คณะกรรมการบริษัท ซีออยล์ จำกัด (มหาชน) ตระหนักถึงความสำคัญของ การบริหารจัดการ และการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัท มีการควบคุมภายในที่ดี ข้อมูลมีความถูกต้อง เชื่อถือได้ และปลอดภัย สามารถดำเนินงานได้อย่างมีประสิทธิภาพ และต่อเนื่อง คณะกรรมการจึงได้กำหนดเป็นนโยบายเพื่อเผยแพร่ให้กับ กรรมการ ผู้บริหาร เจ้าหน้าที่ และผู้ที่เกี่ยวข้องรับทราบและนำไปปฏิบัติ ตลอดจนกำหนดให้มีการทบทวน นโยบายและหลักเกณฑ์การรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี เพื่อให้ผู้ใช้งานเข้าถึงระบบเทคโนโลยีสารสนเทศด้วยความปลอดภัย

บริษัทฯ มีการกำหนดโครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security) ทั้งภายในองค์กร และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก ระบุผู้รับผิดชอบและตัดสินใจในด้านต่างๆ ที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศ มีการกำหนดให้แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CTO) เอกสารต่างๆ ที่เกี่ยวข้องกับนโยบายนี้ต้องได้รับการอนุมัติ รวมถึงการระบุถึงการไม่เปิดเผยความลับของบริษัทฯ และการเข้าถึงข้อมูลของลูกค้าหรือหน่วยงานภายนอก

การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)

บริษัท ได้จัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม มีการจัดทำและสอบทานบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอย่างสม่ำเสมอ รวมทั้งมีการระบุความเป็นเจ้าของในทรัพย์สินต่าง ๆ การเก็บรักษาทรัพย์สินที่มีความสำคัญต่อองค์กรอย่างเป็นระเบียบในสถานที่ที่ปลอดภัยและเหมาะสม เพื่อป้องกันการสูญหายหรือเกิดเสียหายต่อทรัพย์สินเหล่านั้น

ทั้งนี้ การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Information Classification) โดยการกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสาร เพื่อป้องกันสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม และกำหนดให้ผู้ใช้งานสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อเกิดปัญหาขึ้น

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

บริษัทสร้างความความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากรก่อนการทำงาน (Prior to Employment) ในขณะเป็นพนักงาน (During Employment) และยกเลิกการจ้างงาน (Termination of Change of Employment) หน่วยงานภายนอกที่ได้รับการว่าจ้างตามสัญญาการจ้างงานต้องปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยของผู้ให้บริการอย่างเคร่งครัด เพื่อลดความเสี่ยงจากความผิดพลาด การขโมย การปลอมแปลง และการนำไปใช้ในทางที่ไม่เหมาะสมของเจ้าหน้าที่อันเกิดจากการปฏิบัติงานกับระบบสารสนเทศและทรัพยากรสารสนเทศอื่นๆ ผู้ใช้งานมีหน้าที่ศึกษาทำความเข้าใจวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่ผู้ให้บริการกำหนดเพื่อนำไปปฏิบัติในการรักษาความปลอดภัยสินทรัพย์คอมพิวเตอร์ในส่วนที่ตนใช้งานหรือดูแลรับผิดชอบ

บริษัทจัดอบรมให้ความรู้แก่ผู้ใช้งานเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยฯ และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศและการสื่อสาร อีกทั้งกำหนดบทลงโทษทางวินัยไว้สำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติ แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุในแต่ละข้อกฎหมายนั้น

ในกรณีเจ้าหน้าที่พ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของ

การว่าจ้างงาน หลังจากมีการยกเลิกหรือเปลี่ยนแปลงตำแหน่งการเป็นเจ้าหน้าที่แล้ว จะต้องแจ้ง ยกเลิกการเข้าถึงข้อมูลต่าง ๆ ของหน่วยงานและจะแจ้งต่อเจ้าหน้าที่ในองค์กร, ลูกค้า, บริษัทคู่ค้า, ผู้ที่เกี่ยวข้องให้รับทราบตามเหมาะสม

ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

บริษัทกำหนดให้ฝ่ายเทคโนโลยีสารสนเทศ ควบคุมการเข้าออกในเขตรักษาความปลอดภัยให้เหมาะสมกับสถานที่หรือพื้นที่ที่ต้องรักษาความปลอดภัยที่เหมาะสม และต้องมีการบันทึกข้อมูลการเข้าออกห้องคอมพิวเตอร์ (Data Center) ของบุคคลภายนอกทุกครั้ง ส่วนเจ้าหน้าที่หรือผู้ใช้งานต้องจัดวางและป้องกันอุปกรณ์ในสถานที่มิดชิดเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต และให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communication and operations management)

