2.3.3 กำหนดตัวชี้วัดระดับความเสี่ยงสำหรับความเสี่ยงสำคัญที่สอดคล้องกับ ความเสี่ยงที่ระบุตาม ข้อ 3.2.1 รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดดังกล่าว เพื่อให้สามารถบริหารและจัดการความเสี่ยง ได้อย่างเหมาะสมและทันต่อเหตุการณ์

2.3.4 กำหนดหน้าที่และความรับผิดชอบของผู้รับผิดชอบ และผู้ทำหน้าที่ ในการบริหารและจัดการ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2.4 การรักษาความปลอดภัยทางกายภาพ

2.4.1 ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย

2.4.2 อนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ดูแลระบบ ขอเข้าพื้นที่ โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต หรือ ไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชน หรือบัตร ประจำตัวอื่นที่ราชการออกให้ หรือแนบเอกสาร Plant Visit Gate Pass โดยผู้ดูแลระบบจะต้องจดบันทึกบุคคล การขอเข้า-ออก หรือเก็บเอกสาร Plant Visit Gate Pass เป็นหลักฐาน (ทั้งในกรณีที่อนุญาต และไม่อนุญาตใหเข้าพื้นที่) และต้องมีการบันทึก ข้อมูลการเข้าออกห้องคอมพิวเตอร์แม่ข่าย (Server Room/Data Center) ของ บุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี (หรือตามความเหมาะสม)

2.4.3 ไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server Room/Data Center) เว้นแต่จะได้รับ อนุญาตจากผู้ดูแลระบบ / ไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการ

ประกอบธุรกิจส่วนบุคคล / ไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใดๆ / ไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

2.5 การใช้งานระบบเครือข่ายจากเครื่องคอมพิวเตอร์ที่ไม่ใช่ทรัพย์สินสารสนเทศของบริษัทฯ จะต้องได้รับอนุญาตจากผู้ดูแล ระบบก่อน และหากพบว่ามีการใช้งานโดยไม่ได้รับอนุญาต ผู้ดูแลระบบสามารถตัดการใช้งานออกจากระบบเครือข่ายได้ทันที กรณีที่ผู้ใช้งานทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนทรัพย์สินสารสนเทศของบริษัทฯ ผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

2.6 การควบคุมดูแลผู้ให้บริการภายนอก มีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการด้านเทคโนโลยีสารสนเทศของหน่วยงานภายนอกโดยต้องประกอบไป ด้วยรายละเอียดดังนี้

2.6.1 ผู้บริการภายนอกต้องยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ และถูกควบคุมความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อป้องกัน ทรัพย์สินสารสนเทศของบริษัทจากการเข้าถึงอย่างไม่เหมาะสมโดยผู้ให้บริการภายนอก

2.6.2 ขอบเขต รายละเอียด และระดับการให้บริการ (Service Level Agreement)

2.6.3 เอกสารต่าง ๆ เกี่ยวกับมาตรการการควบคุมที่ใช้ทั้งด้านกายภาพและด้าน Logical

2.6.4 กำหนดนโยบายสำหรับคู่ค้าหรือผู้รับจ้าง (Vendor) ในหัวข้อเรื่องการเปิดเผยข้อมูล ข้อมูลที่สามารถเข้าถึงได้สำหรับการทำงาน และสิทธิ์เข้าถึงสำหรับ Server และฐานข้อมูล การยืมหรือการร้องขอใช้อุปกรณ์ของบริษัทฯ รวมถึงการต่อพ่วงอุปกรณ์ภายนอกอื่น ๆ รวมถึงข้อตกลงการเชื่อมโยงระบบเครือข่ายของหน่วยงานภายนอก โดยเป็นไปตามประกาศของบริษัท

2.6.5 ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัท เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท โดยสอดคล้องกับข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูลของบริษัทต้องสื่อสาร และบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัท ข้อกำหนดทางด้านกฎหมาย เช่น ความลับส่วนบุคคล (Privacy) และการป้องกันข้อมูล เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.6.6 กำหนดให้ผู้ดูแลระบบมีการติดตาม ทบทวน และตรวจสอบประเมินการให้บริการภายนอกอย่างสม่ำเสมอตามข้อตกลงที่กำหนดไว้

2.6.7 ให้ผู้ดูแลระบบเป็นผู้รับผิดชอบในการบริหารจัดการการเปลี่ยนแปลงในการให้บริการฯ จากผู้ให้บริการภายนอก รวมถึงการประเมินผู้บริการ เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคง ปลอดภัยสารสนเทศได้ทั้ง 3 ด้านคือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

2.6.8 กำหนดให้ผู้ดูแลระบบเป็นผู้ควบคุมการส่งมอบงานของผู้ให้บริการภายนอก ให้เป็นไป

ตามข้อตกลงที่จัดทำไว้กับผู้ประกอบธุรกิจ

2.6.9 หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญ จะต้องทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

2.6.10 ควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศ (Change management) ต้องมีการกำหนดผู้รับผิดชอบและผู้มีอำนาจในการเปลี่ยนแปลงการควบคุมปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศของบริษัท

