ข้อกำหนดที่ 1 เรื่องนโยบายความมั่นคงปลอดภัยสารสนเทศ

อนุมัติโดย ดร.สมชัย ไทยสงวนวรกุล

(ประธานกรรมการบริหาร) .....

.....

(นายสมชาย งามกิจเจริญลาภ)
รองประธานกรรมการบริหาร

.....

(นางสาวสินีนารถ ไทยสงวนวรกุล)
ผู้ช่วยประธานกรรมการบริหาร

.....

(นายรัฐภูมิ นันทปถวี)
ผู้บริหารสูงสุดฝ่ายการบัญชีและการเงิน

.....

(นายสุรชัย ชัยฌรงค์)
ผู้บริหารสูงสุดฝ่ายปฏิบัติการ

.....

(นายเศรษฐกาณฑ์ เตชะธนนันทวงศ์)
ผู้ช่วยกรรมการผู้จัดการ

.....

(นายวัชรากร สิงหาบุตร)
ผู้จัดการแผนกเทคโนโลยีสารสนเทศ

บันทึกการเปลี่ยนแปลง

ฉบับที่	วันที่	คำอธิบายเหตุผลของการเปลี่ยน
1	01 พฤษภาคม 2562	ออกครั้งแรก
2	03 มีนาคม 2564	ปรับเปลี่ยนแก้ไข ข้อ 24 การควบคุมการเข้าถึงของพนักงาน ข้อ 27 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ ข้อ 30 การบริหารงานผู้ให้บริการภายนอก
3	25 เมษายน 2568	ปรับเปลี่ยนแก้ไข ข้อ 11 การพัฒนาบุคลากรให้ตระหนักต่อนโยบายฯ ข้อ 29 การบริหารระบบการเข้ารหัส

สารบัญ

ข้อกำหนดที่ 1

เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ

บริษัทฯ ขอประกาศ นโยบายความมั่นคงปลอดภัยสารสนเทศ เพื่อให้การใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นไปอย่างมีประสิทธิภาพ มีความน่าเชื่อถือ และสอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี 2560 โดยมีใจความดังนี้

ข้อ 1 ข้อกำหนดนี้เรียกว่า " ข้อกำหนดบริษัทฯ ที่ 1 เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ"

ข้อ 2 ข้อกำหนดนี้ให้ใช้บังคับตั้งแต่วันที่ 1 พฤษภาคม พ.ศ. 2562 เป็นต้นไป

ข้อ 3 ข้อกำหนดนี้

(1) "บริษัทฯ" หมายความว่า บริษัท เอส เอ็น ซี ฟอร์เมอร์ จำกัด (มหาชน) และ บริษัทในเครือ

(2) "กรรมการบริหาร" หมายความว่า ผู้บริหารระดับสูงของบริษัท เอส เอ็น ซี ฟอร์เมอร์ จำกัด (มหาชน) และบริษัทในเครือ

(3) "คณะกรรมการฯ" หมายความว่า พนักงานที่ถูกมอบหมายให้เข้าร่วมกับการจัดทำมาตรฐานความปลอดภัย

(4) "ข้อมูล" หมายความว่า ข้อมูลและข้อมูลสารสนเทศทั้งที่อยู่ในรูปเอกสารและข้อเท็จจริงที่อยู่ในรูปแบบต่างๆ เช่น ข้อมูลที่อยู่ในแบบฟอร์มของบริษัทฯ รวมถึงที่อยู่ในระบบสารสนเทศ เครือข่าย อุปกรณ์คอมพิวเตอร์ หรือสื่อในการจัดเก็บข้อมูลของบริษัทฯ ไม่ว่าข้อมูลเหล่านี้จะอยู่ในรูปแบบใดๆ การอ้างถึงข้อมูลตามข้อกำหนดนี้ จะมีความหมายรวมถึงข้อมูลสารสนเทศด้วย

(5) "ข้อมูลระดับชั้นความลับสำคัญ" หมายความว่า ข้อมูลสารสนเทศที่เมื่อเกิดความเสียหาย หรือรั่วไหลสู่ภายนอกจะมีผลกระทบต่อบริษัทฯ ในการแบ่งแยกข้อมูลระดับชั้นความลับสำคัญได้แก่ ความลับ(Secret) และข้อมูลที่ปกปิด (Confidential)

(6) "ทรัพยากร" หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของฝ่ายเทคโนโลยีสารสนเทศ

(7) "อุปกรณ์คอมพิวเตอร์" หมายความว่า เครื่องคอมพิวเตอร์ ระบบปฏิบัติการ อุปกรณ์เชื่อมต่อเครือข่ายต่างๆ ที่อยู่ภายใต้การดูแลของฝ่ายเทคโนโลยีสารสนเทศ

(8) "ทรัพย์สินของบริษัทฯ" หมายความว่า ข้อมูล และระบบเทคโนโลยีสารสนเทศที่บริษัทฯ เป็นเจ้าของ

(9) "เจ้าหน้าที่/พนักงานบริษัทฯ" หมายความว่า พนักงาน ผู้ที่บริษัทฯทำสัญญาว่าจ้าง (เช่น เพื่อการบำรุงรักษาอุปกรณ์ต่างๆ ของบริษัทฯ) และหน่วยงานภายนอก

(10) "ผู้ใช้งาน" หมายความว่า กรรมการบริษัท ผู้บริหาร พนักงานประจำ ลูกจ้าง และพนักงานชั่วคราวของบริษัทฯ และบุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครือข่ายคอมพิวเตอร์

(11) "ผู้มีอำนาจ" หมายความว่า ผู้ที่ได้รับการมอบหมายจากบริษัทฯ ให้รับผิดชอบต่อกิจกรรม กระบวนการ หรือสารสนเทศองค์กรให้ดำเนินการตามขอบเขตที่บริษัทฯกำหนด

(12) "อินเทอร์เน็ต" หมายความว่า เครือข่ายภายนอกที่เชื่อมต่อกันทั่วโลก

(13) "อินทราเน็ต" หมายความว่า เครือข่ายภายในบริษัทฯ

(14) "เครือข่ายจำลองส่วนบุคคล หรือ Virtual Private Network(VPN)" หมายความว่าการสร้างเครือข่ายที่มีการเข้ารหัสในการติดต่อจากเครือข่ายสาธารณะ หรืออินเทอร์เน็ต

(15) "ระบบงานหลัก หรือ Production environment" หมายความว่าระบบคอมพิวเตอร์ของบริษัทฯ ที่ใช้เพื่อดำเนินการผลักดันการทำงานภายในบริษัทฯ

(16) "รหัสผ่าน" หมายความว่า กลุ่มข้อความที่ประกอบตัวอักษร ตัวเลข หรืออักขระพิเศษที่กำหนดให้ผู้ใช้งานระบบสารสนเทศระบุตัวตน และสิทธิในการเข้าใช้งานระบบสารสนเทศ

(17) "ระบบสารสนเทศ" หมายความว่า ระบบงานที่ถูกออกแบบมาเพื่ออำนวยความสะดวกในการสื่อสาร และจัดการข้อมูลของบริษัทฯ

(18) "เครือข่าย" หมายความว่า ระบบสารสนเทศที่ติดต่อโดยการนำเครื่องคอมพิวเตอร์เชื่อมต่อเพื่อสื่อสารแลกเปลี่ยนข้อมูล

(19) "เครือข่ายสาธารณะ" หมายความว่า ระบบสารสนเทศที่ติดต่อโดยไม่ต้องมีการระบุสิทธิ และตัวตนของผู้ใช้

(20) "ลิขสิทธิ์" หมายความว่า สิทธิที่ได้รับแต่เพียงผู้เดียวตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น

(21) "ไวรัสคอมพิวเตอร์ หรือโค้ดที่มุ่งหวังร้าย" หมายความว่า โค้ดโปรแกรมคอมพิวเตอร์ที่ถูกพัฒนาขึ้นเพื่อเข้าไปดำเนินการดัก ดึง และทำลายข้อมูลสารเทศ และระบบสารสนเทศ

