นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
บริษัท พราว เรียล เอสเตท จำกัด (มหาชน)

บริษัท พราว เรียล เอสเตท จำกัด (มหาชน) ได้นำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานและให้บริการต่อผู้ใช้งานทั้งภายในและภายนอกองค์กร ดังนั้นเพื่อให้การใช้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่เหมาะสม หรือถูกคุกคามจากภัยต่าง ๆ ซึ่งจะช่วยลดความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงาน บริษัทฯ จึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยมีวัตถุประสงค์ ดังนี้

1. เพื่อกำหนดเป็นนโยบายและแนวทางปฏิบัติให้กรรมการ ผู้บริหาร พนักงานบริษัทฯ ตลอดจนบุคคลที่เกี่ยวข้อง ปฏิบัติตามได้อย่างถูกต้องและสอดคล้องกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่น ๆ ที่เกี่ยวข้อง
2. เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทฯ มีมาตรฐานด้านความมั่นคงปลอดภัย สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีความพร้อมใช้งาน (Availability)
3. เพื่อสื่อสารให้กรรมการ ผู้บริหาร พนักงานรับทราบถึงนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเผยแพร่บนเว็บไซต์บริษัทฯ เพื่อให้บุคคลภายนอกที่เกี่ยวข้องรับทราบและถือปฏิบัติตามอย่างเคร่งครัด

นิยาม

บริษัทฯ หมายถึง บริษัท พราว เรียล เอสเตท จำกัด (มหาชน)

บริษัทย่อย หมายถึง บริษัทที่มีลักษณะใดลักษณะหนึ่ง ดังนี้

1. บริษัทที่บริษัทฯ มีอำนาจควบคุมกิจการ
2. บริษัทที่อยู่ภายใต้อำนาจควบคุมกิจการของบริษัทตาม (1) ต่อไปเป็นทอดๆ โดยเริ่มจากการอยู่ภายใต้อำนาจควบคุมกิจการของบริษัทตาม (1)

กลุ่มบริษัทฯ หมายถึง บริษัท พราว เรียล เอสเตท จำกัด (มหาชน) และบริษัทย่อย

อำนาจควบคุมกิจการ หมายถึง การมีความสัมพันธ์ในลักษณะใดลักษณะหนึ่งดังนี้

(1) การถือหุ้นที่มีสิทธิออกเสียงในบริษัทเกินกว่าร้อยละห้าสิบของจำนวนสิทธิออกเสียงทั้งหมดของบริษัทนั้น

(2) การมีอำนาจควบคุมคะแนนเสียงส่วนใหญ่ในที่ประชุมผู้ถือหุ้นของบริษัท ไม่ว่าโดยตรงหรือโดยอ้อม หรือไม่ว่าเพราะเหตุใด

(3) การมีอำนาจควบคุมการแต่งตั้งหรือถอดถอนกรรมการตั้งแต่กึ่งหนึ่งของกรรมการทั้งหมด ไม่ว่าโดยตรงหรือโดยอ้อม

ผู้ใช้งาน หมายถึง กรรมการ ผู้บริหาร พนักงานหรือบุคคลที่เกี่ยวข้อง ซึ่งใช้งานคอมพิวเตอร์ของกลุ่มบริษัทฯ

บุคคลที่เกี่ยวข้อง หมายถึง บุคคลหรือนิติบุคคลไม่ว่าจะเป็นหน่วยงานรัฐบาล หน่วยงานรัฐวิสาหกิจหรือองค์กรภาคเอกชนที่กลุ่มบริษัทฯ ติดต่อสัมพันธ์ทางธุรกิจ หรือการดำเนินการใดเกี่ยวกับทางการเงิน หรือเกี่ยวกับทรัพย์สินของกลุ่มบริษัทฯ เช่น การบริหาร การซื้อ การขาย การว่าจ้าง เป็นต้น

ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่เทคโนโลยีสารสนเทศ

ผู้บริหารระดับสูง หมายถึง ประธานเจ้าหน้าที่บริหาร

ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดยให้หมายความรวมถึงข้อมูลส่วนบุคคลอ่อนไหว ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพของบุคคลนั้นที่บริษัทฯ ได้เก็บรวบรวมไว้เพื่อการประกอบธุรกิจของบริษัทฯ

เจ้าของข้อมูลส่วนบุคคล หมายถึง ผู้บริหาร เจ้าหน้าที่ ลูกค้า และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ

เจ้าหน้าที่ หมายถึง บุคคลที่เป็นลูกจ้างของบริษัทฯ ไม่ว่าจะเป็นลูกจ้างที่ได้รับค่าจ้างเป็นรายวันหรือรายเดือน รวมถึงลูกจ้างที่อยู่ระหว่างทดลองงาน

ลูกค้า หมายถึง บุคคลที่เข้าทำสัญญาจองสินค้าหรือบริการ หรือสัญญาซื้อขายสินค้าหรือบริการกับบริษัทฯ รวมถึงบุคคลที่ให้ความสนใจที่จะเข้าทำสัญญาจองหรือสัญญาซื้อขายสินค้าหรือบริการบริษัทฯ