2.6.11 ให้มีการจัดเก็บหลักฐานการปฏิบัติงานที่สามารถใช้ตรวจสอบได้ในภายหลังการแยกระบบสำหรับการพัฒนาการทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)

2.6.12 ให้กำหนดมาตรการแยกเครื่องคอมพิวเตอร์ของระบบงาน สำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกันตามความจำเป็นเพื่อป้องกันผลกระทบจากการทำงาน

2.6.13 กำหนดมาตรการควบคุมการถ่ายโอนระบบงานจากเครื่องที่ใช้สำหรับการพัฒนาไปสู่เครื่องที่ใช้สำหรับการให้บริการ

2.6.14 ให้มีการป้องกันการเข้าถึงเครื่องมือในการพัฒนาและอรรถประโยชน์ (Software tool and Utility) ที่ใช้สำหรับการพัฒนาระบบงานโดยไม่ได้รับอนุญาต

2.6.15 กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากกันสำหรับระบบงานที่ใช้ในการพัฒนา ทดสอบและใช้ระบบงานจริง

2.6.16 การพัฒนาและดูแลรักษาระบบสารสนเทศกำหนดให้มีการรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศ เพื่อให้การพัฒนาหรือ แก้ไขเปลี่ยนแปลงระบบสารสนเทศประมวลผลได้อย่างถูกต้องครบถ้วนและเป็นไปตามความต้องการของ ผู้ใช้งาน รวมถึงการรักษาไว้ซึ่งความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนาระบบงานสารสนเทศ

2.7 นโยบายการบริหารความต่อเนื่องทางธุรกิจของบริษัท

2.7.1 บริษัทกำหนดให้การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจของบริษัท เพื่อให้ระบบสารสนเทศ อยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

2.7.2 ส่วนเทคโนโลยีสารสนเทศ ต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดขึ้นกับระบบสารสนเทศ ตามแผนบริหารภาวะวิกฤต (Crisis Management Plan) ของบริษัท

2.7.3 ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้นอย่างน้อยปีละ 1 ครั้ง

2.7.4 ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

2.7.5 ต้องมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรอง อย่างน้อยปีละ 1 ครั้ง

2.7.6 การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

2.8 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท

2.8.1 บริษัทกำหนดขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย ของระบบสารสนเทศ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถ และประสบการณ์ รวมถึง จัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ ผ่านบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับ การดำเนินการอย่างถูกต้อง มีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม

2.8.2 ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท

2.8.3 ต้องกำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน

2.8.4 หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ต้องแจ้งเหตุการณ์ดังกล่าวต่อส่วนเทคโนโลยีสารสนเทศ

2.8.5 กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใชงานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว

2.8.6 ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อที่จะได้เรียนรู้และเตรียมการป้องกัน

2.8.7 ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

2.9 การรักษาความปลอดภัยทางกายภาพและมาตรฐานการควบคุมสภาพแวดล้อม

2.9.1 การควบคุมกำกับดูแลการเข้าถึงและควบคุมสภาพแวดล้อมห้องคอมพิวเตอร์แม่ข่ายให้รัดกุมมากยิ่งขึ้นโดยการควบคุม ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (computer operator) เจ้าหน้าที่ดูแลระบบ (system administrator) เป็นต้น

2.9.2 ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีเจ้าหน้าที่ศูนย์คอมพิวเตอร์ควบคุมดูแลการทำงานตลอดเวลา เป็นต้น

2.9.3 ต้องมีระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

2.9.4 ควรจัดศูนย์คอมพิวเตอร์ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (network zone) ส่วนเครื่องแม่ข่าย (server zone) ส่วนเครื่องพิมพ์ (printer zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงาน และยังทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น นอกจากนี้ ควรแยกส่วนที่ต้องมีการเข้าถึงโดยเจ้าหน้าที่หลายฝ่ายออกจากศูนย์คอมพิวเตอร์ เช่น ส่วนที่ใช้เก็บรายงานที่ฝ่ายคอมพิวเตอร์ได้จัดพิมพ์ให้หน่วยงานต่างๆ ส่วนที่ใช้เป็นที่ตั้งเครื่องบันทึกเทปการให้คำแนะนำของเจ้าหน้าที่การตลาด เป็นต้น

2.9.5 การจัดชั้นความลับของสารสนเทศ (Information classification)

2.9.5.1 การจัดลำดับชั้นความลับของสารสนเทศ (Classification of Information)

1) บริษัท ต้องกำหนดให้มีการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยกำหนดชั้นความลับโดยให้นำกฎหมายและข้อกำหนดที่เกี่ยวข้องกับบริษัท มาร่วมพิจารณาการกำหนดชั้นความลับที่เหมาะสม

2) หน่วยงานภายในบริษัท ต้องจัดหมวดหมู่ของข้อมูลและทรัพย์สินสารสนเทศที่ใช้ในการดำเนินงานบริษัท และกำหนดลำดับชั้นความลับของข้อมูลและทรัพย์สินสารสนเทศ

2.9.5.2 การบ่งชี้สารสนเทศ (Labeling of Information)

