นโยบายบริหารจัดการและรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ในการดำเนินกิจการ บริษัทได้นำเทคโนโลยีสารสนเทศมาใช้ในการเพิ่มโอกาสทางธุรกิจและพัฒนาการดำเนินกิจการ ดังนั้นเพื่อให้กิจการสามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของกิจการอย่างมีประสิทธิภาพและ สอดคล้องกับหลักการกำกับดูแลกิจการที่ดี คณะกรรมการบริษัทจึงจัดให้มีนโยบายการบริหารจัดการและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญและมีความเข้าใจเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และใช้เป็นกรอบในการปฏิบัติหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ โดยมีรายละเอียดและแนวปฏิบัติดังนี้

1. แนวทางการจัดทำและการปฏิบัติตามนโยบาย

1.1 ต้องจัดทำนโยบายบริหารจัดการและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษรและผู้บริหาร หัวหน้าแผนกเทคโนโลยีสารสนเทศ และผู้ใช้งานของแต่ละฝ่ายงานต้องมีส่วนร่วมในการจัดทำนโยบาย และอย่างน้อยต้องได้รับอนุมัติจากคณะกรรมการบริษัทหรือ คณะกรรมการชุดย่อยที่ได้รับมอบหมายจากคณะกรรมการบริษัท ทั้งนี้ให้พิจารณาปัจจัยภายในและภายนอกองค์กร บทบาทของเทคโนโลยีสารสนเทศต่อการดำเนินธุรกิจ รวมทั้งความสอดคล้องกับเป้าหมาย และวัตถุประสงค์ของบริษัท และต้องทบทวนและปรับปรุงนโยบาย อย่างน้อยปีละ 1 ครั้ง โดยจะทบทวนโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการบริหารจัดการเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบาย

1.2 ต้องจัดเก็บนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้อง สามารถเข้าถึงได้โดยง่าย

1.3 ต้องจัดให้มีการเผยแพร่นโยบาย เพื่อสื่อสารทำความเข้าใจกับพนักงาน และหน่วยงานภายนอกที่เกี่ยวข้องให้รับทราบและตระหนักถึงความสำคัญของการบริหารจัดการและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

1.4 เจ้าหน้าที่ฝ่ายคอมพิวเตอร์นำระเบียบปฏิบัติการจัดการเทคโนโลยีสารสนเทศ มาใช้เพื่อควบคุม และบังคับใช้ด้านการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และทุกกระบวนการที่เกี่ยวข้อง

1.5 เจ้าหน้าที่ฝ่ายคอมพิวเตอร์นำคู่มือปฏิบัติการรักษาความปลอดภัยด้านทรัพยากรบุคคล และเทคโนโลยีสารสนเทศ. เป็นขั้นตอนมาตรฐานในการดำเนินงาน ประกาศให้พนักงานได้รับทราบและปฏิบัติตามอย่างเคร่งครัด.

1.6 นโยบายต้องระบุวัตถุประสงค์และขอบเขตอย่างชัดเจน และมีเนื้อหาครอบคลุมอย่างน้อยในเรื่องต่อไปนี้

1.6.1 การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

1.6.2 การควบคุมการเข้าออก และการป้องกันความเสียหาย (Physical Security)

1.6.3 การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

1.6.4 การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

1.6.5 การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

1.6.6 การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

1.6.7 การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

1.6.8 ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

(ก) การกำหนดความเสี่ยงที่สามารถยอมรับได้

(ข) การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(ค) การบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

(ง) การกำหนดตัวชี้วัดระดับความเสี่ยง (IT Risk Indicator) และจัดให้มีการติดตามรายงานผลตัวชี้วัดดังกล่าว

(จ) การกำหนดหน้าที่และความรับผิดชอบของบุคลากรผู้ทำหน้าที่บริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.6.9 การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

1.7 ต้องประกาศใช้และสื่อสารนโยบายให้แก่บุคคลที่เกี่ยวข้องอย่างทั่วถึง โดยการติดประกาศหรือส่งอีเมล เป็นต้น รวมถึงจัดการฝึกอบรมและพัฒนาความรู้ด้านเทคโนโลยีให้แก่บุคคลากร ที่เกี่ยวข้อง เพื่อให้สามารถปฏิบัติตามได้

1.8 ต้องมีระบบติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามนโยบายอย่างเคร่งครัดและมีประสิทธิภาพ

