นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(IT Security Policy)

บริษัท ลีซ อิท จำกัด (มหาชน)

ปี 2567

สารบัญ

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

IT SECURITY POLICY

บริษัท ลีซ อิท จำกัด (มหาชน)

บริษัท ลีซ อิท จำกัด(มหาชน) เป็นบริษัทหนึ่งที่ได้นำเอาเทคโนโลยีสารสนเทศเข้ามาสนับสนุนเพื่อเพิ่มประสิทธิภาพในการดำเนินงาน แต่เมื่อระบบสารสนเทศไม่สามารถให้บริการได้ หรือมีความผิดพลาดในการให้บริการไม่ว่าด้วยสาเหตุใดก็ตาม อาจส่งผลให้การดำเนินงานด้านระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของบริษัทไม่สามารถทำงานได้อย่างต่อเนื่อง และไม่มีความปลอดภัย ซึ่งอาจทำให้ส่งผลกระทบต่อชื่อเสียงหรือความน่าเชื่อถือได้ ผู้ใช้งานทุกคนต้องร่วมมือกันป้องกันไม่ให้เกิดความเสียหายหรือลดโอกาสที่จะเกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ ดังนั้นบริษัทจึงเห็นควรกำหนดนโยบายสารสนเทศว่าด้วยการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขึ้น เพื่อให้ บริษัท ลีซ อิท จำกัด(มหาชน) และบริษัทย่อย ที่ใช้ระบบสารสนเทศร่วมกันเป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย และสามารถสนับสนุนกระบวนการทำงานได้อย่างต่อเนื่องและสอดคล้องกับข้อกำหนดของกฎหมายที่เกี่ยวข้อง

หมวด 1 ความหมายและคำจำกัดความ

"**สินทรัพย์คอมพิวเตอร์**" หมายความว่า สินทรัพย์ทุกอย่างที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เป็นต้น

"**ระบบเครือข่าย**" หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ของบริษัท

"**คอมพิวเตอร์แม่ข่าย**" หมายความว่า เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟต์แวร์สำหรับให้บริการแก่เครื่องคอมพิวเตอร์ อื่น ๆ หรือควบคุมการทำงานในเครือข่าย

"**การเข้าถึงเครือข่ายจากระยะไกล**" หมายความว่า การที่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์หรือเครือข่ายอื่นผ่านอุปกรณ์สื่อสารหรือสื่อสัญญาณอื่น ๆ

"**การควบคุมการเข้าถึง**" หมายความว่า การควบคุมการเข้าถึง หรือใช้งานสินทรัพย์คอมพิวเตอร์ให้เป็นไปตามสิทธิที่กำหนดไว้เท่านั้น

"**เครื่องคอมพิวเตอร์**" หมายความว่า อุปกรณ์ที่ใช้ในการประมวลผลข้อมูลที่ทำงาน ด้วยระบบอิเล็กทรอนิกส์ โดยทำงานตามคำสั่งผ่านทางซอฟต์แวร์ให้ได้ผลตามที่ต้องการ อาทิ คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal computer) และคอมพิวเตอร์แบบพกพาได้ (Notebook Computer)

"**อุปกรณ์คอมพิวเตอร์**" หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์ เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ และให้รวมถึงเครื่องคอมพิวเตอร์

"**สื่อสัญญาณ**" หมายความว่า สื่อกลางใด ๆ ที่ใช้เชื่อมต่อระหว่างอุปกรณ์คอมพิวเตอร์ อาทิ สายทองแดง สายใยแก้วนำแสง เครือข่ายไร้สาย

"**ฮาร์ดแวร์**" หมายความว่า อุปกรณ์คอมพิวเตอร์

"**ซอฟต์แวร์**" หมายความว่า ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงานตามต้องการ

"**ซอฟต์แวร์ระบบ**" หมายความว่า ซอฟต์แวร์ที่ควบคุมการทำงานของอุปกรณ์คอมพิวเตอร์ เช่น ระบบปฏิบัติการ เป็นต้น

"**ระบบเทคโนโลยีสารสนเทศ**" หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการการพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ อาทิ อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ระบบงาน และสารสนเทศ

"**สารสนเทศ**" หมายความว่า ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้

"**ระบบงาน**" หมายความว่า การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบจัดเก็บเอกสาร ระบบบัญชี

"**ระบบปฏิบัติการ**" (Operating System) หมายความว่า ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุมการทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) และอุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์)

"**ระบบป้องกันการบุกรุก**" (Firewall) หมายความว่า ระบบรักษาความปลอดภัยที่ประกอบด้วยกลุ่มอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ ซึ่งทำหน้าที่ป้องกันผู้ไม่ได้รับอนุญาตจากเครือข่ายภายนอกเข้าใช้ระบบ และจำกัดการใช้งานของผู้ใช้งานภายในให้เป็นไปตามนโยบายที่บริษัทกำหนด

"**ข้อมูล**" หมายความว่า ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลได้ด้วยวิธีการทางอิเล็กทรอนิกส์บนอุปกรณ์คอมพิวเตอร์ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

"**ไฟล์**" (File) หมายความว่า ข้อมูลที่ถูกรวบรวมลงสื่อบันทึก และระบุเป็นหนึ่งหน่วยโดยมี ชื่อเฉพาะ เช่น ซอฟต์แวร์ใช้งาน และไฟล์เอกสารต่าง ๆ ที่สร้างขึ้นและใส่ชื่อให้แก่ไฟล์นั้นแล้วเก็บบันทึกลงสื่อบันทึก เป็นต้น

"**ผู้ใช้งาน**" (User) หมายความว่า เจ้าหน้าที่ หรือบุคคลภายนอกที่มีสิทธิใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

"**ผู้บริหารเครือข่าย**" (Network Administrator) หมายความว่า บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาเครือข่าย

"**ผู้บริหารคอมพิวเตอร์แม่ข่าย**" (Host/Server Administrator) หมายความว่า บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาคอมพิวเตอร์แม่ข่าย

"**ผู้บริหารระบบป้องกันการบุกรุก**" (Firewall Administrator) หมายความว่า บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษาระบบป้องกันการบุกรุก

"**บัญชีผู้ใช้งาน**" (User Account) หมายความว่า บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งาน ระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบเทคโนโลยีสารสนเทศ

"**บัญชีผู้บริหารคอมพิวเตอร์แม่ข่าย**" (Administrator Account) หมายความว่า บัญชีที่ผู้บริหารคอมพิวเตอร์แม่ข่ายใช้ในการบริหารระบบคอมพิวเตอร์แม่ข่าย

"**เอกสารโครงแบบ**" (Configuration Document) หมายความว่า เอกสารที่แสดงรายละเอียดการกำหนดค่า ต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศใช้งานได้ตามความต้องการ

"**ความเสี่ยง**" หมายความว่า โอกาสของสินทรัพย์คอมพิวเตอร์ในการถูกละเมิดการรักษาความปลอดภัย

"**เหตุการณ์ผิดปกติ**" (Incident) หมายความว่า เหตุการณ์ใด ๆ ที่มีผลกระทบต่อการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

"**เจ้าหน้าที่**" หมายความว่า พนักงานในบริษัท

"**ส่วนงาน**" หมายความว่า ฝ่าย ตามโครงสร้างของบริษัท

"**ส่วนงานเจ้าของข้อมูล**" หมายความว่า เจ้าหน้าที่ในส่วนงานตั้งแต่ 1 คนขึ้นไปที่ได้รับมอบหมายจากส่วนงานให้เป็นผู้รับผิดชอบข้อมูล

"**โปรแกรมประสงค์ร้าย**" หมายความว่า ฮาร์ดแวร์หรือซอฟต์แวร์ที่มีการตั้งใจใส่เข้าไปในระบบโดยไม่ได้รับอนุญาต เพื่อให้ทำงานตามความประสงค์ของผู้ประสงค์ร้าย ซึ่งมีผลให้คอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศ หรือชุดคำสั่งอื่นได้รับความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

"**หน่วยงานภายนอก**" หมายความว่า องค์กรซึ่งบริษัท อนุญาตให้มีสิทธิใน การเข้าถึง หรือใช้ข้อมูลหรือใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท โดยจะได้รับสิทธิ ตามประเภทการใช้งานและต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทโดยไม่ได้รับอนุญาต

หมวด 2 การกำหนดหน้าที่ความรับผิดชอบ และวิธีการปฏิบัติงาน เพื่อการกำกับดูแลและบริหารจัดการ IT ระดับองค์กรที่ดี

(Operation Procedures and Responsibilities for Good Governance of Enterprise IT)

เพื่อให้มั่นใจว่าบริษัทสามารถใช้เทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานและสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้งานได้อย่างมีประสิทธิภาพ เพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมายองค์กร มีการติดตาม รายงานผลการดำเนินงานซึ่งต้องกำหนดนโยบาย คู่มือ ขั้นตอน และวิธีการปฏิยัติงานของฝ่ายเทคโนโลยีสารสนเทศ ตลอดการจัดการ การเปลี่ยนแปลงเพื่อประเมินจัดการกับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น

คู่มือและขั้นตอนการปฏิบัติงาน

1. ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำคู่มือและ/หรือขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืนขั้นตอนการบำรุงรักษา และดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติ และเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ
2. คู่มือและขั้นตอนการปฏิบัติงานต้องได้รับการปรับปรุง เมื่อมีการปรับเปลี่ยนขั้นตอน หรือมีการเปลี่ยนแปลงผู้รับผิดชอบในโครงการปฏิบัติงานนั้น ๆ ดังนั้น คู่มือและขั้นตอนการปฏิบัติงานทุกฉบับต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง
3. ฝ่ายเทคโนโลยีสารสนเทศมีการกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีการปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

การจัดการการเปลี่ยนแปลง

1. ฝ่ายเทคโนโลยีสารสนเทศต้องมีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ ทุกครั้งโดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการจัดการการเปลี่ยนแปลง
2. เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวข้องกับสารสนเทศ เช่น ระบบปรับอากาศ น้ำ ไฟฟ้า สัญญาณเตือนภัย อุปกรณ์ตรวจจับ ฯลฯ เจ้าหน้าที่ต้องประสานงาน หรือรายงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง
3. เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวข้องกับระบบสารสนเทศ ต้องมีเอกสารเป็นทางการในการร้องขอการเปลี่ยนแปลงทุกครั้ง
4. ตาราง และ/หรือแผนการเปลี่ยนแปลงทุกครั้งต้องได้รับความเห็นจากหัวหน้าหน่วยงานที่เกี่ยวข้อง ก่อนจะทำการเปลี่ยนแปลง
5. บันทึกการเปลี่ยนแปลงทุกครั้งจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบ โดยบันทึกต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
   - วันที่รับเรื่อง และวันที่ทำการเปลี่ยนแปลง
   - เจ้าของข้อมูล และผู้ดูแลระบบ
   - วิธีการเปลี่ยนแปลง
   - ผลของการเปลี่ยนแปลง (สำเร็จหรือ ล้มเหลว)

การแบ่งหน้าที่ความรับผิดชอบ

ฝ่ายเทคโนโลยีสารสนเทศต้องมีการกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศให้เกิดความชัดเจน เพื่อหลีกเลี่ยงการใช้งานสินทรัพย์ผิดวัตถุประสงค์ หรือโดยไม่มีสิทธิ์

การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนาและทดสอบ

1. ฝ่ายเทคโนโลยีสารสนเทศต้องมีการแยกเครื่องมือในประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนา และทดสอบ อาทิ การพัฒนาซอฟต์แวร์ควรมีการแยกเครื่องกับระบบที่ใช้งานจริง หากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบที่ใช้งานจริง
2. การกำหนดให้มีการจัดคำร้องขอในการนำการเปลี่ยนแปลงไปติดตั้งและนำไปใช้อย่างเป็นลายลักษณ์และต้องกระทำโดยเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น และคำร้องขอในการนำการเปลี่ยนแปลงไปติดตั้งและนำไปใช้ต้องได้รับการอนุมัติจากผู้บริหารของหน่วยงานที่รับผิดชอบในการติดตั้งและนำไปใช้
3. การนำการเปลี่ยนแปลงไปติดตั้งและนำไปใช้ควรกระทำผ่านระบบการควบคุมการเปลี่ยนแปลงโดยผู้ดูแลสารสนเทศที่ได้รับอนุญาตเท่านั้น เช่น เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ (Operator) เป็นต้น ซึ่งระบบดังกล่าวต้องสามารถรองรับการจัดเก็บสำเนาสารสนเทศหรือโปรแกรมก่อนและหลังการเปลี่ยนแปลงได้