1) บริษัท ต้องควบคุมให้ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นมีการควบคุมและรักษาความมั่นคงอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้บุคลากรและผู้ที่เกี่ยวข้องต้องปฏิบัติตาม เพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม

2) ฝ่ายเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้องต้องทำป้ายชื่อตามทะเบียนบัญชีทรัพย์สินและขั้นตอนการใช้งานติดที่อุปกรณ์คอมพิวเตอร์ทุกชิ้น

2.9.5.3 การบริหารจัดการทรัพย์สิน (Handling of Assets) ทรัพย์สินต้องมีนโยบายในการควบคุมกำกับให้มีขั้นตอนปฏิบัติงานส่วนการบริหารจัดการเพื่อมิให้ข้อมูลสำคัญของ บริษัท รั่วไหล หรือทรัพย์สินสารสนเทศถูกนำไปใช้ผิดประเภท

2.9.6 การจัดการสื่อบันทึกข้อมูล (Media handling)

2.9.6.1 การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (Management of Removable Media)

1) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำขั้นตอนการการปฏิบัติงานสำหรับการบริหารจัดการสื่อที่ใช้ในการบันทึกข้อมูลสารสนเทศที่เคลื่อนย้ายได้อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัท รับทราบและปฏิบัติตาม

2) การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ ต้องมีความสอดคล้องกับการกำหนดลำดับชั้นความลับข้อมูล

2.9.6.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

1) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำขั้นตอนปฏิบัติการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับหรือมีความสำคัญ

2) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดมาตรฐานการควบคุมการทำลายสื่อบันทึกข้อมูลโดยอ้างอิงมาตรฐานซึ่งเป็นที่ยอมรับในสากล

2.9.6.3 การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer) ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดขั้นตอนการปฏิบัติงานหรือข้อตกลงในการดูแลรักษาความปลอดภัยด้านสารสนเทศในกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่ติดตั้งหรือพื้นที่ปฏิบัติงาน

2.10 การป้องกันความเสียหาย

2.10.1 มีระบบป้องกันไฟไหม้

1) ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

2) ศูนย์คอมพิวเตอร์หลักต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับศูนย์คอมพิวเตอร์สำรอง อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

2.10.2 ระบบป้องกันไฟฟ้าขัดข้อง

1) ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ

2) ต้องมีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์สำคัญ เพื่อให้การดำเนินงานมีความต่อเนื่อง

2.10.3 ระบบควบคุมอุณหภูมิและความชื้น ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (specification) ของ ระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

2.10.4 ระบบเตือนภัยน้ำรั่ว ในกรณีที่มีการยกระดับพื้นของศูนย์คอมพิวเตอร์ เพื่อติดตั้งระบบปรับอากาศรวมทั้งเดินสายไฟและสายเครือข่ายด้านล่าง ก็ควรติดตั้งระบบเตือนภัยน้ำรั่วบริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่วได้ทันเวลา นอกจากนี้ หากศูนย์คอมพิวเตอร์ตั้งอยู่ในสถานที่ที่มีความเสี่ยงต่อภัยน้ำรั่วก็ควรหมั่นสังเกตว่ามีน้ำรั่วหรือไม่อย่างสม่ำเสมอ

2.11 โครงสร้างความมั่นคงปลอดภัยสำหรับสารสนเทศ

2.11.1 มีการจัดตั้งคณะกรรมการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท โดยให้มีตัวแทนจากส่วนงานต่างๆ ร่วมเป็นสมาชิกในคณะกรรมการ

2.11.2 กำหนดให้มีการจัดการประเมินความเสี่ยงอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยการประเมินความเสี่ยงดังกล่าวต้องพิจารณาถึงบริบทภายใน บริบทภายนอก ผู้มีส่วนได้ส่วนเสีย วิสัยทัศน์ พันธกิจที่บริษัทกำหนดไว้

2.11.3 ต้องกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้ และความเสี่ยงที่ยอมรับไม่ได้ เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงที่เกิดขึ้นในการประเมินความเสี่ยงที่เกิดขึ้น

2.11.4 ต้องมีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของบริบทภายใน บริบทภายนอก ผู้มีส่วนได้ส่วนเสีย วิสัยทัศน์ พันธกิจ และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความมั่นงคงปลอดภัยสารสนเทศของบริษัท

2.11.5 ต้องประเมินผลสัมฤทธิ์ของนโยบายที่ประกาศใช้เพื่อนำมาปรับปรุงนโยบายแผนกลยุทธ์ให้สอดคล้องกับภัยคุกคามในปัจจุบัน และอาจที่เกิดขึ้นในอนาคต

2.11.6 นโยบายความมั่นคงปลอดภัยสารสนเทศด้วยจัดทำเป็นลายลักษณ์อักษรตามวัตถุประสงค์และขอบเขตได้รับการอนุมัติ เพื่อให้ประกาศใช้และถือปฏิบัติทั่วทั้งบริษัทโดยให้มีผลบังคับใช้กับบุคลากรในทุกระกับชั้นของบริษัทที่เกี่ยวข้องกับการใช้ข้อมูลและสินทรัพย์สารสนเทศของบริษัท