1.9 ต้องมีการตรวจสอบ รวมทั้งประเมินความเพียงพอของนโยบายและระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยหน่วยงานที่เป็นอิสระอย่างน้อยปีละครั้ง ซึ่งอาจเป็นหน่วยงานตรวจสอบภายในของบริษัทเองหรือผู้ตรวจสอบภายนอก

1.10 ต้องแจ้งคณะกรรมการตรวจสอบและ/หรือคณะกรรมการบริษัทโดยเร็ว เมื่อมีกรณีที่พบข้อบกพร่องในกระบวนการ หรือการปฏิบัติตามนโยบายบริหารจัดการและรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่อาจส่งผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ และให้กำหนดผู้มีหน้าที่รับผิดชอบการแก้ไขข้อบกพร่องนั้น ๆ

1.11 ต้องมีขั้นตอนหรือวิธีปฏิบัติเพื่อรองรับให้มีการปฏิบัติตามนโยบายที่ได้กำหนดไว้

1.12 ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องอย่างชัดเจน โดยจัดทำเป็นลายลักษณ์อักษรเพื่อ เผยแพร่ และสร้างความมั่นใจให้ผู้ที่เกี่ยวข้อง เช่น หน้าที่ของผู้ใช้งานในกรณีที่พบว่าเครื่องคอมพิวเตอร์มีการติดไวรัส และหน้าที่และความรับผิดชอบของเจ้าหน้าที่รักษาความปลอดภัยของระบบเครือข่าย เป็นต้น

2. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

การแบ่งแยกอำนาจหน้าที่มีวัตถุประสงค์เพื่อให้บริษัทมีโครงสร้างในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบสารสนเทศระดับองค์กรที่ดี โดยมีรายละเอียดและแนวปฏิบัติดังนี้

2.1 ต้องแบ่งแยกบุคลากรหรือหน่วยงานเพื่อปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ กำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

2.2 ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ และสนับสนุนงานปฏิบัติการ โดยกำหนดให้จัดตั้งแผนกเทคโนโลยีสารสนเทศ

2.3 ต้องจัดให้มีการระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายในแผนกเทคโนโลยีสารสนเทศอย่างชัดเจนเป็นลายลักษณ์อักษร

2.4 ควรจัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น เช่น ผู้จัดการแผนกเทคโนโลยีสารสนเทศ (IT Manager) เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (IT Support) นักพัฒนาระบบงาน (System engineer) เป็นต้น

2.5 เพื่อสนับบสนุนโครงสร้างของโครงสร้างในการบริหารจัดการสำหรับการดำเนินการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ให้คัดเลือกบุคลากรที่มีความเหมาะสมทั้งในด้านประสบการณ์และความรู้ความสามารถและจำนวนที่เพียงพอและความเหมาะสม

3. การควบคุมการเข้าออก และการป้องกันความเสียหาย (Physical Security)

3.1 การควบคุมการเข้าออก มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (availability risk) ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (availability risk) โดยมีรายละเอียดและแนวปฏิบัติดังนี้

3.2 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ใน บริษัทหรือพื้นที่หวงห้าม และต้องกำหนดสิทธิการเข้าออก ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น ผู้จัดการแผนกเทคโนโลยีสารสนเทศ (IT Manager) เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (IT Support) เป็นต้น

3.3 ในกรณีที่บุคคลซึ่งไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกบริษัทในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีเจ้าหน้าที่ควบคุมดูแลการทำงานตลอดเวลา เป็นต้น

3.4 ต้องมีระบบเก็บบันทึกการเข้าออกบริษัทโดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

3.5 จัดพื้นที่ ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (network zone) ส่วนเครื่องแม่ข่าย (server zone) ส่วนเครื่องพิมพ์ (printer zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

3.6 ความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

3.6.1. ระบบป้องกันไฟไหม้

(ก) ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

(ข) ต้องมีระบบการแจ้งเตือนอัคคีภัย และอย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

3.6.2. ระบบป้องกันไฟฟ้าขัดข้อง

(ก) ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ

(ข) ต้องมีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์สำคัญ เพื่อให้การดำเนินงานมีความต่อเนื่อง