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของบริษัทฯ ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

สำนักงาน หมายถึง สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการ์อันไม่อาจทราบได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

แนวทางปฏิบัติ

1. บริษัทฯ ต้องกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย หลักการมาตรฐานสากลของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
2. จัดให้ข้อมูลและระบบเทคโนโลยีสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ สถานที่และสิ่งแวดล้อมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ การพัฒนาและบำรุงรักษาระบบเทคโนโลยีสารสนเทศ และสิ่งใดๆที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ มีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม และมีการควบคุมการเข้าถึงตามข้อกำหนดอย่างชัดเจน
3. จัดให้มีระบบสำรองข้อมูล ระบบกู้คืนข้อมูล และระบบสำรองที่ใช้ทดแทนระบบเทคโนโลยีสารสนเทศหลักในกรณีฉุกเฉิน โดยระบบสำรองต้องอยู่ในสภาพพร้อมใช้ และมีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

4. จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ โดยมีแนวทางที่สอดคล้องกับนโยบายการบริหารความเสี่ยงองค์กร

5. จัดให้มีการตรวจสอบและดำเนินการแก้ไข เมื่อมีเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยเกิดขึ้น พร้อมทั้งดำเนินการป้องกันไม่ให้เกิดซ้ำและให้รายงานและบันทึกไว้อย่างชัดเจน

6. จัดให้ผู้ใช้งานได้รับความรู้เรื่องนโยบาย แนวทางปฏิบัติ มาตรฐาน และระเบียบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยผู้ใช้งานจะต้องยึดถือและปฏิบัติตามอย่างเคร่งครัด

หมวดที่ 1
การกำกับดูแลและบริหารจัดการ IT ระดับองค์กรที่ดี (Governance of Enterprise IT)

การกำกับดูแลเทคโนโลยีสารสนเทศมีจุดมุ่งหมายเพื่อทำให้มั่นใจว่าบริษัทฯ สามารถบรรลุเป้าหมายที่กำหนดไว้โดยนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุนและสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้น จากการนำเทคโนโลยีสารสนเทศมาใช้งานได้อย่างมีประสิทธิภาพ เชื่อทำให้มั่นใจว่าเทคโนโลยีที่บริษัทฯ นำมาใช้งานสามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจ โดยบริษัทฯ ต้องพิจารณาดำเนินการดังต่อไปนี้

1. <u>นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)</u>
    1. บริษัทฯ ต้องกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและสื่อสารผ่านช่องทางของบริษัทฯ เพื่อสร้างความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง
    2. บริษัทฯ ต้องมีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเมื่อมีการเปลี่ยนแปลงใดๆ ที่มีผลกระทบต่อนโยบายต่อบริษัทฯ
2. <u>การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)</u>

    ต้องสอดคล้องกับ นโยบายการบริหารความเสี่ยงองค์กร (Corporate Risk Management) และครอบคลุมในเรื่องดังต่อไปนี้
    1. การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

        ผู้จัดการส่วนเทคโนโลยีมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่ แล้วนำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ
    2. การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk)
        - ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของบริษัท เพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัยหรือไม่ประสงค์ดี เช่น การดาวน์โหลดโปรแกรมจากภายนอกมาติดตั้ง ซึ่งอาจมีมัลแวร์หรือไวรัสคอมพิวเตอร์ หรือมีช่องโหว่เชื่อมต่อเครือข่ายภายนอก เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน เป็นต้น

- ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ของบริษัท ต้องมีตรวจสอบและเฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต โดยมีการจัดทำระบบป้องกันการเข้าถึงและการโจมตีจากภายนอกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงานใช้งาน เช่น ระบบป้องกันการเข้าออกใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ การกรองข้อมูลรับส่งอีเมล เป็นต้น
- ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิ์การใช้งานเข้าถึงระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายต่างๆ และข้อมูล ให้เป็นไปตามสิทธิ์ที่พึงมี เพื่อป้องกันการเข้าแก้ไขหรือเปลี่ยนแปลงข้อมูล

3. การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ 4 ประเภท ดังนี้
   - ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี
   - ความเสี่ยงจากผู้ปฏิบัติงาน ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลเกินกว่าหน้าที่และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้
   - ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้งสถานการณ์อื่น เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น
   - ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากแนวนโยบายที่ทำการใช้งานอยู่อาจไม่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น
4. การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่บริษัทยอมรับได้จัดทำตารางลักษณะรายละเอียดความความเสี่ยง (Description of Risk) โดยมีหัวเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)
5. กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

หมวดที่ 2

การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security)

- **แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของ** IT (Information Security Policy)

วัตถุประสงค์

เพื่อเป็นการป้องกันการกระทำผิดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

1. ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เผยแพร่สิ่งที่ผิดต่อกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
2. ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้
3. ห้ามผู้ใช้งานใช้บัญชีของผู้ใช้งานอื่น โดยไม่ได้รับอนุญาต
4. ห้ามเผยแพร่ข้อมูลของผู้อื่นหรือหน่วยงานใดๆ โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูลนั้นๆ
5. ห้ามก่อกวน ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของกลุ่มบริษัทฯ ซึ่งก่อให้เกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์, การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น
6. ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของกลุ่มบริษัทฯ