2.11.7 สนับสนุนให้มีการอบรมด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละครั้งเพื่อเสริมสร้างความตระหนักทางด้านความมั่นคงปลอดภัยสารสนเทศ

2.12 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

2.12.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communication)

1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีมาตรการที่เหมาะสมเพื่อรองรับความปลอดภัยอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของบริษัท และเมื่อนำอุปกรณ์ออกไปใช้งานนอกสถานที่

2) ผู้ใช้งานที่มีการใช้งานอุปกรณ์สื่อสารประเภทพกพาเพื่อเชื่อมต่อกับระบบสารสนเทศของบริษัท ทั้งหมดต้องปฏิบัติตามนโยบายด้านการรักษาความปลอดภัยของระบบสารสนเทศและตระหนักถึงการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

2.13 การปฏิบัติงานภายนอกบริษัท(Teleworking)

2.13.1 ผู้ใช้งานที่มีการทำงานจากภายนอกบริษัททั้งหมดจะต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท เช่นเดียวกับการทำงานภายในบริษัท

2.13.2 ผู้ใช้งานที่มีการใช้ข้อมูลสารสนเทศของบริษัท ในการทำงานนอกบริษัท หรือการเข้าสู่ระบบผ่านทางไกลต้องได้รับอนุญาตจากเจ้าของข้อมูลสารสนเทศ และหน่วยงานต้นสังกัดโดยมีเหตุอันควร

2.13.3 ผู้ใช้งานที่ต้องการเข้าสู่ระบบผ่านทางไกลต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนเข้าใช้งาน

2.14 การจัดให้มีอุปกรณ์หรือระบบสารสนเทศสำรอง (Redundancies)

2.14.1 บริษัท ต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพความพร้อมใช้งานของระบบสารสนเทศที่มีความสำคัญสูง

2.14.2 บริษัท ต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรองหรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม

2.15 ความสอดคล้อง (Compliance)

2.15.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

1) ฝ่ายเทคโนโลยีสารสนเทศต้องร่วมมือกับฝ่ายกฎหมายและฝ่ายบริหารทรัพยากรบุคคลในการรวบรมกฎหมาย กฎระเบียบ หลักเกณฑ์ และข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและจัดทำเป็นเอกสารเพื่อใช้เป็นข้อกำหนดในการปฏิบัติงานอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

2) บุคลากรทั้งหมดต้องรับผิดชอบในการปฏิบัติตามข้อกำหนดที่ได้มีการระบุไว้อย่างเคร่งครัด

3) ห้ามเจ้าหน้าที่ในบริษัท ใช้งานทรัพย์สินและระบบสารสนเทศของบริษัท กระทำการใดๆ ที่ขัดแย้งต่อกฎหมายราชอาณาจักรไทยและกฎหมายระหว่างประเทศไม่ว่ากรณีใดก็ตาม

หมวดที่ 3
การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ และการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

3.1 มาตรการการรักษาความปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

3.1.1 จัดทำขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร รวมถึงจัดทำคู่มือการปฏิบัติงานระบบเทคโนโลยีสารสนเทศโดยมีรายละเอียดอย่างน้อยดังนี้

- การปฏิบัติงานในห้องแม่ข่าย
- การเปิดและปิดระบบงาน ได้แก่การเปิด- ปิดเครื่องแม่ข่ายการเปิด-ปิดระบบงาน การเปิด
- ปิดระบบให้บริการ
- การสำรองข้อมูล
- การบำรุงรักษาอุปกรณ์
- การจัดการกับสื่อบันทึกข้อมูลได้แก่การท าป้ายชื่อบ่งชี้การลบการป้องกันการทำสื่อบันทึก ข้อมูลกลับมาใช้งานอีกครั้ง
- การส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์และการจัดการกับข้อผิดพลาดที่เกิดขึ้น
- การประมวลผลข้อมูลได้แก่ขั้นตอนในการนำข้อมูลเข้าระบบงานประมวลผลและแสดงผลการใช้งานโปรแกรมยูทิลิตี้
- การรายงานและการจัดการกับปัญหาที่เกิดขึ้น
- การจัดการกับการทำงานล้มเหลวของระบบคอมพิวเตอร์ ระบบงาน และระบบเครือข่าย
- การกู้คืนระบบงานและระบบเครือข่าย

โดยหน่วยงานเทคโนโลยีสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ ผิดปกติ หรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

3.1.2 หน่วยงานเทคโนโลยีสารสนเทศต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้ หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ มีการแจกจ่ายและควบคุมดูแลให้มีการปฏิบัติงานตามแนวทางที่

กำหนดในประกาศของบริษัท และทบทวนปรับปรุงคู่มือการปฏิบัติงานให้เหมาะสมอยู่เสมอ หรือในกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย

3.1.3 ระบบเครือข่ายทั้งหมดของบริษัทฯ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรม ในการทำ Package Filtering เช่น การใช้ Firewall หรือ อุปกรณ์อื่น ๆ ที่ต้องมีความสามารถในการตรวจจับไวรัส ผู้ให้บริการภายนอกต้องมีระบบการกรองข้อมูลเว็บไซต์ที่ไม่ได้รับอนุญาตตาม พรบ. คอมพิวเตอร์ กรณีที่ผู้ใช้งาน ต้องการเข้าถึงเว็บไซต์ที่ไม่ได้รับอนุญาตหากมีความจำเป็นต้องใช้งาน ต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