หมวด 3 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร

(Organization of Information Security)

โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร (Internal Organization)

จุดประสงค์เพื่อบริหาร และการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของบริษัท

ผู้บริหารระดับสูง เป็นผู้กำหนดให้มีตัวแทนหรือคณะทำงานจากหน่วยงานต่าง ๆ ภายในบริษัท เพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ของบริษัทโดยที่ตัวแทนหรือคณะทำงานเหล่านั้น จะต้องมีการกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานทางด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่าย คอมพิวเตอร์ขององค์กรอย่างชัดเจน

ตัวแทนหรือคณะทำงานซึ่งถูกแต่งตั้งโดยผู้บริหารระดับสูง ได้แก่ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศหรือคณะอื่นๆที่ได้รับการแต่งตั้ง เป็นผู้รับผิดชอบในการบริหารจัดการและควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่าย คอมพิวเตอร์ขององค์กร ตลอดจนทบทวนนโยบายระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ จัดทำขั้นตอนและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ต่าง ๆ และเอกสารที่เกี่ยวข้องในการจัดทำการรักษาความมั่นคงปลอดภัยของระบบ เทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ รวมถึงควบคุมการปฏิบัติงานของผู้ใต้บังคับบัญชาให้สอดคล้องกับคู่มือ นโยบาย และแนวทางปฏิบัติของบริษัท

ผู้ปฏิบัติงานส่วนเทคโนโลยีสารสนเทศที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบจะต้องทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยและเมื่อมีสัญญาณเตือนภัยเหตุการณ์ไม่พึงประสงค์จะต้องดำเนินการแก้ไขและรายงานผู้บังคับบัญชา และต้องไม่เปิดเผยความลับของบริษัท เว้นแต่จะได้รับการอนุญาตให้เปิดเผยจากบริษัท ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์โดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อบริษัท ผู้ใช้งาน และหน่วยงาน ทั้งภายในและภายนอก ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวทางปฏิบัติของบริษัท ไม่เปิดเผยข้อมูลความลับและไม่ละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำผิดเกี่ยวกับคอมพิวเตอร์

โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้า หรือหน่วยงานภายนอก (External Parties)

จุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัทที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

ฝ่ายเทคโนโลยีสารสนเทศต้องประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

โดยต้องระบุ และบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัทเมื่อมีความจำเป็นต้องให้บุคคลภายนอก หรือผู้ใช้บริการเข้าถึงสารสนเทศ หรือทรัพย์สินสารสนเทศของบริษัทก่อนที่จะอนุญาตให้สามารถเข้าถึงได้ต้องระบุ และจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างบริษัท และหน่วยงานภายนอก เมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศของบริษัทก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

หมวด 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

(Human Resources Security)

การสร้างความความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากรก่อนการทำงาน (Prior to Employment)

จุดประสงค์เพื่อกำหนด และคัดสรรบุคคลก่อนที่จะเข้ามาทำงาน เพื่อลดความเสี่ยงจากความผิดพลาด การขโมย การปลอมแปลง และการนำไปใช้ในทางที่ไม่เหมาะสมของเจ้าหน้าที่อันเกิดจากการปฏิบัติงานกับระบบสารสนเทศ และทรัพยากรสารสนเทศอื่น ๆ ของบริษัท

หน่วยงานภายนอกที่ได้รับการว่าจ้างตามสัญญาการจ้างงานต้องปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยของบริษัทอย่างเคร่งครัดต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นผู้บริหาร พนักงานชั่วคราวหรือนักศึกษาฝึกงาน โดยต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของ

หน่วยงานใดมาก่อน และต้องมีการลงนามสัญญาระหว่างผู้ปฏิบัติงาน และหน่วยงาน ว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement : NDA)

การสร้างความความมั่นคงปลอดภัยขณะเป็นพนักงาน (During Employment)

จุดประสงค์เพื่อให้เจ้าหน้าที่ได้ตระหนักถึงภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้แก่พนักงานเพื่อให้สามารถป้องกันภัยดังกล่าวได้

เจ้าหน้าที่หรือผู้ใช้งานมีหน้าที่ศึกษาทำความเข้าใจวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่บริษัทกำหนด เพื่อนำไปปฏิบัติในการรักษาความปลอดภัย สินทรัพย์ คอมพิวเตอร์ในส่วนที่ตนใช้งานหรือดูแลรับผิดชอบ

ฝ่ายเทคโนโลยีสารสนเทศต้องสื่อสารให้ความรู้แก่เจ้าหน้าที่และลูกจ้าง เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยฯ และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศของบริษัทด้วย

เจ้าหน้าที่และลูกจ้างใหม่ทุกคนต้องทราบถึงนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานก่อนหรือ อย่างน้อย 30 วันนับจากเข้าทำงานในหน่วยงาน

ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติของบริษัท แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุในแต่ละข้อกฎหมายนั้น ๆ

การยกเลิกการจ้างงาน (Termination of Change of Employment)

จุดประสงค์เพื่อให้มีการยกเลิกสิทธิ์กับเจ้าหน้าที่ที่ถูกยกเลิกการจ้างงานหรือหมดสัญญาฯ เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้การบริหารจัดการ Login หรือ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด หน่วยงานด้านทรัพยากรบุคคลต้องแจ้งให้หน่วยงานเทคโนโลยีสารสนเทศทราบทันทีเมื่อมีเหตุดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร เจ้าหน้าที่ และลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

เจ้าหน้าที่และลูกจ้างซึ่งพ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับ ระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวพนักงาน และบัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน

หลังจากมีการยกเลิกหรือเปลี่ยนแปลงตำแหน่งการเป็นพนักงาน และลูกจ้างแล้วจะต้องแจ้ง ยกเลิกการเข้าถึงข้อมูลต่าง ๆ ของหน่วยงานและจะแจ้งต่อเจ้าหน้าที่ ที่เกี่ยวข้องให้รับทราบตามเหมาะสม

หมวด 5 การบริหารจัดการด้านการสื่อสาร และดำเนินงานของระบบ และเครือข่ายสารสนเทศของบริษัท *(Communication and Operations Management)*

การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน (Operational Procedures and Responsibilities)