(22) "จดหมายอิเล็กทรอนิกส์แบบลูกโซ่" หมายความว่า จดหมายอิเล็กทรอนิกส์ที่มีลักษณะการส่งต่อเรื่อยๆ โดยสังเกตได้จากการมีกลุ่มรายชื่อจดหมายอิเล็กทรอนิกส์เป็นจำนวนมาก

(23) "จดหมายอิเล็กทรอนิกส์แบบสแปม" หมายความว่า การเก็บรายชื่อจดหมายอิเล็กทรอนิกส์เป็นจำนวนมากเพื่อทำการส่งต่อให้ในรายชื่อจดหมายอิเล็กทรอนิกส์ที่เก็บนั้น

(24) "เหตุการณ์ผิดปกติ" หมายความว่า เหตุการณ์ผิดปกติที่เกิดขึ้นทำให้ระบบงานหยุดชะงัก หรือไม่สามารถใช้งานได้ตามปกติ

(25) "ช่องโหว่" หมายความว่า จุดอ่อนของระบบที่ภัยคุกคามสามารถเข้าสู่ระบบงานทำให้ระบบงานเกิดความเสียหาย หรือทำงานผิดปกติ เช่นภัยจากการเจาะระบบจากแฮกเกอร์ เป็นต้น

(26) "สัญญาการไม่เปิดเผยข้อมูล หรือ Non-Disclosure Agreement (NDA)" หมายความว่า การทำข้อตกลง หรือสัญญารักษาความลับของข้อมูลสารสนเทศบริษัทฯ

(27) "นโยบายการยอมรับการใช้สารสนเทศ" หมายความว่า นโยบายที่จัดทำขึ้นเพื่อใช้สื่อสารกับผู้ที่เกี่ยวข้องกับการเข้ามาใช้ระบบสารสนเทศของบริษัทฯ

(28) "ไฟร์วอลล์" หมายความว่า ซอฟต์แวร์หรืออุปกรณ์ที่ป้องกันการเชื่อมต่อของอุปกรณ์หรือเครื่องคอมพิวเตอร์จากเครือข่ายอื่นๆ

(29) "อุปกรณ์ระบบป้องกันผู้บุกรุก" หมายความว่า ซอฟต์แวร์หรืออุปกรณ์ที่ตรวจสอบป้องกันการเข้าบุกรุกจากบุคคลที่ไม่เกี่ยวข้อง

(30) "ล็อก หรือ Log" หมายความว่า ข้อมูลที่บันทึกกิจกรรมที่เกิดขึ้นในการใช้อุปกรณ์สารสนเทศ หรือข้อมูลสารสนเทศโดยต้องตระหนักต่อการควบคุมการแก้ไขบันทึกที่เกิดขึ้น

(31) "ผู้มีอำนาจ" หมายความว่า บุคคลที่มีสิทธิ์ในการอนุมัติให้ดำเนินการตามภาระหน้าที่ขององค์กร

(32) "สื่อสังคมออนไลน์" หมายความว่า ระบบสารสนเทศที่มีการโต้ตอบกันระหว่างบุคคลผ่านเครือข่ายอินเทอร์เน็ต

(33) "อุปกรณ์พกพา" หมายความว่า เครื่องคอมพิวเตอร์โน้ตบุ๊ค อุปกรณ์สมาร์ทโฟน โทรศัพท์มือถือ เป็นต้น

หมวด 1
การจัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับคณะ กรรมการฯ โดยเจ้าหน้าที่บริษัทฯ จะได้รับทราบถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศเกี่ยวกับหน้าที่ ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ ที่เกี่ยวข้องกับสารสนเทศองค์กร

ข้อ 4 การจัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

(1) บริษัทฯ จัดให้มีนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เป็นลายลักษณ์อักษรโดยถูกอนุมัติจากกรรมการบริหารฯ กรณีที่มีการแก้ไขเปลี่ยนแปลงนโยบายต้องถูกอนุมัติโดยกรรมการบริหารฯ ทุกครั้ง

(2) ต้องมีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมอ โดยมีการประเมินความเสี่ยงอย่างน้อยปีละครั้ง ซึ่งมีการระบุความเสี่ยงที่เกี่ยวข้องโดยจัดลำดับตามความสำคัญของข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ

(3) มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ในข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ พร้อมกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยงอย่างเหมาะสม

(4) นโยบายฯ ที่จัดทำต้องมีการกำหนดวัตถุประสงค์ ขอบเขต ความรับผิดชอบ และเนื้อหาอย่างชัดเจน รวมถึงบทลงโทษที่ระบุสอดคล้องกับข้อกำหนดของบริษัทฯ และกฎหมาย

(5) จัดเก็บ และเผยแพร่นโยบายฯ ให้กับเจ้าหน้าที่ และบุคคลเกี่ยวข้องทราบเพื่อสามารถปฏิบัติให้เป็นไปตามนโยบายฯ ที่กำหนด

(6) จัดทำระบบติดตามการปฏิบัติตามนโยบายฯ และดำเนินการตรวจสอบการปฏิบัติตามอย่างต่อเนื่อง

หมวด 2
โครงสร้างองค์กรทางด้านความมั่นคงปลอดภัยสำหรับบริษัทฯ

วัตถุประสงค์

เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัทฯในการกำหนดโครงสร้างการสอบทานการปฏิบัติการที่เหมาะสม และเป็นการป้องกันความสูญเสียอันเนื่องมาจากระบบเทคโนโลยีสารสนเทศเกิดหยุดชะงัก หรือใช้ผิดวัตถุประสงค์

ข้อ 5 การจัดทำโครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

(1) จัดให้มีการกำหนดผู้มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ อย่างชัดเจน

(2) กำหนดให้มีการแบ่งแยกการปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากงานในหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบงานหลัก (Production Environment)

(3) จัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีผู้ปฏิบัติงานหลักไม่สามารถดำเนินการได้

หมวด 3
การบริหารจัดการทรัพย์สินของบริษัทฯ

วัตถุประสงค์

เพื่อป้องกันทรัพย์สินของบริษัทฯจากความเสียหาย และ/หรือ การนำไปใช้อย่างผิดวัตถุประสงค์อันเกิดจากการปฏิบัติหน้าที่ของเจ้าหน้าที่บริษัทฯ และบุคคลภายนอกที่เข้ามาถึงสารสนเทศบริษัทฯ

ข้อ 6 การจัดแบ่งระดับข้อมูล และการจัดการข้อมูลสารสนเทศ

(1) ข้อมูลที่อยู่ในชั้นความลับต้องมีการเข้ารหัสข้อมูลในหน่วยจัดเก็บของอุปกรณ์คอมพิวเตอร์ และการติดต่อระหว่างเครือข่าย

(2) กำหนดให้จำกัดสิทธิ์การเข้าสู่ข้อมูลต่างๆที่มีระดับความสำคัญตั้งแต่ข้อมูลสารสนเทศที่ใช้เฉพาะภายในบริษัทฯ

(3) กรณีที่มีความจำเป็นที่ต้องเปิดเผยข้อมูลที่จัดอยู่ในระดับชั้นความลับสู่ภายนอก ผู้รับข้อมูลดังกล่าวต้องมีการเซ็นสัญญาไม่เปิดเผยความลับ

ข้อ 7 ความเป็นส่วนตัวของสารสนเทศ และระบบสารสนเทศ

(1) ระบบสารสนเทศ และข้อมูลสารสนเทศที่ใช้ภายในบริษัทฯ ถือเป็นทรัพย์สินของบริษัทฯ

(2) เจ้าหน้าที่บริษัทฯ ต้องไม่จัดเก็บข้อมูลที่ไม่เกี่ยวข้องกับกิจการของบริษัทฯ ไว้ในทรัพยากรและระบบสารสนเทศของบริษัทฯ

(3) ต้องมีการจัดทำระบบตรวจสอบล็อก (Log) ในการใช้งานจดหมายอิเล็กทรอนิกส์ เพื่อพิจารณาว่ามีการละเมิดต่อนโยบายฯ และพรบ.คอมฯ

(4) มีการแจ้งให้บุคคล หรือบริษัทฯ ที่ใช้เทคโนโลยีสารสนเทศของบริษัทฯ ได้รับทราบเกี่ยวกับนโยบายการยอมรับการใช้สารสนเทศ