3.1.4 บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุม ข้อมูลสารสนเทศที่ส่ง ผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของบริษัทฯ

3.1.5 ห้ามผู้ใช้งานติดตั้งโมเด็มหรืออุปกรณ์อื่น ๆ หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย เช่น Router, Switch, Hub และ Wireless Access Point เข้ากับเครื่องคอมพิวเตอร์ของตนหรือต่อกับจุดใดก็ตามบน ระบบเครือข่ายของบริษัทฯ โดยไม่ได้รับอนุญาตจากหน่วยงานเทคโนโลยีสารสนเทศ

3.1.6 ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์ และระบบเครือข่ายของบริษัทฯ โดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขอ อนุมัติอย่างเหมาะ สมก่อนทุกครั้ง

3.1.7 ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของบริษัทฯ ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอก ผ่านทางโมเด็มหรือ อุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในบริษัทฯ โดยเด็ดขาด

3.1.8 จัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยถือปฏิบัติตาม พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

3.1.9 ควบคุม ดูแลบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ กรณีพบความผิด ปรกติเกิดขึ้นในระบบ ผู้ดูแลเครือข่ายคอมพิวเตอร์มีอำนาจระงับการใช้เครื่องคอมพิวเตอร์หรือระบบเครือข่าย เพื่อป้องกันความเสียหายได้

3.1.10 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์

3.1.10.1 การควบคุมเครือข่าย (Network Controls) ผู้ดูแลระบบต้องดำเนินการควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย

3.1.10.2 การควบคุมเครือข่าย (Network Controls) ผู้ดูแลระบบต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับของการให้บริการ และตวามต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมดลงในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก

3.1.10.3 การแบ่งแยกเครือข่าย (Segregation in Network) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการแบ่งแยกบนระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยบต้องพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญขของข้อมูลที่อยู่บนเครือข่ายนั้น

3.1.11 ควบคุมระดับการเข้าถึงระบบเทคโนโลยีสารสนเทศ ตามหน้าที่ และความรับผิดชอบ

3.1.12 กำหนดนโยบายสำหรับการเข้าใช้งานระบบภายในให้สามารถระบุตัวตนของผู้เข้าใช้งานได้

3.1.13 กำหนดนโยบายสำหรับการตรวจสอบข้อมูลในฐานอย่างสม่ำเสมอโดยแบ่งแยกข้อมูลเป็น 2 รูปแบบ คือ ข้อมูลที่ไม่ได้ใช้งานและข้อมูลที่หมดอายุ มีการกำหนดระยะเวลาในการตรวจสอบ และผู้ดูแลหากเป็นข้อมูลที่ไม่ได้ใช้งานต้องเปลี่ยนเก็บเป็นประวัติ Archive

3.1.14 กำหนดมาตรฐานในการทำงานระยะไกล เช่น VPN หรือ Access control เป็นต้น โดยผู้เข้าถึงต้องมีการขออนุญาตและมีแบบฟอร์มสำหรับแจ้งข้อมูลเพื่อให้ทางส่วนงานรับทราบ

3.1.15 กำหนดนโยบายสำหรับการแจ้งเรื่อง incident โดยมีการจัดการในด้านความสำคัญของระบบ ความเสี่ยง ผู้มีส่วนได้เสียของระบบ โดยมีการบันทึกทุกครั้งหากเกิดปัญหา ให้ผู้บังคับบัญชารับทราบและลงนาม โดยดำเนินการตามประกาศของบริษัท

3.1.16 จัดทำแบบฟอร์มหรือระบบสำหรับการเปิดขอใช้งานทั้งเซิร์พเวอร์ ฐานข้อมูล และโปรแกรมต่างๆ เพื่อให้มีการบันทึกข้อมูลตามประกาศของบริษัทที่เกี่ยวเนื่องกับการบันทึกข้อมูล

3.1.17 การถ่ายโอนสารสนเทศ (Information Transfer)

3.1.17.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer Policies and Procedures)

1) ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมดูแล กำหับให้มีขั้นตอนการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล

2) กำหนดข้อตกลงสำหรับการแลกเปลี่ยนข้อมูล โดยฝ่ายเทคโนโลยีสารสนเทศต้องเป็นผู้ควบคุม กำกับให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัท และระหว่างบริษัท กับหน่วยงานภายนอกของบริษัท

3) สำหรับการถ่ายโอนข้อมูลสำหรับหน่วยงานภายนอก ต้องได้รับการอนุมัติจากเจ้าของข้อมูลก่อนทุกครั้งและมีการควบคุมโดยการระบุข้อตกลงเป็นลายลักษณ์อักษร รวมถึงกำหนดเงื่อนไขสำหรับการแลกเปลี่ยน ตลอดจนต้องมีการป้องกันข้อมูลสารสนเทศตามลำดับชั้นความลับของข้อมูลอย่างเหมาะสม

4) กรณีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ทั้งในรูปแบบจดหมายอิเล็กทรอนิกส์หรือข้อความตอบโต้ทันที ต้องมีการกำหนดนโยบายสำหรับควบคุมดูแลข้อความที่เป็นความลับหรือเอกสารข้อมูลอิเล็กทรอนิกส์ที่สำคัญ เป็นความลับของบริษัทต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ์

5) กำหนดข้อตกลงในการทำสัญญารักษาความลับหรือไม่เปิดเผยความลับ โดยผู้บริหารต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัท มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของบริษัท อย่างเป็นลายลักษณ์อักษร นอกจากจะได้รับอนุญาตและลงนามอย่างเป็นลายลักษณ์อักษรพิจารณาตามกรณีและมีการระบุความประสงค์ที่ต้องการนำข้อมูลหรืออ้างอิง พาดพิงถึงบริษัท

3.2 มาตรการการรักษาความปลอดภัยด้านการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

3.2.1 หน่วยงานเทคโนโลยีสารสนเทศต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ ในการใช้งาน อาทิ เขียน อ่าน ลบ ได้ กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาต ให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

3.2.2 มีการกำหนดระยะเวลาในการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและอย่างเหมาะสมกับการทำงานเท่านั้น

3.2.3 บุคคลภายนอกต้องปฏิบัติตามนโยบายของบริษัทฯ อย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบ เทคโนโลยีสารสนเทศของบริษัทฯ

3.2.4 สิทธิ์การเข้าถึงไฟล์ข้อมูลสารสนเทศต้องได้รับการควบคุม และได้รับการพิจารณาอนุมัติเท่าที่จำเป็นเท่านั้น เพื่อให้ไฟล์ข้อมูลสารสนเทศได้รับการรักษาความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ รวมทั้งเป็นการแบ่งแยกสิทธิ์ และหน้าที่ของผู้ใช้งาน

3.2.5 ควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงในระบบข้อมูลหรือในเครื่องคอมพิวเตอร์ของพนักงานโดยไม่ให้กระทบต่อระบบหลักหรือก่อให้เกิดความเสียหายต่อระบบรวม

3.2.6 ข้อมูลสำหรับการทดสอบ (Test data) เพื่อให้เกิดการป้องกันข้อมูลสำหรับการทดสอบทางบริษัทจำเป็นต้องมีการกำหนดนโยบายป้องกันข้อมูล โดยมีผู้รับผิดชอบคือส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่อยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง

3.3 มีการตรวจสอบระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ อย่างน้อยปีละ 1 ครั้งดังนี้

3.3.1 วางแผนการตรวจสอบระบบฯ ให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

3.3.2 กำหนดขอบเขตในการตรวจสอบระบบฯ ทางเทคนิคให้ครอบคลุมถึงจุดเสี่ยงที่สำคัญโดยการตรวจสอบดังกล่าว ต้องไม่กระทบต่อการปฏิบัติงาน

3.3.3 ตรวจสอบระบบฯ นอกเวลาทำงาน ในกรณีที่การตรวจสอบนั้นอาจส่งผลกระทบต่อความพร้อมในการใช้งานระบบดังกล่าว

3.3.4 ทบทวน และปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง รวมถึงปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงด้วย

3.4 มาตรการเข้ารหัสลับข้อมูล (Cryptographic controls)

3.4.1 นโยบายการใช้มาตรฐานการเข้ารหัสลับข้อมูล (Policy on the use of Cryptographic Controls)

1) ฝ่ายเทคโนโลยีสารสนเทศต้องเป็นผู้กำหนดมาตรฐานการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับบริษัท และความเสี่ยงที่อาจเกิดขึ้นในแต่ละชั้นความลับที่กำหนดไว้

2) การบริหารจัดการกุญแจเข้ารหัสลับข้อมูล (Key Management) ฝ่ายเทคโนโลยีสารสนเทศต้องเป็นผู้กำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูลโดยให้ครอบคลุมวงจรการบริหารจัดการกุญแจ (Key Management Life Cycle) รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวสม่ำเสมอ

3.5 การควบคุมเข้าถึงระบบปฏิบัติการของบริษัท ระบบงานต่างๆ และข้อมูล

3.5.1 ผู้ดูแลระบบต้องจัดการให้เครื่องมือคอมพิวเตอร์ของผู้ใช้งานทั่วไปทุกเครื่องของบริษัททำงานร่วมกับระบบ Active Directory และการบริหารจัดการให้ระบบ AD สามารถควบคุมเครื่องคอมพิวเตอร์ของผู้ใช้งานทั่วไปทุกเครื่องของบริษัทและกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของบริษัท

3.5.2 เพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่เหมาะสม และมีการจำกัดสิทธิ์การเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line โดยพิจารณาตามความเหมาะสมของกลุ่มผู้ใช้งาน

3.5.3 ตรวจสอบข้อมูลประวัติการเข้าถึงระบบสารสนเทศ Security log อย่างสม่ำเสมอ

3.5.4 กำหนดให้เก็บสิทธิ์การใช้งานของผู้ใช้ ชื่อผู้ใช้ตาม Single Sign-on รวมถึงกิจกรรมที่ต้องการ เช่น การเข้าสู่ระบบ การเพิ่มข้อมูล การลบข้อมูล การแก้ไขข้อมูล เป็นต้น