จุดประสงค์เพื่อให้การใช้ปฏิบัติงาน และการบริหารจัดการโครงสร้างพื้นฐานด้านสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย ให้หน่วยงานเทคโนโลยีสารสนเทศจัดทำคู่มือ และ/หรือขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติและเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบให้หน่วยงานเทคโนโลยีสารสนเทศมีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ ทุกครั้ง

ให้หน่วยงานเทคโนโลยีสารสนเทศ และการสื่อสารบันทึกการเปลี่ยนแปลงทุกครั้ง โดยจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบรายละเอียดของการเปลี่ยนแปลง ให้หน่วยงานเทคโนโลยีสารสนเทศกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศ และเครือข่ายให้เกิดความชัดเจน เพื่อหลีกเลี่ยงการใช้งานสินทรัพย์ผิดวัตถุประสงค์หรือโดยไม่มีสิทธิ์

การจัดการผู้ให้บริการภายนอก (Third Party Service Delivery Management)

จุดประสงค์เพื่อให้มี และคงไว้ซึ่งระดับการรักษาความปลอดภัยสารสนเทศ และระดับการให้บริการที่เหมาะสมและสอดคล้องกับข้อตกลงการบริการกับหน่วยงานภายนอก ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการด้านเทคโนโลยีสารสนเทศของหน่วยงานภายนอกโดยต้องประกอบไปด้วยรายละเอียดดังนี้

- การยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท
- ขอบเขต รายละเอียด และระดับการให้บริการ (Service Level Agreement-SLA)
- เอกสารต่าง ๆ เกี่ยวกับมาตรการการควบคุมที่ใช้ทั้งด้านกายภาพและด้าน Logical
- เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคงปลอดภัยสารสนเทศได้ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
- ข้อตกลงการเชื่อมโยงระบบเครือข่ายของหน่วยงานภายนอก
- ข้อมูลที่หน่วยงานภายนอกสามารถเข้าถึงได้และขั้นตอน และวิธีการร้องขอข้อมูลของบริษัทกรณีต้องการข้อมูลเพิ่มเติม
- สัญญาในการไม่เปิดเผยข้อมูลของบริษัท (Non – Disclosure Agreement : NDA)

- ข้อกำหนดทางด้านกฎหมาย เช่น ความลับส่วนบุคคล (Privacy) และการป้องกันข้อมูล

นโยบายการสำรองข้อมูล (Backup Policy)

จุดประสงค์เพื่อเป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ อาทิ ภัยธรรมชาติ ระบบเสียหาย ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดความถี่ในการทำการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูล และการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือระบบโดยปฏิบัติตามเอกสาร คู่มือ การจัดการการสำรองข้อมูลสารสนเทศฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพสามารถใช้งานได้ตลอดเวลา

ฝ่ายเทคโนโลยีสารสนเทศต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดระยะเวลาในการสำรองข้อมูลตามระดับการบริหารความเสี่ยง

ฝ่ายเทคโนโลยีสารสนเทศต้องมีกระบวนการสำรองข้อมูล และการกู้ข้อมูลของทุกระบบ อย่างน้อยปีละ 1 ครั้ง

การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

จุดประสงค์เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของบริษัท

ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

ฝ่ายเทคโนโลยีสารสนเทศต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญ และแจ้งให้หน่วยงานอื่นๆ ที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย

บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสม และต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของบริษัทด้วย

ระบบเครือข่ายทั้งหมดของบริษัทที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Package Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัส

ฝ่ายเทคโนโลยีสารสนเทศต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของบริษัท และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของบริษัททั้งทางด้านกายภาพและทางด้าน Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายบริษัท

ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัทโดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่าง Router, Switch, Hub และ Wireless Access Point โดยไม่ได้รับอนุญาตเด็ดขาด

ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของบริษัททำการเชื่อมต่อออกไปยังเครือข่ายภายนอกผ่านอุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในบริษัทโดยเด็ดขาด

การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

จุดประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

ให้ฝ่ายเทคโนโลยีสารสนเทศทำการบันทึกกิจกรรม (Audit Logging) การใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ

ให้ฝ่ายเทคโนโลยีสารสนเทศตรวจสอบการใช้งานสินทรัพย์สารสนเทศอย่างสม่ำเสมอ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

ให้ฝ่ายเทคโนโลยีสารสนเทศกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรม หรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

ให้ฝ่ายเทคโนโลยีสารสนเทศบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and Operator Logs)

ให้ฝ่ายเทคโนโลยีสารสนเทศบันทึกเหตุการณ์ข้อผิดพลาด (Fault Logging) ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศวิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร

ให้ฝ่ายเทคโนโลยีสารสนเทศตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในหน่วยงานให้ตรงกัน (Clock Synchronization) โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ของบริษัทถูกบุกรุก

หมวด 6 การควบคุมการเข้าถึง

(Access Control)

การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

จุดประสงค์เพื่อควบคุมการเข้าถึงข้อมูล และระบบสารสนเทศให้มีความมั่นคงปลอดภัย ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำนโยบาย และความต้องการในการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงให้ทำได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งาน และหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้

ฝ่ายเทคโนโลยีสารสนเทศต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท และเฝ้าระวังการละเมิดความปลอดภัยที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

จุดประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ใช้งานใหม่ เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในบริษัท เป็นต้น โดยปฏิบัติตามคู่มือการเข้าถึงระบบสารสนเทศของบริษัท โดยผู้ใช้งานต้องได้รับการทบทวน และพิจารณา อนุมัติตามขั้นตอนของบริษัทอย่างเคร่งครัด

ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์ แยกตามหน้าที่ที่รับผิดชอบด้วย

ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัยอยู่เสมอ

ฝ่ายเทคโนโลยีสารสนเทศต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศ ตามระยะเวลาที่กำหนดไว้ (เช่น อย่างน้อย 1 ครั้งในรอบ 1 ปี เป็นต้น)

ให้มีการจัดเก็บบันทึกข้อมูลการเข้าถึงและการใช้งานระบบสารสนเทศแต่ละระบบ (Log Files) เป็นระยะเวลาอย่างน้อย 1 ปี

การรับผิดชอบหน้าที่ของผู้ใช้งาน (User Responsibilities)

จุดประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์สามารถเข้าถึงระบบสารสนเทศได้

ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ใน เอกสาร 'การควบคุมการเข้าถึงสารสนเทศของบริษัทและการจัดการควบคุมการใช้รหัสผ่าน'

เจ้าหน้าที่ต้องปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศบริษัท การกำหนด การเปลี่ยนแปลง และการยกเลิกรหัสผ่าน และการจัดการควบคุมการใช้รหัสผ่าน

กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

- ควรได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาและผู้ดูแลระบบงานนั้น ๆ

- ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

- ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแลรักษา User Name และรหัสผ่านของตนเอง รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้ให้มีความมั่นคงปลอดภัยอย่างสม่ำเสมอ

รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้ในมาตรฐานการใช้รหัสผ่าน 90 วัน (Password Standard 90 Day)

รหัสผ่านต้องมีความมั่นคงปลอดภัยตามที่ได้กำหนดไว้ มาตรฐานการใช้รหัสผ่าน (Password Policy) ประกอบด้วย

- Minimum Password Length ตัวอักษร , ตัวเลข และควรมีอักขระพิเศษ รวมกันขั้นต่ำจำนวน 8 หลัก
- Maximum Password age รหัสผ่านมีอายุการใช้งานสูงสุด 90วัน
- Minimum Password age รหัสผ่านอายุการใช้งานขั้นต่ำ 1 วัน
- Enforce Password History บังคับรหัสผ่านไม่ให้ซ้ำกับที่เคยใช้มาก่อนหน้า ต้องเปลี่ยน Password อย่างน้อย 4 ครั้ง จึงสามารถกลับมาใช้งาน Password เดิมได้อีกครั้ง
- Account Lockout Duration กำหนดช่วงเวลาในการบล็อกบัญชีผู้ใช้ที่มีการเดารหัสผิดพลาดเกินจำนวนครั้งที่ได้ตั้งไว้
- Account Lockout Threshold กำหนดจำนวนครั้งสูงสุดในการเดารหัสผ่าน 5 ครั้ง
- Reset Account Lockout Counter กำหนดช่วงเวลาก่อนที่วินโดว์จะทำการรีเซตจำนวนครั้งในการเดารหัสที่ผิดพลาดเป็นระยะเวลา 60 นาที หรือติดต่อฝ่ายสารสนเทศเพื่อทำการปลดล็อก

รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย ห้ามใช้ Account ร่วมกันหรือให้ผู้อื่นเข้าใช้งาน Account ของตนโดยเด็ดขาด ทั้งนี้รวมถึงสมาชิกในครอบครัวเมื่อผู้ใช้งานนำงานกลับไปทำที่บ้านด้วย

ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่าน User ID และรหัสผ่านของตนทั้งหมด หากผู้ใช้งานสงสัยว่า User ID หรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อฝ่ายเทคโนโลยีสารสนเทศและทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที

การ Reset Password ต้องผ่านกระบวนการมาตรฐานของบริษัทเท่านั้น เพื่อให้มั่นใจว่าตรงกับ User ที่ต้องการ Reset รหัสผ่านจริง อีกทั้งเจ้าหน้าที่ ที่ดูแลระบบมีสิทธิ์ในการขอข้อมูลและพิสูจน์ตัวตนของผู้ใช้งานตามความเหมาะสม

ในทางกลับกันผู้ใช้งานอาจได้รับการร้องขอจากฝ่ายเทคโนโลยีสารสนเทศให้ทำการเปลี่ยนรหัสผ่านใหม่ ในกรณีที่รหัสผ่านของผู้ใช้งานไม่มีความมั่นคงปลอดภัย สามารถถูกคาดเดา หรือถูกล่วงละเมิดได้ง่าย ทั้งนี้ผู้ใช้งานต้องตรวจสอบความถูกต้องของแหล่งที่มาของคำร้องขอดังกล่าวด้วย เพื่อให้มั่นใจว่าการร้องขอนั้นไม่ได้เป็นการหลอกลวงต้องกำหนดการป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์สานักงานที่ไม่มีผู้ดูแล เจ้าหน้าที่ต้องกำหนดการควบคุมเอกสารข้อมูล หรือสื่อต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

จุดประสงค์เพื่อควบคุมการใช้บริการบนเครือข่ายของบริษัท

ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำแนวทาง/นโยบายควบคุมการเข้าถึงเครือข่าย และบริการบนเครือข่ายโดยเฉพาะเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต ในส่วนนี้ ฝ่ายสารสนเทศ อ้างอิงแนวทางการขอเข้าถึงเครือข่ายตาม SVOA GROUP เนื่องจากเป็นการควบคุมจากส่วนกลาง (Internal / External Network Access)

การควบคุมการใช้งานระบบปฏิบัติการ (Operating System Access Control)

จุดประสงค์เพื่อป้องกันการใช้งานระบบปฏิบัติการโดยไม่ได้รับอนุญาต

ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการจะปฏิเสธการใช้งานหากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 5 ครั้ง เป็นต้น

ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานระบบเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

การควบคุมการใช้งานระบบสารสนเทศและสารสนเทศ (Application and Information Access Control)

จุดประสงค์เพื่อป้องกันการใช้งานระบบสารสนเทศและสารสนเทศโดยไม่ได้รับอนุญาต

ฝ่ายเทคโนโลยีสารสนเทศต้องมีการควบคุมการใช้งานสารสนเทศใน ระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน อาทิ เขียน อ่าน ลบ ได้ กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

บุคคลภายนอกต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ของบริษัทอย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท

การควบคุมการเข้าถึงข้อมูลสารสนเทศ (Information Technology Access Control)

จุดประสงค์เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

สิทธิ์การเข้าถึงไฟล์ข้อมูลสารสนเทศต้องได้รับการควบคุม และได้รับการพิจารณาอนุมัติเท่าที่จำเป็นเท่านั้น เพื่อให้ไฟล์ข้อมูลสารสนเทศได้รับการรักษาความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ รวมทั้งเป็นการแบ่งแยกสิทธิ์ และหน้าที่ของผู้ใช้งาน

คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถานที่ (Mobile Computing)

จุดประสงค์เพื่อควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทเคลื่อนที่ได้ รวมทั้งการปฏิบัติงานนอกสำนักงานให้เป็นไปอย่างปลอดภัย

ต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Notebook, Laptop) และอุปกรณ์สื่อสารอื่น ๆ อาทิ เมื่อปฏิบัติงานอยู่นอกสถานที่

- ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง
- ต้องใส่รหัสผ่านป้องกันข้อมูลที่สำคัญ

ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and Environmental Security)

1. **บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย** (Secure Areas)
   1.1 หน่วยงานจะต้องมีการจำแนก และกำหนดพื้นที่ในการใช้งานระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม และรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ เมื่อมีการกำหนดพื้นที่แล้วให้มีการควบคุมการเข้าออก
   1.2 หน่วยงานจะต้องกำหนดจำแนกและแบ่งบริเวณ "พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspaces)" รวมทั้งจัดทำแผนผังแสดงตำแหน่ง และชนิดของพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ และประกาศให้ทราบทั่วกัน (หน่วยงานควรระบุให้ชัดเจนว่ามีพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศประเภทใดบ้าง และมีพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศใดที่อาจจำแนกได้มากกว่า 1 ประเภท)

1.3 หน่วยงานต้องกำหนดการติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศใน "พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ" ให้สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

2. **การควบคุมการเข้าออก** (Physical Entry Controls)

หน่วยงานที่เกี่ยวข้องกับการบริหารจัดการอาคารและสถานที่ต้องจัดให้มีการควบคุมการเข้าออกในบริเวณ "พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ" โดยให้ผ่านเข้าออกได้เฉพาะ "เจ้าหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศ" ที่มีสิทธิ์เท่านั้น และมีแนวทางปฏิบัติ ดังนี้

2.1 ต้องกำหนด "เจ้าหน้าที่เทคโนโลยีสารสนเทศ" ที่มีสิทธิ์ผ่านเข้าออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ "พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ" อย่างชัดเจน

2.2. "เจ้าหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศ" จะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

2.3 หากมีบุคคลอื่นใดที่ไม่ใช่ "เจ้าหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศ" ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผล และความจำเป็นก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ต้องมีการบันทึกข้อมูลการเข้าออกห้องคอมพิวเตอร์แม่ข่าย (Data Center) ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี

หมวด 7 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

(Information System Acquisition, Development and Maintenance)

การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

จุดประสงค์เพื่อการสร้างความปลอดภัยให้กับระบบสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งาน

ฝ่ายเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้

- มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย อาทิ การสำรองข้อมูล ระบบเครือข่ายสำรอง

- มาตรการปฏิบัติหลังจากเกิดความเสียหาย อาทิ แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล

การประมวลผลระบบสารสนเทศ (Correct Processing in Applications)

จุดประสงค์เพื่อป้องกันความผิดพลาดของระบบสารสนเทศ จากความถูกต้องของข้อมูล การสูญหาย และการแก้ไขอย่างไม่ถูกต้อง

ผู้พัฒนาระบบสารสนเทศต้องตรวจสอบข้อมูลนำเข้าระบบสารสนเทศ ได้แก่ ตรวจสอบช่วงของค่าตัวเลขที่ใส่เข้ามา ตรวจสอบแต่ละตัวอักษรที่ใส่เข้ามา ตรวจสอบว่าข้อมูลใส่เข้ามาครบทุกฟิลด์ เป็นต้น เพื่อตรวจสอบความครบถ้วน และไม่ก่อให้เกิดความเสียหายต่อระบบ

ผู้พัฒนาระบบสารสนเทศต้องวิเคราะห์ความเสี่ยงที่ทำให้ข้อมูลเสียหาย (Areas of Risk) ทำการวิเคราะห์ว่ามีความเสี่ยงใดบ้างที่อาจทำให้ข้อมูลเกิดความเสียหาย

ผู้พัฒนาระบบสารสนเทศต้องมีวิธีการตรวจสอบการประมวลข้อมูลสารสนเทศ (Checks and Controls) ว่ามีข้อผิดพลาดหรือไม่

ผู้พัฒนาระบบสารสนเทศต้องมีวิธีการตรวจสอบการส่งข้อมูลในระบบสารสนเทศ เพื่อให้แน่ใจว่าข้อมูลในระบบสารสนเทศมีความปลอดภัยและมีความถูกต้องสมบูรณ์

ผู้พัฒนาระบบสารสนเทศต้องมีขั้นตอนการตรวจสอบ ทดสอบและประมวลผล เพื่อให้มั่นใจว่าระบบสามารถใช้ได้จริงและมีผลลัพธ์ที่ถูกต้อง

ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ (Security of System Files)

จุดประสงค์เพื่อให้โครงการสารสนเทศได้รับการดำเนินการอย่างปลอดภัย

ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดีว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ใช้งานอยู่

ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบจะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จ จะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้ เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริง เช่น

- ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย

- ต้องไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริงแล้ว

ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

จุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย

ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ สำหรับระบบสารสนเทศที่ใช้งานจริง อยู่แล้ว อาทิ

- คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์
- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับ
- ต้องเก็บรายละเอียดของคำขอไว้

เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่าง ๆ ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบ และทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดผู้พัฒนาระบบสารสนเทศต้องมีการป้องกันโอกาสการรั่วไหลของข้อมูล อาทิ การดักจับข้อมูลจากสายสัญญาณภายนอกบริษัท การปลอมแปลง การใช้ซอฟต์แวร์ที่มีความเสี่ยงในการรั่วไหลของข้อมูล

ในการทำสัญญาว่าจ้างการพัฒนาระบบของบริษัทต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบการตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

การบริหารจัดการช่องโหว่ในฮาร์ดแวร์ และซอฟต์แวร์ (Technical Vulnerability Management)

จุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตี โดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่ หรือตีพิมพ์ในสถานที่ต่าง ๆ

ฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งาน และประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

หมวด 8 ความรับผิดชอบต่อสินทรัพย์

(Responsibility for Assets)

ทะเบียนสินทรัพย์

1. หน่วยงานทรัพย์สินต้องจัดทำ และเก็บทะเบียนสินทรัพย์ ซึ่งรวมถึงสินทรัพย์ข้อมูล และเอกสาร (Information and Document Asset) สินทรัพย์ซอฟต์แวร์ (Software Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) เพื่อเป็นข้อมูลเบื้องต้นสำหรับ

การนำไปวิเคราะห์ ประเมินความเสี่ยง และบริหารจัดการความเสี่ยงที่มีต่อสินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุม และจัดการสินทรัพย์ขององค์กร