- **การจัดโครงสร้างความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ** (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศภายในกลุ่มบริษัทฯ

แนวทางปฏิบัติ

1. ผู้บริหารระดับสูง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทฯ
2. หัวหน้าหน่วยงานเทคโนโลยีสารสนเทศต้องกำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในแผนกเทคโนโลยีสารสนเทศรับผิดชอบการดูแลระบบสารสนเทศที่บริษัทฯ ใช้งานให้มีความมั่นคงปลอดภัยและควบคุมการปฏิบัติงานเพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ

3. เจ้าหน้าที่เทคโนโลยีสารสนเทศ ที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator รับผิดชอบต่อระบบที่ดูแลนั้น จะต้องทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยในการใช้งาน (Security logs review) และมีการบันทึกการตรวจสอบตามช่วงเวลาที่หัวหน้าหน่วยงานเทคโนโลยีสารสนเทศกำหนดหากมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด จะต้องดำเนินการแก้ไขและรายงานต่อผู้บังคับบัญชา
4. ผู้ใช้งานและบุคคลที่เกี่ยวข้องต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัทฯ ในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- **การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)**

วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทฯ

แนวทางปฏิบัติ

1. ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับบุคคลที่เกี่ยวข้องที่ว่าจ้างมาปฏิบัติงาน และจะต้องสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ
2. ต้องให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องที่ว่าจ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ
3. เพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ฝ่ายทรัพยากรบุคคลหรือหน่วยงานที่เกี่ยวข้องต้องแจ้งให้เจ้าหน้าที่เทคโนโลยีสารสนเทศทราบทันทีเมื่อมีเหตุได้แก่
   - การลาออกจากงาน หรือการสิ้นสุดการว่าจ้าง
   - การโยกย้ายหน่วยงาน
4. ต้องให้ผู้ใช้งานและหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
5. หลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงานหรือสิ้นสุดโครงการต้องยกเลิกการเข้าถึงข้อมูลในระบบเทคโนโลยีสารสนเทศทันที
6. ต้องมีการลงนามในสัญญาระหว่างผู้ปฏิบัติงานและหน่วยงาน ว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างผู้ปฏิบัติงานนั้นๆ ทั้งนี้ ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว
7. ผู้ปฏิบัติงานใหม่ของบริษัทต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ

- **การบริหารจัดการสินทรัพย์สารสนเทศ** (Asset Management)
  - **การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์** (Computer and Peripheral Access Control)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และ อุปกรณ์คอมพิวเตอร์ของบริษัท รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัดอันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

1. ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของกลุ่มบริษัทฯ ต้องเป็นผู้รับผิดชอบสินทรัพย์ (Asset) ที่ใช้งาน
2. ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของกลุ่มบริษัทฯ เพื่อประกอบธุรกิจการค้าตลอดจนบริการใดๆ ที่เป็นของส่วนตัวหรือไม่เกี่ยวข้องกับกิจการของกลุ่มบริษัทฯ
3. ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมส่วนประกอบต่างๆของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของเครื่องคอมพิวเตอร์ของกลุ่มบริษัทฯ เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชาและหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศเพื่อให้ผู้ดูแลระบบดำเนินการติดตั้ง แก้ไขเปลี่ยนแปลงโปรแกรม เท่านั้น และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม
4. ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ
5. ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง หรือในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
6. ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน
7. หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
8. ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน
9. การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท
10. ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

- **การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์** (Software License Management)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานคอมพิวเตอร์สิทธิ์ในการใช้งานโปรแกรมคอมพิวเตอร์ตลอดจนเข้าใจการใช้โปรแกรมที่ถูกต้องลิขสิทธิ์และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัดสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

แนวทางปฏิบัติ

ข้อกำหนดสำหรับผู้ดูแลระบบ

1. มีหน้าที่รับผิดชอบในการควบคุมดูแลการใช้งานโปรแกรมคอมพิวเตอร์ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัทตามสิทธิ์การใช้งานที่กำหนด
2. มีหน้าที่รับผิดชอบในการติดตั้งและอัพเกรดโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งานตามวันเวลาที่นัดหมาย
3. ถอดและยกเลิกสิทธิการใช้งานโปรแกรมคอมพิวเตอร์ทันทีเมื่อบริษัทฯและ/หรือหน่วยงาน แจ้งยกเลิกและ/หรือย้ายสิทธิการใช้งาน