3.5.5 กำหนดผู้ดูแลสอบทาน Security log เช่น ผู้ดูแลระบบจะต้องเข้ามาตรวจสอบ Security log ทุก 2 อาทิตย์ เป็นต้น เพื่อตรวจสอบกิจกรรมที่อาจจะทำให้เกิดความเสี่ยงต่อระบบสารสนเทศ

3.5.6 กำหนดระยะเวลาที่ต้องมีการทวนสอบและทำลาย Security log ทิ้ง เพราะว่าหากเก็บไว้นานไปไม่มีผลดีต่อระบบ เช่น แบ่งช่วงระยะเวลาของความสำคัญของข้อมูล หากเป็นระบบที่ทั้งบริษัท ใช้ต้องมีการเก็บข้อมูลกิจกรรม เป็นระยะเวลา 1 ปี ระบบที่มีความสำคัญลงมาให้เก็บข้อมูลเป็นระยะเวลา 6 เดือน เป็นต้น

3.5.7 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

1) ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมให้ระบบสารสนเทศของบริษัท ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง

2) ผู้ดูแลระบบต้องดูแลและบำรุงรักษาระบบ เพื่อรักษาระดับความมั่นคงปลอดภัยด้านสารสนเทศของระบบอย่างสม่ำเสมอ ได้แก่ การตรวจสอบหาช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ที่ตรวจสอบพบ และการแก้ไขปรับปรุงช่องโหว่ของระบบสารสนเทศ

3.6 ระบุและยืนยันตัวตนของผู้ใช้งาน

3.6.1 ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างเป็นผู้ใช้งานที่ระบุถึง

3.6.2 การสร้างบัญชีผู้ใช้ใหม่ การแก้ไข หรือยกเลิกบัญชีผู้ใช้ ต้องแจ้งผู้ดูแลระบบให้ดำเนินการ โดยได้รับความเห็นชอบจากผู้บังคับบัญชาของผู้ใช้งาน และผู้บังคับบัญชาที่กำกับดูแลระบบ 3.6.3 การขอเพิ่ม/เปลี่ยนแปลง/เพิกถอนบัญชีรายชื่อและสิทธิ์ให้มีหลักฐานการร้องขอที่เป็นลายลักษณ์อักษร

3.6.4 ผู้ใช้งานทุกคนต้องมี User ID ของตนและไม่ซ้ำกับผู้ใช้งานคนอื่นๆ โดย User ID ที่ออกให้นั้นต้องสามารถตรวจสอบและยืนยันกลับไปยังตัวผู้ใช้งานได้

3.6.5 ผู้ใช้งานต้องระบุชื่อผู้ใช้งาน และรหัสผ่านเพื่อใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของบริษัท

3.7 การใช้งานโปรแกรมอรรถประโยชน์ จำกัดและควบคุมดูแลการใช้งานโปรแกรมอรรถประโยชน์เพื่อป้องกันการละเมิดลิขสิทธิ์หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

3.7.1 จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

3.7.2 กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

3.7.3 จัดเก็บโปรแกรมแรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

3.7.4 ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

3.7.5 ต้องติดตั้งโปรแกรมอรรถประโยชน์ที่มีลิขสิทธิ์ถูกต้องในการใช้งาน

3.7.6 การเข้าใช้งาน Application ต่างๆ จะต้องได้รับอนุญาตจากผู้บังคับบัญชาโดยตรง ต้องมีการแจ้งความประสงค์ในการใช้งาน และมีการลงบันทึกเรื่องการร้องขอโปรแกรม

3.7.7 กำหนดให้พนักงานใช้โปรแกรมและ Application ที่บริษัทกำหนดให้ใช้เท่านั้น

3.7.8 ห้ามพนักงานนำโปรแกรม หรือ Application ใดๆ มาติดตั้งบนเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์รวมถึงอุปกรณ์ประกอบอื่นๆ บริษัท โดยไม่ได้รับความยินยอมจากหน่วยงานคอมพิวเตอร์และผู้บังคับบัญชาโดยตรง

3.7.9 ห้ามพนักงานใช้ โปรแกรม หรือ Application ที่ไม่ถูกลิขสิทธิ์

3.7.10 ถ้าหากพนักงานมีความต้องการใช้งานโปรแกรมที่ไม่มีการซื้อลิขสิทธิ์ให้แจ้งความประสงค์ผ่านแบบฟอร์มและมีการดำเนินการอนุมัติผ่านสายการอนุมัติ

3.8 การกำหนดเวลาในการใช้งานระบบ

3.8.1 เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น ต้องยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา 30 นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงสูงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นจิ้นตามความเหมาะสม หรือเป็นเวลา 10 นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

3.8.2 ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศ หรือแอพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ 3 ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของบริษัท ตามปกติเท่านั้น

3.9 การป้องกันภัยคุกคามต่อระบบสารสนเทศ กำหนดการป้องกันโปรแกรมไม่ประสงค์ดี เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการป้องกันภัยคุกคาม จากโปรแกรมไม่ประสงค์ดี