กำหนดให้ฝ่ายเทคโนโลยีสารสนเทศของบริษัท จัดทำคู่มือ และ / หรือ ขั้นตอนการปฏิยัติงานสารสนเทศในหน่วยงาน เช่น การแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติและเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ หากมีการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ ฝ่ายเทคโนโลยีสารสนเทศจะบันทึกการเปลี่ยนแปลงทุกครั้ง โดยจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบรายละเอียดของการเปลี่ยนแปลง และให้ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศและเครือข่ายให้เกิดความชัดเจน เพื่อหลีกเลี่ยงการใช้งานสินทรัพย์ผิดวัตถุประสงค์ หรือโดยไม่มีสิทธิ

ฝ่ายเทคโนโลยีสารสนเทศต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถทรัพยากรปัจจุบันอย่างสม่ำเสมอตามความเหมาะสมของทรัพยากรชนิดต่างๆ และวางแผนจัดการขีดความสามารถของระบบอย่างน้อยปีละครั้ง เพื่อลดความเสี่ยงต่อการเกิดความล้มเหลวของระบบลงให้เหลือน้อยที่สุด

การจัดการผู้ให้บริการภายนอก (Third Party Service Delivery Management) ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอกโดยให้ฝ่ายเทคโนโลยีสารสนเทศทบทวนและตรวจสอบบริการจากผู้ให้บริการภายนอกตามข้อตกลงที่กำหนด และเป็นผู้รับผิดชอบในการบริหารจัดการการเปลี่ยนแปลงจากผู้ให้บริการภายนอก เพื่อให้มีและคงไว้ซึ่งระดับการรักษาความปลอดภัยสารสนเทศ และระดับการให้บริการที่เหมาะสมและสอดคล้องกับข้อตกลงการบริการกับหน่วยงานภายนอก

การควบคุมและป้องกันการใช้งานระบบและอุปกรณ์เคลื่อนที่ผิดวัตถุประสงค์ เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์สื่อสารอิเล็กทรอนิกส์แบบไร้สายสารสนเทศที่ต้องการใช้งานผ่านระบบเครือข่ายของผู้ให้บริการ จะต้องได้รับการลงทะเบียนและกำหนดสิทธิการใช้งานตามนโยบายความปลอดภัย ก่อนได้รับการอนุมัติเพื่อให้งานในระบบ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุด (Update Latest Pattern) อยู่เสมอ เครื่องให้บริการ เครื่องตั้งโต๊ะ และโน้ตบุ๊คทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส

บริษัทยังมีการสำรองข้อมูล (Information Back-up) โดยฝ่ายเทคโนโลยีสารสนเทศทำการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูลหรือระบบ และมีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพ สามารถใช้งานได้ตลอดเวลา และกำหนดระยะเวลาในการสำรองข้อมูลตามระดับการบริหารความเสี่ยง พร้อมกระบวนการสำรองข้อมูลและการกู้ข้อมูลของทุกระบบ ต้องมีการทำเอกสาร และมีการตรวจสอบและทดสอบเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

ส่วนระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management) ฝ่ายเทคโนโลยีสารสนเทศต้องรับผิดชอบรวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด ระบบเครือข่าย

ทั้งหมดของผู้ให้บริการที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมสามารถในการตรวจจับไวรัสได้ และบริษัทจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของผู้ให้บริการ และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายโดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง ทั้งนี้บริษัทยังกำหนดวิธีการจัดส่งสื่อบันทึกข้อมูล (สารสนเทศหรือซอฟต์แวร์) ให้มีความมั่นคงปลอดภัย กำหนดขั้นตอนการป้องกันการแลกเปลี่ยนข้อมูลระหว่างผู้ให้บริการ เพื่อป้องกันการสูญหายของสารสนเทศและซอฟต์แวร์ รวมทั้งเพื่อป้องกันการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต หรือการนำสารสนเทศไปใช้ในทางที่ไม่เหมาะสม

การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring) บริษัทกำหนดให้ฝ่ายเทคโนโลยีสารสนเทศทำการบันทึกกิจกรรม (Audit Logging) การใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ และตรวจสอบการใช้งานสินทรัพย์สารสนเทศอย่างสม่ำเสมอ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่ และบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and Operator Logs) และบันทึกเหตุการณ์ข้อผิดพลาด (Fault Logging) ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น ดำเนินการแก้ไขได้ตามสมควร และรายงานผู้บริหารระบบรับทราบอยู่เสมอ

การควบคุมการเข้าถึง (Access Control)

บริษัทมีการกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย ซึ่งผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศได้ ดังนั้น ฝ่ายเทคโนโลยีสารสนเทศจึงมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของผู้ให้บริการ และเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

ทั้งนี้ ผู้ใช้งานต้องพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ และฝ่ายเทคโนโลยีสารสนเทศต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัยอยู่เสมอ และทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ และให้มีการจัดเก็บบันทึกข้อมูลการเข้าถึงและการใช้งานระบบสารสนเทศแต่ละระบบ (Log Files) เป็นระยะเวลาอย่างน้อย 1 ปี

ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษา User Name และรหัสผ่านของตนเอง รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้ ให้มีความมั่นคงปลอดภัยอย่างสม่ำเสมอ และรหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอ หากผู้ใช้งานสงสัยว่า User ID หรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อฝ่ายเทคโนโลยีสารสนเทศและทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที

ส่วนการควบคุมการเข้าถึงเครือข่าย (Network Access Control) การใช้งานระบบปฏิบัติการ (Operating System Access Control) การใช้งานระบบสารสนเทศและสารสนเทศ (Application and Information Access Control) การเข้าถึงข้อมูลสารสนเทศ (Information Technology Access Control) บริษัทมีแนวทาง/นโยบายควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต และกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการจะปฏิเสธการใช้งานหากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง หรือพิสูจน์ตัวตนสำหรับผู้ใช้งานระบบเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ และจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด ทั้งนี้ สิทธิการเข้าถึงไฟล์ข้อมูลสารสนเทศต้องได้รับการควบคุม และได้รับการพิจารณาอนุมัติเท่าที่จำเป็นเท่านั้น เพื่อให้ไฟล์ข้อมูลสารสนเทศได้รับการรักษาความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ รวมทั้งเป็นการแบ่งแยกสิทธิและหน้าที่ของผู้ใช้งาน ส่วนคอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถานที่ ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง และ/หรือ

ใส่รหัสผ่านป้องกันข้อมูลที่สำคัญ เพื่อควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทเคลื่อนที่ได้ รวมทั้งการปฏิบัติงานนอกสำนักงานให้เป็นไปอย่างปลอดภัย

การบริหารจัดการเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

บริษัทกำหนดให้เจ้าหน้าที่และผู้ใช้งานทุกคนต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของผู้ให้บริการ โดยผ่านช่องทางการรายงานที่กำหนดไว้และฝ่ายเทคโนโลยีสารสนเทศ จะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้ เพื่อเตรียมการในการรองรับเหตุการณ์ผิดปกติที่อาจเกิดขึ้นให้ฝ่ายเทคโนโลยีสารสนเทศทำหน้าที่เป็นศูนย์กลางประสานงานและดำเนินการแก้ไขปัญหาที่เกิดจากเหตุการณ์ผิดปกติและเพื่อประโยชน์ในการนี้ โดยจัดตั้งคณะทำงานขึ้นชุดหนึ่งเรียกว่า “คณะทำงานเพื่อแก้ไขปัญหาจากเหตุการณ์ผิดปกติ” เพื่อทำหน้าที่ จัดทำแผนฉุกเฉินรองรับเหตุการณ์ผิดปกติที่อาจเกิดขึ้น / ประสานงานกับส่วนงานที่เกี่ยวข้อง และดำเนินการแก้ไขปัญหาเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น / กำหนดวิธีปฏิบัติในการแก้ไขปัญหาจากเหตุการณ์ผิดปกติที่เกิดขึ้น เพื่อเป็นแนวทางสำหรับผู้ใช้งานและคณะทำงาน / ประเมินวิธีปฏิบัติในการแก้ไขปัญหาจากเหตุการณ์ผิดปกติทุก 1 ปี และปรับปรุงแก้ไขวิธีปฏิบัติให้เหมาะสม หากพบข้อบกพร่อง ให้ส่วนงานต่าง ๆ ให้ความร่วมมือและประสานงานกับฝ่ายเทคโนโลยีสารสนเทศและคณะทำงานในการจัดทำแผนฉุกเฉิน และการแก้ไขปัญหาเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น

ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใดๆ ในผู้ให้บริการต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา หน่วยงานจัดการความปลอดภัย (Security Management) และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

บริษัทกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของผู้ให้บริการ การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ และกำหนดให้มีการทดสอบกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของผู้ให้บริการ อย่างสม่ำเสมอ เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ทางด้านการปฏิบัติงานของผู้ให้บริการ เพื่อป้องกันกระบวนการทางด้านการปฏิบัติงานของผู้ให้บริการที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย (Compliance with Legal Requirements)

บริษัทตระหนักถึงนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน และต้องการให้เจ้าหน้าที่ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและ การสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด เช่น นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ พ.ร.บ.ลิขสิทธิ

บริษัทห้ามเจ้าหน้าที่ทุกคนใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของผู้ให้บริการ กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม และเจ้าหน้าที่หรือฝ่ายเทคโนโลยีสารสนเทศต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด และต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิการใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิถูกต้องหรือไม่ และห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิบนระบบเทคโนโลยีสารสนเทศของผู้ให้บริการโดยเด็ดขาด

ส่วนการตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยและรายละเอียดทางเทคนิค (Reviews of Security Policy and Technical Compliance) และการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations) ต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้ โดยตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้วตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบ ใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย และวางแผนการตรวจสอบระบบทั้งหมด โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบ และกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด และต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด หรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้นเพื่อทำให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมดมีผลกระทบน้อยที่สุดต่อการดำเนินงานของบริษัท