(5) กลุ่มงานภายนอกที่เข้าใช้สารสนเทศภายในชั้นความลับจำเป็นต้องมีการเซ็นสัญญาการไม่เปิดเผยข้อมูลก่อนดำเนินการทุกครั้ง

(6) ผู้ที่ละเมิดต่อการปฏิบัตินโยบายฯ การรักษาความลับข้อมูลของบริษัทฯ จะพิจารณาบทลงโทษตามวินัยของบริษัทฯ กรณีที่มีการละเมิดต่อกฎหมายให้พิจารณาลงโทษตามข้อบัญญัติของกฎหมาย

ข้อ 8 ความเป็นส่วนตัวของเว็บ

(1) ผู้ที่ไม่มีหน้าที่เกี่ยวข้องในการดูแลบริหารระบบ และเครือข่าย หากต้องการใช้บริการต่างๆ นอกเหนือจากเว็บไซต์ของบริษัทฯ ต้องมีการขออนุญาตอย่างเป็นลายลักษณ์อักษรจากผู้มีอำนาจก่อนที่จะเผยแพร่ข้อมูลสู่สาธารณะ

(2) เว็บไซต์ที่มีการเก็บข้อมูลของบริษัทฯ ต้องมีการกำหนดสิทธิ์และควบคุมการเข้าถึงเว็บไซต์ของบริษัทฯ

(3) เว็บไซต์ต่างๆ ของบริษัทฯ ต้องมีข้อความประกาศให้ทราบเกี่ยวกับลิขสิทธิ์ และทรัพย์สินของบริษัทฯ

(4) กำหนดผู้รับผิดชอบในการปรับปรุงเว็บไซต์อย่างชัดเจน กรณีที่มีข้อสงสัยให้ปรึกษาฝ่ายกฎหมาย สำหรับแหล่งที่มาของข้อมูลต่างๆที่ไม่ได้มาจากบริษัทฯต้องมีการระบุแหล่งที่มาอย่างชัดเจน ห้ามนำข้อมูลที่ไม่ทราบแหล่งที่มา ใช้ในการจัดทำเว็บไซต์ของบริษัทฯ

ข้อ 9 การปฏิบัติงานของเจ้าหน้าที่ต่อทรัพย์สินของบริษัทฯ

(1) เจ้าหน้าที่บริษัทฯ ต้องไม่นำทรัพย์สินสารสนเทศบริษัทฯ ไปใช้ในงานส่วนตัว

(2) เจ้าหน้าที่บริษัทฯ ต้องรับผิดชอบในการรักษาข้อมูลสารสนเทศที่ตนเป็นเจ้าของให้อยู่ในสภาพที่สมบูรณ์

(3) กรณีที่ระบบสารสนเทศอยู่ในพื้นที่ปราศจากผู้ดูแล เจ้าหน้าที่บริษัทฯ ต้องดำเนินการจัดเก็บ หรือล็อคอุปกรณ์ไว้อย่างรัดกุม

(4) เจ้าหน้าที่บริษัทฯ ต้องเฝ้าระวังขณะพิมพ์รายงานที่มีความสำคัญ โดยมีการเฝ้าระวังรายงานที่จัดพิมพ์จากบุคคลที่ไม่เกี่ยวข้อง

หมวด 4
ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

วัตถุประสงค์

เพื่อให้เจ้าหน้าที่บริษัทฯ เข้าใจถึงบทบาท และหน้าที่ความรับผิดชอบของตน และลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์อย่างผิดวัตถุประสงค์ภายในบริษัทฯ

ข้อ 10 การจัดการกับเจ้าหน้าที่เข้าดำเนินการ

(1) แจ้งให้เจ้าหน้าที่ หรือบุคคลที่เกี่ยวข้องทราบถึงนโยบายการใช้ระบบสารสนเทศบริษัทฯ เพื่อปกป้องสารสนเทศ และข้อมูลสารสนเทศจากบุคคลที่ไม่เกี่ยวข้อง

ข้อ 11 การพัฒนาบุคลากรให้ตระหนักต่อนโยบายฯ

(1) เจ้าหน้าที่ หรือบุคคลที่เกี่ยวข้องต้องเข้ารับการอบรม และเข้าร่วมกับการให้ความรู้เกี่ยวกับ กฎระเบียบ และนโยบายฯ เพื่อให้ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศอย่างถูกต้องเหมาะสม

(2) จัดทำและปรับปรุงคู่มือการปฏิบัติงาน เพื่อใช้เป็นแนวทางในการปฏิบัติงาน ทั้งนี้ คู่มือดังกล่าวสามารถจัดทำในรูปแบบสิ่งพิมพ์หรืออิเล็กทรอนิกส์

(3) ทดสอบการปฏิบัติงานตามคู่มือที่จัดทำขึ้น

ข้อ 12 การยุติการว่าจ้าง

(1) ดำเนินการยกเลิกสิทธิ์ด้านการใช้ทรัพย์สินบริษัทฯ และทรัพย์สินที่เป็นสารสนเทศองค์กรทันทีที่มีการยุติการว่าจ้าง หรือมีการเปลี่ยนความรับผิดชอบในหน่วยงาน

หมวด 5
ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่หวงห้ามภายในบริษัทฯโดยไม่ได้รับอนุญาต อันจะก่อให้เกิดความเสียหาย การรบกวน และ/หรือการแทรกแซงต่อทรัพย์สินสารสนเทศของบริษัทฯ

ข้อ 13 การปฏิบัติของเจ้าหน้าที่ในพื้นที่บริษัทฯ

(1) ติดบัตรเจ้าหน้าที่ตลอดเวลาเพื่อแสดงตัวการเป็นเจ้าหน้าที่ของบริษัทฯ

(2) เพื่อป้องกันการรั่วไหลของข้อมูลที่มีความสำคัญ ต้องดำเนินการขออนุญาตก่อนการนำสื่อสารสนเทศ ข้อมูลสารสนเทศที่มีความสำคัญออกนอกบริษัทฯ

ข้อ 14 การปฏิบัติของเจ้าหน้าที่ในพื้นที่ห้องคอมพิวเตอร์

(1) จัดเตรียมห้องคอมพิวเตอร์เพื่อจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ที่สำคัญในระบบสารสนเทศ

(2) กำหนดผู้รับผิดชอบในการดูแลห้องคอมพิวเตอร์อย่างชัดเจน โดยมีการบันทึกเวลาที่ปฏิบัติงานในห้องคอมพิวเตอร์

(3) จัดเตรียมระบบตรวจสอบผู้เข้าออกห้องคอมพิวเตอร์ และมีการตรวจสอบอย่างรัดกุม

(4) กรณีที่มีบุคคลภายนอก หรือบุคคลที่ไม่มีส่วนเกี่ยวข้องกับการเข้าใช้ศูนย์คอมพิวเตอร์ แต่จำเป็นที่ต้องเข้าไปสู่ศูนย์คอมพิวเตอร์ต้องมีการขออนุญาตอย่างเป็นทางการ

(5) แผนผังแสดงรายละเอียดโครงสร้างระบบเครือข่าย ถือว่าเป็นข้อมูลความลับ (Confidential) ห้ามไม่ให้มีการเผยแพร่สู่บุคคลภายนอกโดยไม่ได้รับอนุญาต

(6) ห้องคอมพิวเตอร์ต้องมีระบบสำรองไฟฟ้าและ/หรือระบบผลิตไฟฟ้าอย่างเพียงพอ และมีการกำหนดรอบในการตรวจสอบ และบำรุงรักษาระบบอย่างเหมาะสม

(7) ห้องคอมพิวเตอร์ต้องมีระบบควบคุมอุณหภูมิ และป้องกันความชื้น และมีการกำหนดรอบตรวจสอบ และบำรุงรักษาระบบอย่างเหมาะสม

(8) ผู้ดูแลห้องคอมพิวเตอร์ต้องให้ความร่วมมือในการจัดทำแผนการปฏิบัติงานบริษัทฯอย่างต่อเนื่องทั้งในด้านการจัดทำขั้นตอนปฏิบัติ และความร่วมมือในการฝึกแผนฉุกเฉิน