ข้อกำหนดสำหรับผู้ใช้งาน

1. ไม่นำโปรแกรมคอมพิวเตอร์ของกลุ่มบริษัทฯ ไปใช้ในทางที่ผิดกฎหมาย ซึ่งอาจก่อให้เกิดความเสียหายกับกลุ่มบริษัทฯ
2. โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของกลุ่มบริษัทฯ เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวเพื่อกระทำการใดๆ ที่ไม่เกี่ยวข้องกับกลุ่มบริษัทฯ
3. ห้ามคัดลอกจำหน่ายเผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาตโดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำผิดกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้อง
4. ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของกลุ่มบริษัทฯอย่างเด็ดขาดกรณีผู้ใช้งานนำโปรแกรคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่กลุ่มบริษัทฯ มีอยู่มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะมี Licensed Software หรือ Freeware ก็ตามหากมีความเสียหายหรือละเมิดเกิดขึ้น ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
5. การติดตั้งใช้งานการยกเลิกการใช้งานการโอนย้ายและการคืนเครื่องคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติและผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ ได้รับอนุมัติในแต่ละขั้นตอน

- **การควบคุมสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการเข้าใช้งานระบบคอมพิวเตอร์**
  (Asset And Information System Control)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการไม่ให้สินทรัพย์และข้อมูลสารสนเทศอยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ์หรืออำนาจหน้าที่เกี่ยวข้อง

แนวทางปฏิบัติ

ข้อกำหนดสำหรับผู้ดูแลระบบ

1. จัดทำและเก็บทะเบียนสินทรัพย์สารสนเทศ เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อสินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์ของกลุ่มบริษัทฯ
2. ตรวจสอบสินทรัพย์ (Inventory check) ทุกประเภทตามระยะเวลาที่กำหนดไว้ทุกๆ 6 เดือน
3. ประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์ เมื่อมีสินทรัพย์ใหม่หรือมีการเปลี่ยนแปลงสินทรัพย์ที่สำคัญเกิดขึ้น

ข้อกำหนดสำหรับผู้ใช้งาน

1. ออกจากระบบสารสนเทศ (Log out) โดยทันทีเมื่อเสร็จสิ้นการใช้งาน
2. มีการป้องกันเครื่องคอมพิวเตอร์โดยใช้การพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน
3. ต้องจัดเก็บและสำรองข้อมูลสารสนเทศที่มีความสำคัญของหน่วยงานไว้ในที่ที่ปลอดภัย การจัดเก็บข้อมูลของผู้ใช้งาน จะจัดเก็บได้อยู่ในรูปแบบในฐานข้อมูลของระบบ Application นั้นๆ ที่จัดเก็บภายใน Data Center ของบริษัท
4. สามารถจัดเก็บใน Shared File (Drive กลาง) ใน Folder ตามสิทธิ์ที่ได้รับ
5. ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อไม่มีการใช้งานนานเกิน 1 ชั่วโมง หรือเมื่อใช้งานประจำวันเสร็จสิ้นงาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง
6. การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากไม่ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 10 นาที
7. ระมัดระวังและดูแลรักษาทรัพย์สินของกลุ่มบริษัทฯ ที่ตนเองใช้งานเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเลินเล่อ ผู้ใช้งานต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

- **การใช้งานจดหมายอิเล็กทรอนิกส์ (Email Control)**

วัตถุประสงค์

เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สามารถสนับสนุนการ ปฏิบัติงานและเป็นไปอย่างถูกต้องสะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ ปลอดภัย ภายใต้ข้อกำหนดของกฎหมายระเบียบ ข้อบังคับและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของกลุ่มบริษัทฯ ตลอดจนเพื่อให้ผู้ใช้งานเข้าใจถึงความสำคัญและตระหนักถึงปัญหา ที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้งาน จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด

แนวทางปฏิบัติ

1. ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (Email Address) ในนามของบริษัทฯ จะต้องไม่ใช้ Email Address ในการกระทำผิดกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้อง
2. หน่วยงานหรือผู้ปฏิบัติงานผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท จะต้องใช้จดหมายอิเล็กทรอนิกส์ เพื่อผลประโยชน์ของบริษัท
3. ผู้ปฏิบัติงานจะได้รับสิทธิ์ในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียนผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อผู้ปฏิบัติงานที่ได้รับแจ้งมาจากฝ่ายทรัพยากรบุคคล
4. ผู้ใช้งานจะต้องไม่ใช้ที่อยู่ Email Address ของผู้อื่นกระทำการใดๆ ไม่ว่าจะเป็นอ่าน, รับ-ส่งข้อความ เว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์นั้น
5. ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น
6. การส่ง Email Address ให้กับบุคคลที่เกี่ยวข้องตามภารกิจของกลุ่มบริษัทฯ ผู้ใช้งานจะต้องใช้ Email Address ของบริษัทฯ เท่านั้น ห้ามใช้ Email Address อื่น เว้นแต่ในกรณีที่ระบบ Email Address ของบริษัทฯ ขัดข้องและต้องได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
7. การใช้งาน Email Address ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่นยั่วยุเสียดสีส่อไปในทางที่ผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคลโดยอ้างเป็นความเห็นของกลุ่มบริษัทฯ หรือก่อให้เกิดความเสียหายต่อกลุ่มบริษัทฯ
8. ห้ามใช้ Email Address ของบริษัทฯ เพื่อเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดซึ่งมีลักษณะขัดต่อ ศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์หรือกระทบต่อการ ดำเนินงานของกลุ่มบริษัทฯ ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งบุคคลที่เกี่ยวข้องของกลุ่มบริษัทฯ