2. หน่วยงานทรัพย์สินต้องมีการตรวจสอบสินทรัพย์ (Inventory Check) ต้องจัดให้มีการตรวจสอบ บัญชีสินทรัพย์ทุกประเภทตามระยะเวลาที่กำหนดไว้ เช่น ปีละ 1 ครั้ง หรือภายใน 1 เดือน เมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น เป็นต้น
3. หน่วยงานทรัพย์สินต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์ เมื่อมีสินทรัพย์ใหม่ หรือสินทรัพย์ที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

ความเป็นเจ้าของสินทรัพย์

1. หน่วยงานทรัพย์สินจะต้องกำหนดบุคคล หรือหน่วยงานผู้รับผิดชอบข้อมูล และสินทรัพย์ทั้งหมด ด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทอย่างชัดเจน

การอนุญาตให้ใช้สินทรัพย์

1. หน่วยงานทรัพย์สินจะต้องกำหนดแสดงบันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูล และ สินทรัพย์จะต้องถูกใช้
2. การอนุญาตให้ใช้งานสินทรัพย์ด้านอุปกรณ์คอมพิวเตอร์มี ดังนี้
   - ระบบเทคโนโลยีสารสนเทศ และอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่บริษัท เป็นผู้จัดหามานั้นมีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานขององค์กร การใช้งานระบบ และอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวน หรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่
   - เจ้าหน้าที่ตลอดจนบุคคล และ/หรือนิติบุคคลที่ได้รับว่าจ้างโดยสำนักงาน จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศของสำนักงาน
   - ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ขององค์กรอย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน
   - เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดขององค์กรต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง
   - ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายขององค์กร รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ขององค์กรก่อนได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ
   - เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในองค์กร อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์

- อุปกรณ์คอมพิวเตอร์ขององค์กรต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์ หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ขององค์กรอย่างเด็ดขาด

3. การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์มีดังนี้
   - ห้ามเจ้าหน้าที่และผู้ใช้งานทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ขององค์กร
   - ซอฟต์แวร์ที่นำมาใช้ในการประมวลผล และจัดเก็บข้อมูลลับหรือข้อมูลสำคัญขององค์กร ทั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมาต้องได้รับการตรวจสอบควบคุม และอนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูลก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศขององค์กร
   - ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไปต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอเพื่อให้ผู้ใช้งานทั่วไปขององค์กรมีความเข้าใจ และสามารถใช้งานระบบสารสนเทศได้
   - รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานขององค์กรเท่านั้น

4. การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้
   - องค์กรจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการทำวิจัยการค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงาน และการให้บริการขององค์กร
   - ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้องค์กร และบุคคลผู้ที่เกี่ยวข้องกับองค์กรเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย
   - การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ องค์กรขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม
   - ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต
   - ห้ามผู้ใช้งานเข้าชมดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
   - องค์กรไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ด หรือบล็อก) ของเจ้าหน้าที่ ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

5. การอนุญาตให้ใช้งานอีเมล์มี ดังนี้

- ผู้ใช้งานอีเมล์ทั้งหมดขององค์กรต้องมี E-mail Account เป็นของตนเอง
- E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิด และการนำอีเมล์ไปใช้ในทางที่ผิด
- E-mail Account ที่มีวัตถุประสงค์พิเศษ เช่น Center@leaseit.co.th อาจได้รับการสร้างขึ้นเพื่อเป็น E-mail Account กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของ E-mail Account นั้น
- E-mail Account ทั้งหมด และอีเมล์ทุกฉบับ (รวมถึงอีเมล์ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายขององค์กรถือเป็นสินทรัพย์ขององค์กร
- ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบอีเมล์ขององค์กร
- พื้นที่เก็บอีเมล์บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้ เมื่อปริมาณของอีเมล์มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ และถ้าหากปริมาณของอีเมล์มากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับ- ส่งอีเมล์ได้ตามปกติอีกต่อไป
- ขนาดของอีเมล์ และไฟล์แนบได้รับการจำกัดไว้ โดยหากอีเมล์และไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายตีกลับแจ้งว่าไม่สามารถส่งอีเมล์ดังกล่าวได้
- ผู้ใช้งานต้องลบอีเมล์ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล์ให้เป็นไปตามขนาดที่องค์กรกำหนด ทั้งนี้ ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงาน และอีเมล์ตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้ E-mail Account ขององค์กรเพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมายตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น
- ห้ามใช้ E-mail Account ขององค์กรในการประกาศข้อมูลใด ๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับองค์กร
- ห้ามผู้ใช้งานทำสำเนาข้อความหรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนขององค์กร
- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นในอีเมล์ หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ e-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม
- ผู้ใช้งานต้องทำการส่งอีเมล์ให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้น และห้ามใช้คำสั่ง "Reply All" ถ้าหากอีเมล์ฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน

- ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้าต่าง ๆ (Spam Mail) เป็นต้น
- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่งอีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด
- ห้ามผู้ใช้งานส่ง หรือส่งต่ออีเมล์ที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม ศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมล์ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงาน และส่งผลเสียต่อองค์กร
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง (โทรจัน)
- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันทีจนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