(9) จัดทำแผนกู้คืนกรณีที่เกิดภัยพิบัติ หรือดำเนินจัดทำศูนย์คอมพิวเตอร์สำรองขึ้น เพื่อรองรับต่อภัยคุกคามที่มีผลต่อการดำเนินงานในกรณีที่เกิดภัยพิบัติ

หมวด 6
การบริหารจัดการงานด้านการสื่อสารข้อมูลสารสนเทศ

วัตถุประสงค์

เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศทั้งเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และคอมพิวเตอร์ลูกข่ายเป็นไปอย่างถูกต้องปลอดภัย และพร้อมใช้งานอยู่เสมอ โดยลดปัญหาความเสี่ยงที่เกิดขึ้นจากภัยคุกคามต่างๆที่มีผลต่อระบบสารสนเทศของบริษัทฯ

ข้อ 15 การใช้งานจดหมายอิเล็กทรอนิกส์

(1) จดหมายอิเล็กทรอนิกส์ของบริษัทฯห้ามนำไปใช้ในงานส่วนตัวที่ส่งผลกระทบต่อระบบโดยรวม และมีผลต่อชื่อเสียงของบริษัทฯ

(2) ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ต้องได้รับทราบ มีความรู้และความเข้าใจในการใช้งานจดหมายอิเล็กทรอนิสก์ที่ถูกต้อง และมีความตระหนักถึงความปลอดภัยในการใช้งานอยู่ตลอดเวลา

(3) เจ้าหน้าที่ต้องปฏิบัติตามข้อกำหนดของการใช้งานจดหมายอิเล็กทรอนิกส์อย่างเคร่งครัด เช่นการใช้งานไฟล์แนบที่เหมาะสม ขนาดสูงสุดการรับส่งข้อมูล การบริหารขนาดที่จัดเก็บของระบบจดหมายอิเล็กทรอนิกส์ เป็นต้น

(4) บริษัทฯ ต้องมีกระบวนการตรวจสอบการใช้งานจดหมายอิเล็กทรอนิกส์ทั้งรับเข้าและส่งออกของบริษัทฯ ที่มีผลต่อบริษัทฯ ถ้ามีการร้องขอจากทางราชการ และผ่านความเห็นชอบจากกรรมการบริหารฯ ฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิ์ในการเข้าไปตรวจสอบบันทึกกิจกรรมที่เกิดขึ้น โดยไม่ละเมิดความเป็นส่วนตัว

(5) จดหมายอิเล็กทรอนิกส์ที่มีรูปแบบลูกโซ่ หรือสแปม (Spam Mail) ห้ามไม่ให้เจ้าหน้าที่ทำการสร้าง หรือส่งต่อภายในบริษัทฯ เมื่อพบว่ามีจดหมายสแปม หรือสิ่งผิดปกติที่แนบมาพร้อมกับจดหมายอิเล็กทรอนิกส์เข้ามาในระบบ ให้แจ้งฝ่ายเทคโนโลยีสารสนเทศทราบทันที และดำเนินการลบจดหมายดังกล่าวทิ้ง

(6) ไม่อนุญาตให้ส่งจดหมายอิเล็กทรอนิกส์ของบริษัทฯ ที่มีความหมาย อันก่อให้เกิดผลเสียหายต่อความมั่นคงของประเทศ การก่อการร้าย ลามกอนาจาร หรือให้ผู้อื่นเสียหาย

(7) กำหนดให้มีการเข้ารหัสจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาสาระที่สำคัญ

(8) เครื่องที่ใช้งานจดหมายอิเล็กทรอนิกส์ต้องมีการติดตั้ง และลงโปรแกรมในการป้องกันไวรัสคอมพิวเตอร์ รวมถึงการปฏิบัติตามข้อปฏิบัติในการป้องกันไวรัสของบริษัทฯ

(9) ผู้ไม่ปฏิบัติตามกฎเกณฑ์ในการใช้งานจดหมายอิเล็กทรอนิกส์ จะถูกระงับการใช้งานจนกว่าจะได้รับอนุญาตจากผู้มีอำนาจ

ข้อ 16 การเชื่อมต่อสู่เครือข่ายภายนอก

(1) ผู้ใช้งานอินเตอร์เน็ตต้องได้รับบัญชีรายชื่อ (User Password) ในการเข้าใช้ ก่อนดำเนินการใช้งาน

(2) ต้องมีการจัดทำขั้นตอนการขออนุญาตในการจัดทำการเชื่อมต่อสู่เครือข่ายภายนอก โดยกระบวนการต้องผ่านความเห็นชอบจากผู้มีอำนาจก่อนมีการเชื่อมต่อเครือข่ายสู่ภายนอก

(3) ผู้ใช้งานอินเตอร์เน็ตต้องได้รับทราบ มีความรู้และความเข้าใจในการใช้งานอินเตอร์เน็ตที่ถูกต้อง และมีความตระหนักถึงความปลอดภัยในการใช้งานอยู่ตลอดเวลา

(4) เครื่องที่เชื่อมต่อระบบเครือข่าย ต้องมีการติดตั้ง และลงโปรแกรมในการป้องกันไวรัสคอมพิวเตอร์ รวมถึงการปฏิบัติตามข้อปฏิบัติในการป้องกันไวรัสของบริษัทฯ

(5) ต้องมีระบบตรวจสอบเนื้อหา และข้อมูลที่รับเข้า และส่งออกจากเครือข่ายของบริษัทฯ เพื่อตรวจสอบโค้ดที่มุ่งร้าย และข้อความที่ไม่เหมาะสม

(6) เมื่อพบหรือสงสัยว่ามีสิ่งผิดปกติในการใช้งาน ให้แจ้งฝ่ายเทคโนโลยีสารสนเทศ

(7) กรณีที่มีการกำหนดการเชื่อมต่อเครือข่ายอินเตอร์เน็ตแบบเรียลไทม์กับคอมพิวเตอร์ภายในบริษัทฯ ที่ใช้ผ่านเครือข่ายจำลองส่วนบุคคล (VPN) ต้องได้รับอนุญาตจากผู้มีอำนาจ

(8) ห้ามประกาศข้อความใดๆที่เกี่ยวข้องกับบริษัทฯในทางเสื่อมเสีย ในเว็บบอร์ดหรือห้องสนทนาบนกลุ่มสาธารณะใดๆ บนอินเตอร์เน็ต

(9) บริษัทฯห้ามใช้นามสมมุติ หรือนามผู้อื่นบนระบบสารสนเทศใดๆ ของบริษัทฯ

(10) การเปิดเผยข้อมูลหรือความลับของบริษัทฯ จะต้องเป็นไปตามข้อกำหนดของฝ่ายทรัพยากรบุคคลและฝ่ายกฎหมาย

ข้อ 17 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์

(1) ใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ สำหรับงานของบริษัทฯเท่านั้น

(2) การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ที่มีผลกระทบต่อการทำงาน ประสิทธิภาพระบบเครือข่าย ต้องผ่านความเห็นชอบจากผู้มีอำนาจ

(3) ผู้ใช้ที่ต้องการใช้อินเทอร์เน็ตและสื่อสังคมออนไลน์ต้องผ่านการอบรมเรื่องความปลอดภัยในการใช้งานอินเทอร์เน็ตและอินทราเน็ต

(4) หลีกเลี่ยงการประกาศข้อความใดๆ ในเว็บบอร์ด ห้องสนทนาเครือข่าย หรือกลุ่มสาธารณะใดๆ บนอินเทอร์เน็ต โดยใช้รายชื่อจดหมายอิเล็กทรอนิกส์ของบริษัทฯ เพื่อป้องกันการถูกสแปมในจดหมายอิเล็กทรอนิกส์

(5) หลีกเลี่ยงการประกาศข้อความใดๆ ในเว็บบอร์ด ห้องสนทนาเครือข่าย หรือกลุ่มสาธารณะใดๆ บนอินเทอร์เน็ตและอินทราเน็ต ที่มีความหมายในทางหลอกลวงให้ผู้อื่นเสียหาย ทำให้เกิดเสียหายต่อความมั่นคงของประเทศ ก่อการร้าย หรือลามกอนาจาร