9. ห้ามผู้ใช้งานนำที่อยู่ Email Address ไปใช้ในกิจการงานส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากบริษัทฯ ตรวจพบว่ามีการกระทำดังกล่าวให้ถือว่าเจ้าของ Email Address เป็นผู้รับผิดชอบการกระทำดังกล่าว
10. ห้ามกระทำการใดที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่ (Chain mail) การส่งจดหมายจำนวนมาก (Spam mail) การส่งจดหมายต่อเนื่อง (Letter bomb) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์ เป็นต้น
11. ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของกลุ่มบริษัทฯ เช่น ข้อมูลลูกค้า แผนการดำเนินการ เป็นต้น ให้กับบุคคลภายนอกหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของกลุ่มบริษัทฯ
12. กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย บริษัทฯ ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับการบริการชั่วคราวแก่ผู้ใช้งาน นั้น ๆ เพื่อสอบสวนและตรวจสอบหาสาเหตุทันทีโดยไม่ต้องแจ้งล่วงหน้าหรือขออนุญาตใดๆ
13. หากผู้ใช้งานพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิดกฎหมายเกิดขึ้นในบริษัทฯ ให้แจ้งเบาะแสไปที่ผู้ดูแลระบบของฝ่ายเทคโนโลยีสารสนเทศ
14. การกระทำใดๆ ที่เกี่ยวข้องกับการเผยแพร่ ทั้งในรูปแบบของ Email Address และโฮมเพจของผู้ใช้บริการให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการเท่านั้น ผู้ดูแลระบบและบริษัทฯ ไม่มีส่วน เกี่ยวข้องใดๆ

- **การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ** (Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานระบบอินเทอร์เน็ตผ่านระบบเครือข่ายของบริษัท เพื่อให้เกิดประสิทธิภาพและมีความมั่นคงปลอดภัย และเพื่อให้ผู้ใช้งานมีความตระหนักในการใช้งานเว็บไซต์ต่าง ๆ ผ่านระบบเครือข่ายของบริษัท

แนวทางปฏิบัติ

1. ส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่ายเพื่อการเข้าใช้งานระบบอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy เป็นต้น
2. เครื่องคอมพิวเตอร์ของบริษัท ก่อนทำการเชื่อมต่อระบบเครือข่าย ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการก่อน
3. หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น
4. ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของบริษัท

5. ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของบริษัท ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของบริษัท
6. ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดเพื่อปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
7. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำไปใช้งาน
8. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ลามกอนาจาร เป็นต้น
9. ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่นๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อบริษัท รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่บริษัทกำหนดไว้อย่างเคร่งครัด
10. การควบคุมการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Access Control)
    1) ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงกำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
    2) ต้องกำหนดสิทธิ์การใช้ข้อมูลและระบบสารสนเทศ เช่น สิทธิ์การใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิ์การใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ โดยให้ดำเนินการตามวิธีที่บริษัทกำหนด
    3) ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิ์พิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม ดูหัวข้อการจัดการสิทธิ์ผู้ใช้งานที่มีสิทธิ์พิเศษ (High Privilege User)
11. การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

1). ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบสารสนเทศที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น บริษัทจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

• ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร (Alphabet + Numeric)

• ควรใช้อักขระพิเศษประกอบ เช่น : ; < > $ @ # เป็นต้น

• สำหรับผู้ใช้งานทั่วไป และ ผู้ใช้งานที่มีสิทธิ์พิเศษ เช่น ผู้จัดการระบบ (System Administrator) และผู้ใช้งานที่ติดมากับระบบ (Default User) เป็นต้น ควรเปลี่ยนรหัสผ่านทุก ๆ 90 วัน

• ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน หรือคาดเดาได้ง่าย เช่น “abcdef” “aaaaaa” “123456” “password” “P@ssw0rd” เป็นต้น

• ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น

• ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

• ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด (Logon Attempt -Retires) ซึ่งในทางปฏิบัติโดยทั่วไปให้อยู่ที่ 4 ครั้ง หากการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนดไว้ระบบงานหรือโปรแกรมจะไม่อนุญาตหรือระงับการใช้งาน

• ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น

• ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

• ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ไม่ควรจดใส่กระดาษแล้วติดไว้หน้าเครื่อง ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

• สำหรับกรณีผู้ใช้งานมีการใช้งานร่วมกันลักษณะ Shared Users Licenses เช่นระบบ SAP เป็นต้น ทางผู้ดูแลจะมีการส่งอีเมลแจ้งเตือนผู้รับผิดชอบการใช้งานให้ทำการเปลี่ยนรหัสผ่านในการเข้าระบบงานนั้นเมื่อมีการเปลี่ยนแปลงของผู้ใช้งานในสังกัด

2) ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง

3) ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอตามตารางสิทธิ์และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของผู้ปฏิบัติงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยน รหัสผ่าน เป็นต้น โดยให้มีการกำหนดแนวทางปฏิบัติการเพิ่มหรือแก้ไขสิทธิ์การใช้งานระบบให้ชัดเจน

12. การจัดการสิทธิ์ผู้ใช้งานที่มีสิทธิ์พิเศษ (High Privilege User)

ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิ์พิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิ์พิเศษมีความรัดกุมเพียงพอหรือไม่นั้น บริษัทจะใช้ปัจจัยประกอบการพิจารณาในภาพรวมดังต่อไปนี้

• ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่

- ควรควบคุมการใช้งานของผู้ใช้งานที่มีสิทธิ์พิเศษอย่างเข้มงวด เช่น จำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ควรมีการเปลี่ยน Password อย่างเคร่งครัด เช่น กรณีที่ใช้สิทธิ์ High Privilege แบบใส่ซอง หรือมีการใช้งานไม่ต่อเนื่อง ให้ทำการเปลี่ยน Password ทุกครั้งที่ใช้งานครั้งนั้นเสร็จสิ้น หรือ กรณีผู้ใช้งานที่มีสิทธิ์พิเศษ เช่น ผู้จัดการระบบ (System Administrator) และผู้ใช้งานที่ติดมากับระบบ (Default User) เป็นต้น ควรเปลี่ยนรหัสผ่านทุก ๆ 90 วัน หรือ อ้างอิงตามการควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) ที่บริษัทกำหนด

13. การควบคุมการเข้าใช้งานระบบจากภายนอก (Remote Access Management)
    1) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบจากภายนอก เช่น พนักงาน หรือ Vendor ระบบ ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงาน IT เพื่อขอใช้สิทธิ์ในการเข้าถึงระบบจากภายนอก และต้องได้รับอนุมัติจากผู้บริหารของหน่วยงาน IT หรือ ผู้ที่ได้รับมอบหมายก่อนดำเนินการ ทั้งนี้ การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกผู้ใช้งานระบบทุกคนเมื่อจะเข้าใช้งานระบบของบริษัท ต้องผ่านการพิสูจน์ตัวตน โดยแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) และพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password) ตามที่กำหนด การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน โดยใช้รหัสผ่าน หรือ ใช้วิธีการเข้ารหัส เช่น VPN/ SSL
    2) ผู้ดูแลระบบ มีหน้าที่ดูแลความมั่นคงปลอดภัยจากการเข้าใช้งานระบบจากภายนอก ทั้งนี้ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบและข้อมูลอย่างเคร่งครัด กรณีเมื่อมีความจำเป็น ให้ผู้ดูแลระบบกำหนดให้ผู้ใช้งานดำเนินการบันทึกคลิปการปฏิบัติงานระหว่างใช้งานระบบจากภายนอกเพื่อเป็นหลักฐานสำหรับการตรวจสอบ
    3) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากภายนอก ผู้ดูแลระบบต้องอนุญาตตามพื้นฐานของความจำเป็นเท่านั้น และให้ปิดช่องทางเมื่อผู้ใช้งานได้ใช้งานเสร็จสิ้นแล้วทันที

6. **การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)**

วัตถุประสงค์

เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ หรือแก้ไขเปลี่ยนแปลง ข้อมูลหรือการทำงานของระบบสารสนเทศในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง

แนวทางปฏิบัติ

<u>การบริหารจัดการข้อมูล</u>

1. ต้องมีการจัดลำดับชั้นความลับ ต้องมีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนดวิธีบริหารจัดการกับข้อมูลแต่ละประเภท รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการยกเลิกหรือการนำกลับมาใช้ใหม่
2. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL(Secure Socket Layer) การใช้ VPN (Virtual Private Network) เป็นต้น
3. ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน
4. ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม เป็นต้น หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน
5. ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิ์และหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น
1. ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิ์ผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share Files เป็นต้น จะต้องเป็นการให้สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิ์ดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิ์ดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
2. ในกรณีที่มีความจำเป็นต้องให้สิทธิ์บุคคลอื่น ให้มีสิทธิ์ใช้งานระบบสารสนเทศและระบบเครือข่ายในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

7. **การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ** (Operations Security)

วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับระบบเทคโนโลยีสารสนเทศของบริษัทฯ เป็นไปอย่างถูกต้อง มั่นคง ปลอดภัย และป้องกันการสูญหายของข้อมูล และได้รับการปกป้องจากโปรแกรมไม่ประสงค์ดี