หมวดที่ 4
หลักเกณฑ์อื่น ๆ

4.1 พนักงาน / ผู้ใช้งาน

4.1.1 ปฏิบัติตามคู่มือพนักงาน คู่มือจรรยาบรรณทางธุรกิจอย่างเคร่งครัด

4.1.2 พนักงานทุกคนมีสิทธิใช้ทรัพย์สินสารสนเทศภายใต้ข้อกำหนดดังกล่าว การฝ่าฝืนจนเป็นเหตุหรืออาจเป็นเหตุให้ เกิดความเสียหายแก่บริษัทฯ หรือบุคคลหนึ่งบุคคลใด บริษัทฯ จะพิจารณาดำเนินการทางวินัยและกฎหมายแก่ พนักงานที่ฝ่าฝืนตามความเหมาะสม

4.1.3 พนักงานพึงใช้ข้อความสุภาพ หรือใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น รวมทั้งปฏิบัติ ให้ถูกต้องตามธรรมเนียมปฏิบัติของการใช้เครือข่าย

4.1.4 พนักงานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่พึงอนุญาตให้บุคคลอื่นเข้าใช้ เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง

4.1.5 เพื่อป้องกันหากมีผู้อื่นล่วงรู้และนำรหัสผ่านของพนักงานไปใช้ในทางที่ผิดและเกิดความเสียหายต่อบริษัทฯ พนักงานจะต้องเก็บรหัสผ่านไว้เป็นความลับ และไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่

4.1.6 เพื่อความปลอดภัยในการใช้ระบบเครือข่ายคอมพิวเตอร์ กรณีพนักงานพบไวรัสคอมพิวเตอร์จะต้องแจ้งให้ผู้ดูแล ระบบดำเนินการกำจัดไวรัสโดยเร็ว

4.1.7 พนักงานพึงลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน เพื่อเป็นการ ประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

4.1.8 พนักงานพึงให้ความร่วมมือและอำนวยความสะดวกแก่ ผู้ดูแลระบบในการตรวจสอบระบบความปลอดภัยของ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำที่เกี่ยวข้องกับความ ปลอดภัยในระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ

4.2 การควบคุมภายในสำหรับการปฏิบัติงานให้เป็นไปตามนโยบาย ฯ

4.2.1 บริษัทจัดให้มีรอบการตรวจสอบระบบสารสนเทศโดยผู้เชี่ยวชาญภายนอกที่เป็นอิสระ

4.2.2 กำหนดนโยบายสำหรับการเชื่อมต่อสำหรับอุปกรณ์พกพาโดยต้องสามารถระบุตัวตนของผู้ใช้งานและเครื่องที่ใช้งานได้เก็บข้อมูลของเครื่องที่สามารถเข้าใช้งานและชื่อบุคคลผู้เข้าใช้งาน โดยสามารถตรวจสอบรูปแบบการกำหนดการใช้งานและวิธีการระบุตัวตนได้จากประกาศต่อไป

4.2.3 บริษัทดำเนินกิจการภายใต้กฎหมายไทย ดังนั้น การใช้งานระบบเครือข่ายคอมพิวเตอร์ ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2560

4.2.4 บริษัทไม่สนับสนุนหรือยินยอมให้พนักงานของบริษัทกระทำความผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2560 และกฎหมายประกอบอื่นๆที่เกี่ยวข้อง

4.2.5 บริษัทจะจัดให้มีชื่อผู้ใช้ (USER ID) และรหัสผ่าน (Password) ให้กับพนักงานที่มีหน้าที่เกี่ยวข้องกับการใช้งานระบบเครือข่ายคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ตเป็นรายบุคคล และมีกฎสำหรับการตั้งรหัสผ่านและใช้งานรหัสผ่าน

4.2.6 รหัสผ่านของพนักงานถือเป็นทรัพย์สินของบริษัท ไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และพนักงานทุกคนมีหน้าที่ในการป้องกันรหัสผ่านของบริษัท อย่างเคร่งครัด

4.2.7 บริษัทไม่อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน

4.2.8 พนักงานอาจจะได้รับมอบหมายให้เข้าใช้ระบบงานอื่นๆที่บริษัทกำหนดให้ใช้ พนักงานจะต้องปฏิบัติตามกฎการใช้ระบบและเก็บรักษาชื่อและรหัสผ่านไว้ ห้ามมิให้เปิดเผยกับผู้อื่น ยกเว้นได้รับอนุมัติจากผู้บังคับบัญชาโดยตรงเป็นลายลักษณ์อักษร

4.2.9 หากจะต้องมีการเลิกใช้ชื่อและรหัสผ่าน ให้แจ้งกับผู้บังคับบัญชาโดยตรงเพื่อทำเรื่องขอเลิกใช้โดยจะต้องกระทำทันทีที่จะเลิกใช้งาน

4.2.10 เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบถือเป็นทรัพย์สินของบริษัทพนักงานมีหน้าที่รักษาให้สามารถใช้งานได้ ทั้งนี้รวมไปถึงการ อัพเดท ระบบปฏิบัติการและ โปรแกรมป้องกันไวรัส หรือชุดคำสั่งมาพึงประสงค์

ภาคผนวก

ตารางปรับปรุงข้อมูล