ข้อ 18 การใช้งานระบบสารสนเทศบนเครือข่ายไร้สาย

(1) การใช้งานเครือข่ายไร้สายต้องได้รับอนุญาตจากผู้มีอำนาจ

(2) ห้ามเปิดเผยข้อมูลเกี่ยวกับค่ากำหนดหรือรหัสในเครือข่ายไร้สายกับบุคคลที่ไม่เกี่ยวข้อง

(3) ควบคุมการใช้งานเครือข่ายไร้สาย และกำหนดพื้นที่ให้บริการเฉพาะเท่าที่จำเป็นเท่านั้น

(4) การเข้าใช้งานเครือข่ายไร้สายต้องมีระบบตรวจสอบตัวตน และการเข้ารหัส รองรับอีกระดับหนึ่ง รวมถึงต้องมีการบันทึกล็อก (Log) การใช้งานระบบเครือข่ายไร้สาย

(5) ต้องมีระบบป้องกันการแก้ไขเปลี่ยนแปลงค่าบันทึกล็อก (Log) และกำหนดสิทธิ์การเข้าถึงบันทึก ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(6) ต้องมีการจัดเตรียมเครื่องมือตรวจสอบการใช้งานอุปกรณ์ไร้สาย และระบุให้กับบุคคลที่รับผิดชอบเท่านั้น

ข้อ 19 การใช้งานระบบป้องกันผู้บุกรุกหรือไฟร์วอลล์

(1) อุปกรณ์ป้องกันผู้บุกรุกหรือไฟร์วอลล์ต้องตั้งไว้ในพื้นที่ที่มีความปลอดภัย และมีความเหมาะสม

(2) อุปกรณ์ป้องกันผู้บุกรุกหรือไฟร์วอลล์ต้องมีระบบป้องกันการโจมตี เพื่อสนับสนุนการทำงานของอุปกรณ์ เช่น อุปกรณ์ระบบป้องกันผู้บุกรุก ระบบป้องกันไวรัสผ่านเกตเวย์ เป็นต้น

(3) มีการออกแบบ และกำหนดตำแหน่งในการตั้ง อุปกรณ์ระบบป้องกันผู้บุกรุก ให้เหมาะสม โดยเฉพาะเครือข่ายที่เชื่อมต่อกับภายนอก

(4) อุปกรณ์ไฟร์วอลล์ต้องมีการปรับปรุงซอฟต์แวร์ให้เป็นปัจจุบันทันสมัยอยู่เสมอ โดยไม่ส่งผลกระทบต่อการทำงานของบริษัทฯ

(5) ผู้ใช้งาน และผู้ดูแลระบบต้องไม่แจ้งช่องโหว่ที่พบไปยังบุคคลภายนอก หรือบุคคลภายในที่ไม่เกี่ยวข้อง นอกเสียจากจะถูกกำหนดให้เป็นผู้รับผิดชอบในการแก้ปัญหานั้นๆ

(6) ต้องตรวจสอบเกี่ยวกับความปลอดภัยอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่นตรวจสอบไวรัส ตรวจสอบการกำหนดค่าพารามิเตอร์ต่างๆ เกี่ยวกับความปลอดภัยรวมไปถึงการตัดการเชื่อมต่ออุปกรณ์คอมพิวเตอร์ออกจากระบบเครือข่าย

(7) ติดตั้งซอฟต์แวร์ตรวจสอบไวรัสที่ได้รับการอนุมัติจากผู้มีอำนาจบนเครื่องที่ติดตั้งอุปกรณ์ระบบป้องกันผู้บุกรุกทั้งหมด

(8) กรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะการเข้าใช้จากทางไกล (Remote access) หรือการเชื่อมต่อเครือข่ายภายนอกโดยใช้ผ่านเครือข่ายจำลองส่วนบุคคล (VPN) ต้องมีการจัดตั้งอุปกรณ์ระบบป้องกันผู้บุกรุกเพื่อตรวจสอบการละเมิดการใช้งาน

หมวด 7
การดำเนินงานใช้งานระบบข้อมูลสารสนเทศของบริษัทฯ

ข้อ 21 การกำหนดหน้าที่ในการปฏิบัติงานประจำกับการดูแลระบบสารสนเทศ

(1) มีการกำหนดสายบังคับบัญชา และขอบเขตการทำงาน ในการปฏิบัติงานประจำในด้านต่างๆที่สำคัญอย่างชัดเจน

(2) ต้องมีการเขียนขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer operator) ทราบ

(3) กำหนดให้เจ้าที่ปฏิบัติการคอมพิวเตอร์ปฏิบัติงานโดยผ่านเมนู และจำกัดการปฏิบัติงานโดยใช้บรรทัดคำสั่ง (Command line) เท่าที่จำเป็น

(4) กำหนดให้มีการบันทึกล็อก (log book) หรือเทียบเท่า ซึ่งมีรายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่างๆ ดังนี้ ผู้ปฏิบัติงาน เวลาปฏิบัติงาน รายละเอียดการปฏิบัติงาน ปัญหาที่เกิดขึ้นและการแก้ไข สถานะของระบบ และผู้ตรวจสอบการปฏิบัติงาน

(5) ติดตามสถานะการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่อง และมีประสิทธิภาพ เช่น การรับส่งข้อมูล การใช้ฮาร์ดดิสก์ การใช้งานหน่วยประมวลผล (CPU) การใช้งานหน่วยความจำ เป็นต้น

(6) กำหนดให้มีการบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่างๆให้อยู่ในสภาพที่ดี และพร้อมใช้งานอยู่เสมอ

(7) กำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ปัญหาอย่างชัดเจน รวมถึงหมายเลขโทรศัพท์ของผู้เกี่ยวข้อง เพื่อใช้ในการติดต่อเมื่อเกิดปัญหาทุกระดับ

(8) จัดทำระบบจัดเก็บบันทึกปัญหา และเหตุการณ์ผิดปกติที่เกิดขึ้น พร้อมรายงานให้ผู้บังคับบัญชาได้ทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหา และตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาในอนาคต

(9) การขอให้จัดพิมพ์รายงานต่างๆ ของระบบงานที่สำคัญต้องได้รับความเห็นชอบจากเจ้าของข้อมูลสารสนเทศหรือผู้ที่ได้รับมอบหมาย

(10) เอกสารหรือข้อมูลสารสนเทศที่ได้ยกเลิกให้ดำเนินการจัดทำลายทิ้งตามขั้นตอนปฏิบัติในการจัดทำลายเอกสาร

ข้อ 22 การใช้งานเครื่องคอมพิวเตอร์พกพาและอุปกรณ์พกพา

(1) ข้อมูลในอุปกรณ์พกพาต้องมีหรือมีวิธีการป้องกันการเข้าใช้อย่างรัดกุม

(2) ห้ามกำหนดค่าเพื่อแบ่งปันไฟล์ข้อมูลในเครื่องคอมพิวเตอร์พกพา/อุปกรณ์พกพาผ่านเครือระบบเครือข่าย นอกเสียจากมีความจำเป็นในการสำเนา หรือย้ายไฟล์ เมื่อดำเนินการเสร็จเรียบร้อยแล้วให้ทำการยกเลิกการแบ่งปันข้อมูลดังกล่าวทันที

(3) เครื่องคอมพิวเตอร์พกพา/อุปกรณ์พกพาต้องมีการติดตั้ง และปฏิบัติตามนโยบายการป้องกันไวรัสที่กำหนดไว้ของบริษัทฯ

(4) การเข้าใช้คอมพิวเตอร์/อุปกรณ์พกพาทางไกลจากภายนอกต้องได้รับการอนุญาตจากผู้มีอำนาจ ซึ่งต้องมีการกำหนดอายุการใช้งาน และมีรอบการตรวจสอบในทุกปี