แนวทางปฏิบัติ

1. จัดทำคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับระบบเทคโนโลยีสารสนเทศที่สำคัญของบริษัทฯ เพื่อป้องกันความผิดพลาดในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
2. ต้องมีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ
3. ควรติดตั้งระบบเพื่อตรวจสอบติดตามทรัพยากรของระบบเทคโนโลยีสารสนเทศ เช่น CPU, Memory, Hard Disk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต
4. ระบบที่มีความสำคัญสูง ควรแยกระบบการพัฒนาออกจากระบบการให้บริการจริง เพื่อเป็นการรักษาความปลอดภัยของระบบและป้องกันความผิดพลาดหรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต
5. ต้องสำรวจข้อมูลเพื่อจัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรองและความถี่ในการสำรองข้อมูล
6. ข้อมูลที่มีความสำคัญสูง ต้องจัดให้มีความถี่ การสำรองข้อมูลและควรจัดให้มีการย้ายข้อมูลไปเก็บที่ภายนอกบริษัทฯ
7. ต้องทดสอบสภาพพร้อมใช้งานระบบสำรองของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง
8. ต้องมีมาตรการป้องกันโปรแกรมที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ เช่น การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แบบพกพาส่วนบุคคลจากภายนอกบริษัทฯ ต้องเชื่อมต่อระบบเครือข่ายของบริษัทฯ ผ่านการ VPN
9. ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราเซอร์
10. ผู้ใช้งานต้อง Update ระบบปฏิบัติการและโปรแกรมที่ใช้งาน ที่ได้มีการออก Patch และ/หรือ Hotfix อย่างสม่ำเสมอโดยสามารถดาวน์ โหลดจากเว็บไซต์ของเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่
11. ผู้ใช้งานที่ต้องการจะติดตั้งซอฟต์แวร์ที่อื่นนอกเหนือจากที่บริษัทฯ เตรียมไว้ให้ ต้องแจ้งส่วนฝ่ายเทคโนโลยีสารสนเทศเพื่อตรวจสอบความปลอดภัยและเป็นผู้ดำเนินการติดตั้งให้เท่านั้น

8. **การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์** (Communications Security)

วัตถุประสงค์

เพื่อป้องกันข้อมูลสารสนเทศในเครือข่ายจาก บุคคล, ไวรัส รวมทั้งมัลแวร์ต่าง ๆ มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

1. **การบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย** (Network Security Management)
    1. กำหนดการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย
    2. จัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับบริษัท
2. **การถ่ายโอนข้อมูล** (Agreements on Information Transfer)
    1. ต้องดำเนินการจัดทำข้อตกลงสำหรับการถ่ายโอนข้อมูล (Agreements on Information Transfer) โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
    2. ต้องมีการลงนามในสัญญาระหว่างบริษัทฯ และหน่วยงานภายนอกว่าจะไม่เปิดเผยความลับของกลุ่มบริษัทฯ (Non Disclosure Agreement: NDA)

9. **การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ** (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศและจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศให้ได้รับทราบ

แนวทางปฏิบัติ

1. ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท
2. ต้องกำหนดช่องทางการติดต่อสื่อสารเพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน
3. หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องแจ้งเหตุการณ์ดังกล่าวต่อหน่วยงานเทคโนโลยีสารสนเทศ
4. กำหนดให้เจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศประเมินระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยด่วน

10. **การจัดหา-พัฒนาและดูแลรักษาระบบสารสนเทศ** (System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศมีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

แนวทางปฏิบัติ

1. ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน
2. ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง
3. ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

1. การร้องขอ
   - การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร ตามวิธีที่บริษัทกำหนด และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หรือผู้รับผิดชอบระบบสารสนเทศ เป็นต้น
   - ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง
   - ควรสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางการ
2. การปฏิบัติงานพัฒนาระบบงาน
   - ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้
   - ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้อง ควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ

- ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

3. การทดสอบ
   - ผู้ที่ร้องขอและส่วนเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบเพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง
4. การโอนย้ายระบบงานเพื่อใช้งานจริง
   - ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ
5. การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ Version ของระบบงานที่ได้รับการพัฒนา
   - ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา
   - ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิ์ใช้งาน ขั้นตอนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน
   - ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้
6. การทดสอบหลังการใช้งาน (Post-Implementation Test)
   - ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน
7. การสื่อสารการเปลี่ยนแปลง
   - ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

11. **การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ** (IT Outsourcing)

วัตถุประสงค์

เพื่อเป็นการป้องกันสินทรัพย์ของกลุ่มบริษัทฯ ที่มีการเข้าถึงโดย IT Outsourcing และมีการรักษา ไว้ซึ่งระดับความมั่นคงปลอดภัย และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ

แนวทางปฏิบัติ

1. ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของกลุ่มบริษัทฯ เมื่อมีความ จำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของกลุ่มบริษัทฯ โดยสอดคล้องกับข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูลของกลุ่มบริษัทฯ
2. ต้องสื่อสารและบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของกลุ่มบริษัทฯ เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของกลุ่มบริษัทฯ ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้
3. ในข้อตกลงการให้บริการต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการภายนอกอย่างสม่ำเสมอ
4. หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญ จะต้องทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

12. **การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ** (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อเป็นการป้องกันการหยุดชะงักในการดำเนินงานของบริษัท อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของบริษัท

แนวทางปฏิบัติ

1. ส่วนเทคโนโลยีสารสนเทศ ต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดขึ้นกับระบบสารสนเทศ ตามแผนบริหารภาวะวิกฤต (Crisis Management Plan) ของบริษัท
2. ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้น อย่างน้อย ปีละ 1 ครั้ง
3. ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง
4. ต้องมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรอง อย่างน้อยปีละ 1 ครั้ง