6. การอนุญาตให้ใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร มีดังนี้
   - ผู้ใช้งานต้องปกป้องความมั่นคงปลอดภัยของข้อมูลลับอย่างเต็มที่เมื่อจำเป็นต้องส่งข้อมูลนั้นผ่านเครื่องโทรสาร
   - ถ้าหากผู้ใช้งานได้รับข้อมูลจากการส่งโทรสารที่ผิดพลาด ตัวอย่างเช่น ส่งโทรสารผิด หมายเลข ผิดส่วนงาน เป็นต้น ผู้ใช้งานต้องแจ้งให้ผู้ส่งโทรสารนั้นรับทราบ และทำลายเอกสารข้อมูลนั้น
   - ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น
   - ห้ามผู้ใช้งานบันทึก หรือฝากข้อความที่มีข้อมูลลับในเครื่องตอบรับโทรศัพท์อัตโนมัติ หรือระบบวอยซ์เมล์โดยเด็ดขาด
   - ห้ามสนทนาเกี่ยวกับข้อมูลลับผ่านลำโพงของเครื่องโทรศัพท์ (Speakerphones) หรือผ่านสื่ออิเล็กทรอนิกส์ใด ๆ เช่น Voice Over IP หรือในระหว่างการประชุมทางไกล เว้นแต่ผู้เข้าร่วมการประชุมทุกหน่วยงานได้รับการพิสูจน์ตัวตนแล้วว่าเป็นผู้ที่เกี่ยวข้อง และมีสิทธิ์รับทราบข้อมูล
   - ผู้ที่เกี่ยวข้องตรวจสอบจนมั่นใจแล้วว่าไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณใกล้เคียงที่อาจได้ยินข้อมูลลับที่สนทนาอยู่
   - การประชุมทางไกลถูกจัดขึ้นในบริเวณที่มีความมั่นคงปลอดภัย เช่น ห้องประชุมที่มีผนัง และประตูที่เหมาะสมสามารถป้องกันเสียงลอดออกมาได้ เป็นต้น
   - ผู้ใช้งานต้องสนทนาโทรศัพท์ด้วยความระมัดระวัง เพื่อป้องกันข้อมูลลับถูกแอบฟังโดยบุคคลที่ไม่ได้รับอนุญาต
   - ในกรณีที่ต้องมีการเปิดเผยข้อมูลลับใด ๆ ทางโทรศัพท์ ผู้ให้ข้อมูลต้องทำการตรวจสอบให้มั่นใจว่าคู่สนทนานั้นเป็นผู้ได้รับอนุญาตให้รับทราบข้อมูลดังกล่าวก่อนที่จะเปิดเผยข้อมูล

- ผู้ใช้งานต้องขออนุญาตจากเจ้าของข้อมูลก่อนทำการถ่ายเอกสารหรือสแกนเอกสารที่มีข้อมูลลับ โดยสำเนาเอกสารนั้นต้องได้รับการปกป้องดูแลในระดับเทียบเท่ากับเอกสารต้นฉบับ
- เจ้าหน้าที่ต้องไม่เปิดเผยสถานที่ตั้งของห้องเครื่องคอมพิวเตอร์แม่ข่ายต่อบุคคลภายนอกโดยเด็ดขาด เว้นแต่บุคคลภายนอกนั้นมีความจำเป็นต้องรับทราบเพื่อการปฏิบัติงาน

หมวด 9 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

(Business Continuity Management)

จุดประสงค์เพื่อป้องกันการติดขัด หรือการหยุดชะงักของกิจกรรมต่าง ๆ ทางด้านการปฏิบัติงานของบริษัท เพื่อป้องกันกระบวนการทางด้าน การปฏิบัติงานของบริษัทที่สำคัญอันเป็นผลมาจากการล้มเหลว หรือหายนะที่มีต่อระบบเทคโนโลยีสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม กำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัท การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ กำหนดให้มีการทดสอบกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัทอย่างสม่ำเสมอ

- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มี Disaster Recovery Site (DR Site) เพื่อใช้สำหรับการสำรองข้อมูลไปอีกสถานที่นึงและใช้สำหรับกู้คืนข้อมูลเมื่อเกิด ไฟไหม้ น้ำท่วม แผ่นดินไหว หรือเหตุการณ์ต่างๆ ที่ทำให้ไม่สามารถเข้าพื้นที่ DC Site ได้
- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มี Disaster Recovery Plan (DRP) ซึ่งเป็นแผนสำหรับการซ้อมกู้คืนระบบหรือข้อมูลในกรณีเกิดเหตุการณ์ไม่พึงประสงค์ทำให้ระบบหรือข้อมูลเกิดความเสียหาย สูญหาย ไม่สามารถใช้งานได้ปกติ

หมวด 10 การปฏิบัติตามข้อกำหนด

(Compliance)

การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย (Compliance with Legal Requirements)

จุดประสงค์เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติระเบียบข้อบังคับรวมทั้งสัญญาต่าง ๆ

ฝ่ายเทคโนโลยีสารสนเทศต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศของหน่วยงาน

เจ้าหน้าที่ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของ นโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ ที่กำหนดขึ้นอย่างเคร่งครัด โดยมีรายการดังต่อไปนี้เป็นอย่างน้อย

- นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์

- พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

- พ.ร.บ. ลิขสิทธิ์

ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัทถือเป็นทรัพย์สินของบริษัท (ยกเว้นข้อมูลที่เป็นทรัพย์สินของลูกค้าหรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่นๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธ์ของบุคคลภายนอก) ทั้งนี้บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้ เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ที่กำหนดไว้ตลอดจนการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งานโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตามการตรวจสอบดังกล่าวจะดำเนินการต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใด ๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคาสั่งศาล ตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น

ห้ามเจ้าหน้าที่ทุกคนใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัท กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม

ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด

ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่

ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัทโดยเด็ดขาด

เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจหรือพลั้งเผลอ จึงไม่ควรจะทำสาเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัทเพื่อจุดประสงค์ใด ๆ ก็ตาม โดยที่ไม่ได้รับอนุญาต

การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยและรายละเอียดทางเทคนิค
(Reviews of Security Policy and Technical Compliance)

จุดประสงค์เพื่อตรวจสอบระบบให้มีความสอดคล้องกับนโยบายความมั่นคงปลอดภัย

ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ตามที่กำหนดไว้

ฝ่ายเทคโนโลยีสารสนเทศต้องตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้วตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

การพิจารณาการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations)

จุดประสงค์เพื่อทำให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมดมีผลกระทบน้อยที่สุดต่อการดำเนินงานของหน่วยงาน

ฝ่ายเทคโนโลยีสารสนเทศต้องวางแผนการตรวจสอบระบบทั้งหมด โดยการตรวจสอบ ที่จะดำเนินการจะต้องไม่มีผลกระทบต่อระบบ และกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด

ฝ่ายเทคโนโลยีสารสนเทศต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด หรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น

ประกาศ ณ วันที่ 2 พฤษภาคม 2567

ฝ่ายเทคโนโลยีสารสนเทศ

บริษัท ลีซ อิท จำกัด (มหาชน)

นายวสุวัฒน์ ฐานอริยมานนท์	นางสาวสิตาพัชร์ นิโรจน์ธนรัฐ	นายอลงกต บุญมาสุข
ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ	รองประธานเจ้าหน้าที่บริหาร	ประธานเจ้าหน้าที่บริหาร
ผู้นำเสนอ	ผู้ตรวจสอบ	ผู้อนุมัติ