(5) ห้ามเก็บรหัสผ่าน รหัสผู้ใช้ หรือระบบกลไกควบคุมการเข้าใช้ต่างๆ ในเครื่องคอมพิวเตอร์พกพา/อุปกรณ์พกพา หากจำเป็นต้องจัดเก็บให้กำหนดอยู่ในรูปแบบที่ไม่สามารถเข้าถึงได้จากบุคคลที่ไม่เกี่ยวข้อง

(6) กรณีอยู่ในที่สาธารณะและไม่มีผู้ดูแล ต้องมีการล็อค (Lock) เครื่องคอมพิวเตอร์พกพา/อุปกรณ์พกพา หรือจัดเก็บคอมพิวเตอร์พกพาในพื้นที่ควบคุมจากบุคคลภายนอก

ข้อ 23 การป้องกันไวรัส

(1) เครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ของบริษัทฯต้องมีซอฟต์แวร์ป้องกันไวรัสที่ถูกลิขสิทธิ์ พร้อมทั้งปรับปรุงฐานข้อมูลของซอฟต์แวร์ป้องกันไวรัสให้เป็นปัจจุบันอยู่เสมอ

(2) เมื่อพบสิ่งผิดปกติในระบบสารสนเทศของบริษัทฯ ให้แจ้งฝ่ายเทคโนโลยีสารสนเทศทราบทันที

(3) ผู้ใช้งานคอมพิวเตอร์ต้องการเชื่อมต่อเครือข่ายภายนอกบริษัทฯ ต้องตรวจสอบข้อมูลชื่อเครือข่ายและรหัสผ่านให้ถูกต้องตามแหล่งที่มา หรือเครือข่ายที่ไม่มีการใส่รหัสผ่านก่อนเข้าใช้งาน ให้หลีกเลี่ยงการเข้าใช้งานเครือข่ายประเภทนี้

(4) ผู้ใช้งานเครื่องคอมพิวเตอร์ต้องไม่ทำการติดตั้งโปรแกรมใดๆ ที่ไม่ทราบแหล่งที่มา หรือไม่ได้มาจากแหล่งที่ทางฝ่ายเทคโนโลยีสารสนเทศรับรอง

(5) ห้ามพัฒนาโปรแกรมไวรัสคอมพิวเตอร์ หรือนำโปรแกรมไวรัสคอมพิวเตอร์หรือไวรัสมาเผยแพร่

(6) ต้องมีการเฝ้าระวังระบบเครือข่าย และคอมพิวเตอร์ เพื่อป้องกันปัญหาด้านไวรัสคอมพิวเตอร์ เมื่อพบเครื่องต้องสงสัยว่าติดไวรัสให้ปฏิบัติตามแนวทางปฏิบัติที่ทางฝ่ายเทคโนโลยีสารสนเทศกำหนด

(7) ไม่ถอดถอน (Remove/Uninstall) หรือปิดบริการซอฟต์แวร์ป้องกันไวรัสบนเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต

หมวด 8
การควบคุมการเข้าถึงสารสนเทศบริษัทฯ (Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงสารสนเทศของบริษัทฯ จากผู้ที่ไม่ได้รับอนุญาตทั้งระบบเครือข่าย ระบบปฏิบัติการ และแอพพลิเคชัน โดยมุ่งเน้นที่การป้องกันปัญหาจากการพิสูจน์ตัวตน กำหนดสิทธิ์และการบันทึกกิจกรรมที่ดำเนินการในด้านการเข้าถึงระบบสารสนเทศต่างๆ ภายในบริษัทฯ

ข้อ 24 การควบคุมการเข้าถึงของพนักงาน

(1) รหัสผ่านถือเป็นข้อมูลสารสนเทศระดับชั้นความลับของบริษัทฯ ดังนั้นพนักงานบริษัทฯต้องรักษารหัสผ่านไม่ให้มีผู้ใดสามารถเข้าถึง หรือขโมยได้

(2) ปฏิบัติตามข้อกำหนดในเรื่องการกำหนดค่ารหัสผ่าน และ
- ไม่ใช้ข้อมูลส่วนตัวของผู้ใช้มาเป็นรหัสผ่าน เช่น ชื่อ นามสกุล วันเดือนปีเกิด รหัสพนักงาน
- ทำการเปลี่ยนรหัสผ่านทุกๆ 90 วัน
- ไม่จดรหัสผ่านในที่ผู้อื่นเข้าถึงได้

(3) ล็อคหน้าจอเครื่องคอมพิวเตอร์ทุกครั้งเมื่อไม่อยู่ที่หน้าเครื่องคอมพิวเตอร์

(4) ทุกครั้งที่มีผู้ใต้บังคับบัญชาที่ใช้ระบบสารสนเทศพ้นจากหน้าที่งานในระบบสารสนเทศจะต้องแจ้งมายังฝ่ายเทคโนโลยีสารสนเทศเพื่อระงับการใช้งานของผู้ใช้งานนั้นทันที

(5) สำหรับการสร้าง การแก้ไขเปลี่ยนแปลง และการระงับหรือลบข้อมูลผู้ใช้ ต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษรหรือมีหลักฐานทาง e-mail แจ้งมายังฝ่ายเทคโนโลยีสารสนเทศเพื่อดำเนินการสร้าง เปลี่ยนแปลง และแก้ไขทันที

(6) การสอบทานรหัสผู้ใช้งานระบบ จะดำเนินการตรวจสอบทุกไตรมาส เพื่อให้ได้รายละเอียดและสถานะของรหัสผู้ใช้งานและผู้ใช้งานที่แท้จริง ในกรณีที่เป็นรหัสผู้ใช้งานร่วมกัน (Shared User) ให้ระบุรายชื่อผู้ที่รับผิดชอบหรือผู้ใช้งานจริงในระบบเพื่อสำหรับการพิสูจน์ตัวตนในการเข้าใช้งานระบบสารสนเทศ

(7) รหัสผู้ใช้งานที่ไม่สามารถระบุตัวตนได้ (Generic User) จะมีเฉพาะรหัสสำหรับการทำงานอัตโนมัติของระบบสารสนเทศเท่านั้น ส่วนรหัสผู้ใช้งานจะต้องเป็นรหัสผู้ใช้งานที่ระบุตัวตนได้เท่านั้น

ข้อ 25 การควบคุมรหัสผ่าน

(1) ต้องกำหนดรหัสผ่านให้มีระดับความปลอดภัยที่เหมาะสม และรัดกุม
- กำหนดรหัสผ่านให้มีความยาวไม่น้อยกว่า 8 ตัวอักษร
- กำหนดรหัสผ่านให้มีความสลับซับซ้อนโดยประกอบด้วยอักขระพิเศษ ตัวอักษรเล็ก ตัวอักษรใหญ่ และตัวเลข
- กำหนดให้ผู้ใช้พิมพ์รหัสผ่านผิดต่อเนื่องกันได้ไม่เกิน 3 ครั้ง

- ไม่กำหนดรหัสผ่าน โดยใช้ข้อมูลส่วนตัวหรือเกี่ยวข้องกับตนเอง
- ไม่กำหนดรหัสผ่านที่เป็นคำอยู่ในพจนานุกรม
- การปรับเปลี่ยนรหัสผ่านไม่ซ้ำของเดิมอย่างน้อย 3 ครั้ง

(2) ไม่เขียนรหัสผ่าน หรือจดบันทึกไว้ในที่มองเห็นได้โดยง่าย ยกเว้นแต่มีรูปแบบการเขียนที่ไม่สามารถอ่านได้ง่าย หรือจัดเก็บไว้ในพื้นที่ส่วนตัว

ข้อ 26 การควบคุมการเข้าถึงของผู้ดูแลระบบ

(1) ต้องมีการกำหนดสิทธิ์การใช้ข้อมูล และระบบคอมพิวเตอร์หลักของบริษัทฯ เช่น การใช้โปรแกรมคอมพิวเตอร์ การใช้งานอินเตอร์เน็ต โดยผู้ใช้ได้รับสิทธิ์เท่าที่จำเป็น และได้ผ่านความเห็นชอบจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษร

(2) มีระบบตรวจสอบตัวตน และสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานหลัก

(3) ค่ากำหนดเริ่มต้นของระบบไฟล์ และข้อมูลสารสนเทศต่างๆ ต้องถูกกำหนดโดยควบคุมไม่อนุญาตให้ใช้ก่อนเสมอ