13. การควบคุมข้อมูลส่วนบุคคล (PDPA)

วัตถุประสงค์

1. เพื่อให้ผู้บริหาร เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ตระหนักถึงความสำคัญของความเป็นส่วนตัวของลูกค้า เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ
2. เพื่อกำหนดมาตรฐาน และแนวทางปฏิบัติสำหรับผู้บริหาร เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ให้ปฏิบัติงานโดยสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล
3. เพื่อให้ผู้บริหาร และเจ้าหน้าที่ทุกระดับได้รับทราบและปฏิบัติตามนโยบายฉบับนี้อย่างเคร่งครัด

แนวทางปฏิบัติ

1. บรรดาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัทฯ ถือเป็นทรัพย์สินของบริษัทฯ ผู้บริหาร เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ มีหน้าที่ปกป้อง และรักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับ และจะต้องใช้ข้อมูลส่วนบุคคลดังกล่าวไม่ว่าจะอยู่ในรูปแบบใดก็ตาม ด้วยความระมัดระวัง
2. ผู้บริหารและเจ้าหน้าที่ของบริษัทฯ จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลบนพื้นฐานของความจำเป็นเพื่อการปฏิบัติงานของบริษัทฯ เท่านั้น ในกรณีที่ได้รับข้อมูลส่วนบุคคลที่ไม่จำเป็นหรือไม่เกี่ยวข้องกับการปฏิบัติงาน ให้ผู้บริหารและเจ้าหน้าที่ของบริษัทฯ ดำเนินการให้ข้อมูลส่วนบุคคลนั้นไม่สามารถระบุตัวบุคคลนั้นได้ หรือทำให้ไม่สามารถมองเห็นได้
3. ผู้บริหาร เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ มีหน้าที่ป้องกันและระมัดระวังไม่ให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด
4. ผู้บริหาร เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ มีหน้าที่ต้องดูแลและรับผิดชอบต่อทรัพย์สินของบริษัทฯ ที่ได้รับมอบไว้เพื่อการปฏิบัติงานเสมือนหนึ่งว่าเป็นทรัพย์สินของตนเอง
5. ห้ามไม่ให้ผู้บริหาร เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ทำการคัดลอก ทำสำเนา เปิดเผย เผยแพร่ แก้ไข เปลี่ยนแปลง ทำซ้ำ จำหน่าย โอน หรือทำลายข้อมูลดังกล่าว โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา หากบริษัทฯ ตรวจสอบแล้วพบว่ามีการคัดลอก ทำสำเนา เผยแพร่ แก้ไข เปลี่ยนแปลง ทำซ้ำ โอน หรือทำลายข้อมูลดังกล่าว โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ผู้บริหาร เจ้าหน้าที่ หรือบุคคลภายนอกดังกล่าวจะต้องรับผิดชอบกับบริษัทฯในความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นจากเหตุการณ์นั้น

6. ในกรณีที่มีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้บริหารและเจ้าหน้าที่ของบริษัทฯ ผู้บริหารและเจ้าหน้าที่ของบริษัทฯ ต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และวิธีการอื่นใดที่บริษัทฯ กำหนด เพื่อป้องกันมิให้บุคคลหรือนิติบุคคลอื่นนั้นเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
7. บรรดาข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลอ่อนไหว และข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัทฯ ที่ผู้บริหาร เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯได้ล่วงรู้นั้นก็เพื่อการปฏิบัติงานของบริษัทฯ เท่านั้น ห้ามมิให้นำข้อมูลดังกล่าวไปเปิดเผย หรือใช้เพื่อวัตถุประสงค์อื่นใดที่บริษัทฯ ไม่ได้กำหนดหรืออนุญาต หรือนำข้อมูลดังกล่าวไปเปิดเผย หรือใช้ในลักษณะที่จะก่อให้เกิดความเสียหายต่อบริษัทฯ
8. บรรดากฎหมายที่ใช้บังคับอยู่และที่จะได้ประกาศใช้ ตลอดจนนโยบาย กฎระเบียบ และข้อบังคับต่าง ๆ ของบริษัทฯ ถือเป็นสิ่งสำคัญที่ผู้บริหาร เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ต้องให้ความสำคัญและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดหรือฝ่าฝืนกฎหมาย นโยบาย กฎระเบียบ และข้อบังคับดังกล่าว

ทั้งนี้ ให้มีผลใช้ตั้งแต่วันที่ 20 ธันวาคม 2566

(นายภูมิพัฒน์ สินาเจริญ)
ประธานเจ้าหน้าที่บริหาร

เสนอโดย_____(นายกรวรา สายอินทร์) VP of Business Process Improvement and Information Technology

หน่วยงานเทคโนโลยีสารสนเทศ

หมายเหตุ แจ้งกรรมการ ผู้บริหารและพนักงานผ่านระบบจดหมายอิเล็กทรอนิกส์