(4) กรณีที่ผู้ปฏิบัติงานไม่อยู่หน้าเครื่องคอมพิวเตอร์ ต้องมีการป้องกันการใช้งานโดยบุคคลอื่นๆ ที่ไม่มีหน้าที่เกี่ยวข้องหรือไม่มีสิทธิ์

(5) ระบบงานต่างๆ ต้องมีการติดตั้งระบบให้มีระบบความปลอดภัยสูงสุดในปัจจุบันเท่าที่เป็นไปได้

(6) ต้องมีการควบคุมการเข้าถึงเครื่องแม่ข่าย และมีการควบคุมไฟล์ที่เปิดเข้าใช้งาน ทั้งการพิสูจน์ตัวตน การควบคุมสิทธิ์ และการจัดเก็บล็อก

(7) ระบุผู้รับผิดชอบในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่ากำหนดต่างๆ ที่ใช้ในระบบ

(8) ต้องมีการตรวจสอบ หรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์ และเมื่อพบสิ่งผิดปกติในระบบ ต้องรีบดำเนินการแก้ไขทันที

(9) การเข้าถึงระบบเครือข่ายในลักษณะเข้าถึงทางไกล (Remote access) ต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษร

(10) ซอฟต์แวร์ที่ติดตั้งใช้งานเพื่อกิจการของบริษัทฯต้องมีลิขสิทธิ์ถูกต้อง หรือได้รับอนุมัติจากเจ้าของผลิตภัณฑ์ หรือตกลงกับตัวแทนผู้ขายภายในประเทศล่วงหน้า

(11) ต้องมีตรวจสอบและวัดประสิทธิภาพการทำงานของระบบงานสำคัญ เพื่อรองรับการใช้งานในอนาคต

หมวด 9
การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศที่ได้ตรงกับความต้องการของบริษัทฯ และมีความมั่นคงปลอดภัยที่เหมาะสม โดยเจ้าหน้าที่ และบุคคลที่เกี่ยวข้องต่างๆ มีความเข้าใจต่อการดำเนินการที่มีการจัดทำอย่างเป็นรูปธรรม

ข้อ 27 พัฒนาระบบสารสนเทศ และการเข้ามีส่วนร่วมของพนักงานในการการจัดหา ทดสอบระบบ

(1) ผู้ใช้งานระบบมีความต้องการพัฒนา แก้ไขหรือจัดซื้อระบบสารสนเทศใหม่ จะต้องแจ้งมาความต้องการเพื่อขออนุมัติจากผู้มีอำนาจพิจารณาในหน่วยงาน สำหรับการพัฒนา แก้ไข และส่งมายังฝ่ายเทคโนโลยีสารสนเทศ

(2) ฝ่ายเทคโนโลยีสารสนเทศได้รับเอกสารการอนุมัติจากผู้มีอำนาจ จะต้องดำเนินการเก็บข้อมูลและมีหลักฐานในการยืนยันการพัฒนา แก้ไขหรือจัดซื้อระบบสารสนเทศใหม่จากผู้ใช้งานระบบเก็บไว้ทุกครั้ง

(3) หลังจากที่มีการพัฒนา แก้ไขหรือจัดซื้อระบบสารสนเทศใหม่เสร็จเรียบร้อย ทางผู้ใช้งานระบบต้องได้เข้าร่วมทดสอบระบบสารสนเทศที่มีการพัฒนา แก้ไขหรือจัดซื้อใหม่ เพื่อให้เหมาะสมกับผู้ใช้งานในระบบสารสนเทศนั้น

(4) ผู้ใช้ระบบลงนามยอมรับผลการทดสอบ เมื่อพบว่าซอฟต์แวร์หรือระบบที่มีการพัฒนา แก้ไขหรือจัดซื้อใหม่มีความสามารถตรงกับที่ผู้ใช้ต้องการก่อนนำขึ้นระบบใช้งานจริง

(5) ฝ่ายเทคโนโลยีสารสนเทศต้องขอพิจารณาอนุมัติการนำระบบที่ผ่านการทดสอบจากผู้ใช้งาน ดำเนินการแจ้งผู้มีอำนาจในการอนุมัติของหน่วยงานเพื่อนำขึ้นระบบจริงทุกครั้ง

(6) แจ้งผลการนำขึ้นระบบจริงให้กับผู้ใช้งานและติดตามผล

ข้อ 28 การควบคุมการจัดหา และการพัฒนาเปลี่ยนแปลงระบบงานคอมพิวเตอร์

(1) จัดทำขั้นตอนหรือวิธีปฏิบัติในการพัฒนา การแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน (กำหนดขอบเขต และให้ทุกคนส่งบันทึกมาที่สารสนเทศบริษัทฯเพื่อสรุปรายงาน)

(2) จัดทำขั้นตอน หรือวิธีปฏิบัติในการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และมีบันทึกเหตุผลความจำเป็น และการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

(3) ระบบงานหลักต้องมีการแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาและทดสอบระบบงาน (Development & Test environment) ออกจากส่วนที่ใช้งานจริง (Production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้เกี่ยวข้องในแต่ละส่วนเท่านั้น

(4) การร้องขอให้มีการพัฒนา หรือการเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำอย่างเป็นลายลักษณ์อักษรจากผู้มีอำนาจหน้าที่

(5) ในระบบงานสำคัญต้องมีหน่วยงาน หรือทีมงานเข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนา และการทดสอบระบบก่อนที่จะโอนย้ายไปใช้งานจริง

(6) ต้องจัดเก็บโปรแกรมเวอร์ชันก่อนการพัฒนาไว้ใช้ในกรณีที่เวอร์ชันปัจจุบันทำงานผิดพลาดหรือไม่สามารถทำงานได้

หมวด 10
การเข้ารหัสข้อมูลสารสนเทศ

วัตถุประสงค์

เพื่อให้การจัดเก็บข้อมูลสารสนเทศของบริษัทฯ ที่ปัจจุบันเริ่มมีการจัดเก็บในพื้นที่สาธารณะ หรือในอุปกรณ์พกพาจำนวนมากมีความปลอดภัย และป้องกันการถูกเปิดเผยข้อมูลดังนั้นบริษัทฯ จึงเห็นสมควรที่จัดทำนโยบายด้านการเข้ารหัสข้อมูลสารสนเทศเพื่อให้เกิดความปลอดภัยในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์พกพา หรือในพื้นที่จัดเก็บข้อมูลสาธารณะเช่น Cloud storage ต่างๆ

ข้อ 29 การบริหารระบบการเข้ารหัส

(1) ผู้ให้บริการจะต้องทำการเข้ารหัสในการจัดเก็บและกระบวนการสื่อสารในข้อมูลสารสนเทศที่สำคัญ โดยปฏิบัติตามข้อกำหนดมาตรฐานในการเข้ารหัสที่เป็นสากล

(2) ประชาสัมพันธ์ และสร้างความตระหนักต่อการใช้งานข้อมูลสารสนเทศองค์กรให้กับผู้ใช้ข้อมูลสารสนเทศโดยระบุให้มีความปลอดภัยสอดคล้องต่อมาตรการของคณะกรรมการฯ

(3) การบริหารความเสี่ยงการใช้บริการคลาวด์ ควรสอดคล้องกับความเสี่ยงจาก การใช้บริการ โดยต้องได้รับความเห็นชอบจากคณะกรรมการฯ

(4) มีการกำหนดหน้าที่ผู้ให้บริการให้เหมาะสมกับรูปแบบ และประเภทการใช้ ตามลักษณะการใช้บริการ
- เลือกใช้และกำหนดรายละเอียดรูปแบบการใช้ประเภทการบริการ ที่รองรับการดำเนินของบริษัทฯ
- กำหนดมาตรฐานการรักษาความลับ ความปลอดภัยของข้อมูล
- ต้องจัดให้มีกระบวนการ ขั้นตอน หรือระบบในการติดตาม ตรวจสอบผู้ให้บริการ เพื่อให้มั่นใจว่าผู้ให้บริการสามารถดำเนินการได้ตามแนวทางที่ได้ตกลงไว้

(5) ผู้ให้บริการต้องจัดให้มีการสำรองข้อมูล และระบบงานสารสนเทศให้อยู่ในสภาพ พร้อมใช้งาน

(6) ผู้ให้บริการต้องจัดให้มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) หรือ แผนสำรองฉุกเฉิน (Disaster Recovery Plan) ของระบบสารสนเทศของบริษัทฯ ที่ครอบคลุมถึงการใช้บริการ เพื่อให้สามารถปฏิบัติงานได้จริง รวมทั้งต้อง จัดให้มีกระบวนการในการบริหารจัดการปัญหาหรือเหตุการณ์ผิดปกติ ที่เกิดจาก การใช้บริการ และมีการรายงานปัญหาหรือเหตุการณ์ผิดปกติ และการจัดการปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว ให้บริษัทฯ รับทราบตามข้อตกลงการให้บริการ

หมวด 11
การบริหารจัดการผู้ให้บริการภายนอก

วัตถุประสงค์

เพื่อให้ผู้ให้บริการภายนอกที่บริษัทฯได้เลือกมามีความเหมาะสมต่อการเข้ามาดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสารบริษัทฯ จึงจำเป็นที่ต้องออกนโยบายการบริหารจัดการผู้ให้บริการภายนอก เพื่อเป็นเกณฑ์ในการปฏิบัติต่อผู้มีส่วนได้ส่วนเสียกับการบริหารจัดการผู้ให้บริการภายนอก

ข้อ 30 การบริหารงานผู้ให้บริการภายนอก

(1) กำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการโดยพิจารณาจากฐานข้อมูลการคัดกรองของหน่วยงานกลาง และ/หรือเกณฑ์ที่บริษัทฯได้จัดทำขึ้นเพื่อใช้เป็นเงื่อนไขของการจัดซื้อจัดจ้างของงานสารสนเทศ

(2) กรณีที่ผู้ให้บริการภายนอกเข้าถึงระบบงานสำคัญให้จัดทำสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Non-Disclosure Agreement) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน

- ในกรณีที่ผู้ให้บริการภายนอกมีความจำเป็นที่จะเข้าถึงระบบงานสำคัญ ให้ทำการแจ้งอีเมลเป็นลายลักษณ์อักษรเพื่อขอพิจารณาอนุมัติจากผู้มีอำนาจของฝ่ายเทคโนโลยีสารสนเทศก่อนการเข้าถึงระบบทุกครั้ง
- ระบุรายละเอียดของการเข้าถึง ระบบที่ต้องการเข้าถึงและระบุรหัสผู้ใช้งานในการเข้าถึง
- หลังจากที่ได้รับการอนุมัติจากผู้มีอำนาจของฝ่ายเทคโนโลยีสารสนเทศ ผู้ดูแลระบบจะเปิดให้บริการภายในระยะเวลา 7 วัน, 15 วันและ 30 วัน แล้วแต่ลักษณะของงานนั้น ถ้าหมดอายุให้ทำการร้องขอพิจารณาอนุมัติทางอีเมลอีกครั้ง

(3) กรณีที่ใช้บริการด้านการพัฒนาระบบงานต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Development environment) เท่านั้น หากให้เข้าใช้ระบบงานหลัก (Production environment) ต้องมีการควบคุมและการตรวจสอบผู้ให้บริการอย่างเข้มงวด

(4) ผู้ให้บริการภายนอกต้องรับทราบถึงมาตรการด้านความปลอดภัยที่บริษัทฯ ได้ระบุ และพร้อมปฏิบัติตามอย่างเคร่งครัด

(5) ต้องมีการจัดทำขั้นตอนในการตรวจรับงานของผู้ให้บริการ โดยมีรายละเอียดที่ตระหนักต่อด้านความปลอดภัยสารสนเทศ

หมวด 12
การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทฯ

วัตถุประสงค์

เพื่อให้เหตุการณ์ผิดปกติและจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัทฯได้รับการดำเนินการที่ถูกต้องเหมาะสมในช่วงระยะเวลาอันรวดเร็ว โดยมีการระบุความรับผิดชอบต่อการดำเนินการตอบสนองต่อเหตุการณ์ และบันทึกกิจกรรมที่เกิดขึ้น พร้อมกับการจัดทำขั้นตอนปฏิบัติที่เหมาะสม

ข้อ 31 การปฏิบัติของพนักงานต่อการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทฯ

(1) รายงานเหตุการณ์ผิดปกติให้กับเจ้าหน้าที่ที่เกี่ยวข้องทราบเมื่อพบเห็นเหตุการณ์ผิดปกติทันที

(2) เหตุการณ์ผิดปกติ หรือช่องโหว่ของระบบต้องไม่แจ้งให้กับบุคคลภายนอกทราบ นอกเสียจากเป็นตัวแทนของบริษัทฯในการติดต่อสื่อสารกับกลุ่มงานภายนอกในระบบที่รับผิดชอบอยู่

ข้อ 32 การปฏิบัติของผู้รับผิดชอบต่อการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทฯ

(1) กำหนดผู้รับผิดชอบในเหตุการณ์ผิดปกติแต่ละประเภท

(2) จัดทำบันทึกเหตุการณ์ที่ผิดปกติ ประกอบด้วยรายละเอียดไม่น้อยกว่า ประเภทเหตุการณ์ วันเวลา สถานที่ ลำดับความสำคัญ บุคคลที่ติดต่อ (คนที่แจ้ง)

(3) มีการเลือกยุทธวิธีที่เหมาะสมกับสถานการณ์ต่างๆที่เกิดขึ้นทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้โจมตี เพื่อยุติปัญหาที่เกิดขึ้นได้อย่างทันเวลา และถูกต้อง

(4) ระบบงานต่างๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์ และเครื่องมือสำหรับการสำรองเพื่อใช้เมื่อเกิดปัญหาขึ้น

หมวด 13
การบริหารความต่อเนื่องในการดำเนินงานของบริษัทฯ

วัตถุประสงค์

เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ของบริษัทฯ ที่สำคัญอันเป็นผลมาจากความขัดข้องหรือความล้มเหลวของระบบสารสนเทศนั้น และสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

ข้อ 33 บทบาทของพนักงานในบริษัทฯในการบริหารความต่อเนื่อง

(1) ร่วมทดสอบแผนการบริหารความต่อเนื่องในการดำเนินงานของบริษัทฯ ที่เกี่ยวข้องกับการทำงานของตน

ข้อ 34 การจัดเตรียมระบบคอมพิวเตอร์และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

หมวด 14
การปฏิบัติตามข้อกำหนด

วัตถุประสงค์

เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับบริษัทฯ โดยมีการระบุกลุ่มผู้รับผิดชอบในการตรวจสอบผลการดำเนินการ และการพัฒนาแบบฟอร์มในการตรวจสอบที่มีประสิทธิภาพและมีความชัดเจน

ข้อ 35 การปฏิบัติตามของผู้ใช้งาน

(1) ปฏิบัติตามนโยบายฯสำหรับผู้ใช้งานอย่างเคร่งครัด และรับทราบบทลงโทษในการละเมิดนโยบาย

(2) ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และการใช้ทรัพย์สินถูกต้องตามลิขสิทธิ์ทั้งที่เป็นซอฟต์แวร์ และฮาร์ดแวร์

(3) ผู้ใช้งานที่ไม่ปฏิบัติตามนโยบายที่บริษัทฯ กำหนด จะถูกดำเนินการตามบทลงโทษทางวินัยของบริษัทฯ

(4) ผู้ใช้งานที่ละเมิดต่อการปฏิบัติตามกฎหมายจะพิจารณาลงโทษตามข้อปฏิบัติทางกฎหมาย

ข้อ 36 การตรวจสอบของเจ้าหน้าที่ที่รับผิดชอบ

(1) กำหนดหน้าที่รับผิดชอบต่อผู้ตรวจสอบความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน

(2) ต้องดำเนินการตรวจสอบการปฏิบัติตามนโยบายอย่างรัดกุม และมีรอบการตรวจสอบที่ชัดเจน