3.6.3. ระบบควบคุมอุณหภูมิและความชื้น

ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

3.6.4. การเตือนภัยน้ำรั่ว

หากบริษัทตั้งอยู่ในสถานที่ที่มีความเสี่ยงต่อภัยน้ำรั่ว ก็ควรหมั่นสังเกตว่ามีน้ำรั่วหรือไม่อย่างสม่ำเสมอ และใต้เครื่องปรับอากาศภายในห้องเซิร์ฟเวอร์ต้องมีถาดรองน้ำ เพื่อลดความเสี่ยงที่จะทำให้ห้องเซิร์ฟเวอร์เสียหายในกรณีที่มีเหตุการณ์น้ำรั่ว

4. การบริหารจัดการและรักษาความปลอดภัยของทรัพย์สินสารสนเทศ

การบริหารจัดการและการรักษาความปลอดภัย ความลับ ความน่าเชื่อถือ และความพร้อมใช้ของทรัพย์สินสารสนเทศ อันได้แก่ ทรัพย์สินสารสนเทศประเภทระบบ ทรัพย์สินสารสนเทศประเภทอุปกรณ์ และทรัพย์สินสารสนเทศประเภทข้อมูล มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (integrity risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง malicious code ต่างๆ มิให้เข้าถึง (access risk) หรือสร้างความเสียหาย (availability risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย ดังนี้

4.1. การบริหารจัดการข้อมูลต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

4.2. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น

4.3. ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (storage) นำเข้า (input) ประมวลผล (operate) และแสดงผล (output) นอกจากนี้ ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (distributed database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

4.4. ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

4.5. การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน[1] (user privilege)

4.5.1. ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (application system) สิทธิการใช้งานอินเทอร์เนต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

4.5.2. ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิพิเศษ (Privilege User ID) ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิพิเศษมีความรัดกุมเพียงพอหรือไม่นั้นบริษัทจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

(ก) ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่

(ข) ควรควบคุมการใช้งาน User ที่มีสิทธิพิเศษอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งาน User ดังกล่าวในลักษณะ Dual Control โดย แบ่งรหัสผ่านใส่ซองปิดผนึกเป็นสองส่วน โดยมีการลงนาม 3 ท่านคือ

1. ผู้จัดการแผนกเทคโนโลยีสารสนเทศ
2. ผู้อำนวยการฝ่ายบัญชี
3. ประธานเจ้าหน้าที่วัฒนธรรมองค์กร

(ค) เก็บซองส่วนแรกไว้ในตู้เซฟ ผู้ดูแลคือผู้อำนวยการฝ่ายบัญชี

(ง) เก็บซองส่วนที่สองไว้ที่แผนกเทคโนโลยีสารสนเทศ ผู้ดูแลคือผู้จัดการแผนกเทคโนโลยีสารสนเทศ

(จ) ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว และจำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(ฉ) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

---

[1] ผู้ใช้งาน หมายถึง เจ้าของข้อมูล ผู้บริหารระบบ (IT Manager) เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (IT Support) นักพัฒนาระบบงาน (System engineer) และเจ้าหน้าที่อื่นที่ใช้งานระบบคอมพิวเตอร์

4.5.3. ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (log out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

4.5.4. ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ share files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

4.5.5. ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

4.6. การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (user account) และรหัสผ่าน (password)

4.6.1. ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (identification and authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี user account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น บริษัทจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

(ก) ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร

(ข) ควรใช้อักขระพิเศษประกอบอย่างน้อย 1 ตัว เช่น ! @ # $ % ^ & * ( ) _ + { } | * - + [ ] < > \ ? " / ' : ; สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 6 เดือน ส่วนผู้ใช้งานที่มีสิทธิพิเศษ เช่น ผู้บริหารระบบ (system administrator) และผู้ใช้งานที่ติดมากับระบบ (default user) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 3 เดือน

(ค) ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

(ง) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “123456” เป็นต้น

(จ) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกระยะเวลา 90 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน และควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น

(ฉ) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

(ช) ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

(ซ) ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญ2 อย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของพนักงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (default user) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น disable ลบออกจากระบบ หรือ เปลี่ยน password เป็นต้น

4.7. การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

4.7.1. ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

4.7.2. ต้องเปิดใช้บริการ (service)[3] ที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

4.7.3. ต้องดำเนินการติดตั้ง patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (system software) เช่น update antivirus เป็นต้น อย่างสม่ำเสมอ

4.7.4. ควรทดสอบ system software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

4.7.5. ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของโปรแกรมระบบอย่างชัดเจน

4.8. การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)

4.8.1. ต้องแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก เป็นต้น

4.8.2. ต้องมีระบบป้องกันการบุกรุก เช่น firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก

4.8.3. ต้องมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ

(ก) ความพยายามในการบุกรุกผ่านระบบเครือข่าย

(ข) การใช้งานในลักษณะที่ผิดปกติ

---

[2] ระบบงานสำคัญ หมายถึง ระบบ Formula ระบบShare File และระบบเครือข่าย

(service) หมายถึง บริการต่างๆ ของเครื่องแม่ข่าย เช่น telnet หรือ ftp หรือ ping เป็นต้น

(ค) การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

4.8.4. ต้องจัดทำแผนผังระบบเครือข่าย (network diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

4.8.5. ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า parameter ต่างๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (physical disconnect) และจุดเชื่อมต่อ (disable port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง

4.8.6. ในกรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ remote access หรือการเชื่อมต่อเครือข่ายภายนอกโดยใช้ modem (dial out) ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่และมีการควบคุมอย่างเข้มงวด เช่น การใช้ระบบ call back การควบคุมการเปิดปิด modem การตรวจสอบตัวตนจริงและสิทธิของผู้ใช้งาน การบันทึกรายละเอียดการใช้งาน และในกรณี dial out ก็ควรตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อออกจากระบบเครือข่ายภายใน เป็นต้น รวมทั้งต้องตัดการเชื่อมต่อการเข้าถึงดังกล่าวเมื่อไม่ใช้งานแล้ว

4.8.7. ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่าย และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ก็ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

4.8.8. การใช้เครื่องมือต่างๆ (tools) เพื่อตรวจเช็คระบบเครือข่าย ควรได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

4.9. การบริหารการเปลี่ยนแปลงระบบคอมพิวเตอร์ (configuration management)

4.9.1. ก่อนการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์ ควรมีการประเมินผลกระทบที่เกี่ยวข้องและบันทึกการเปลี่ยนแปลงให้เป็นปัจจุบันอยู่เสมอ รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ

4.9.2. ควรติดตั้งซอฟต์แวร์เท่าที่จำเป็นแก่การใช้งาน และถูกต้องตามลิขสิทธิ์

4.10. การวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (capacity planning)

4.10.1. ต้องประเมินการใช้งานระบบคอมพิวเตอร์สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต

4.11. การป้องกันภัยคุกคามต่อระบบสารสนเทศ

4.11.1. การป้องกันภัยคุกคามต่อระบบสารสนเทศต้องมีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น

4.11.2. ควรควบคุมมิให้ผู้ใช้งานระงับการใช้งาน (disable) ระบบป้องกันไวรัสที่ได้ติดตั้งไว้ และควรแจ้งบุคคลที่เกี่ยวข้องทันทีในกรณีที่พบว่ามีไวรัส

4.12. บันทึกเพื่อการตรวจสอบ (audit logs)

4.12.1. ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ (login-logout logs) และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน

4.12.2. ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

4.12.3. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

4.12.4. มีการกำหนดการเข้าถึงทางเทคนิคของระบบ (Flow Chart) โดยอ้างอิงรูปแบบและวิธีการต่าง ๆ จากระเบียบปฏิบัติ (PM)

5. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง โดยมีรายละเอียดและแนวปฏิบัติดังนี้

5.1 การกำหนดขั้นตอนการปฏิบัติงาน

5.1.1. ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน

5.1.2. ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (emergency change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

5.1.3. ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

5.2 การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

5.2.1 การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร (อาจเป็น electronic transaction เช่น อีเมล เป็นต้น) และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ ผู้จัดการแผนกเทคโนโลยีสารสนเทศ เป็นต้น

5.2.2 ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (operation) ระบบรักษาความปลอดภัย (security) และการทำงาน (functionality) ของระบบงานที่เกี่ยวข้อง

5.2.3 ควรสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางการ

5.3 การปฏิบัติงานพัฒนาระบบงาน

5.3.1 ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) ออกจากส่วนที่ใช้งานจริง (production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

5.3.2 ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ

5.3.3 ควรตระหนักถึงระบบรักษาความปลอดภัย (security) และเสถียรภาพการทำงาน (availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

5.4 การทดสอบ

5.4.1 ผู้ที่ร้องขอและแผนกเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

5.4.2 ในระบบงานสำคัญควรมีหน่วยงานหรือทีมงานอิสระ เข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนาและการทดสอบระบบ ก่อนที่จะโอนย้ายไปใช้งานจริง

5.5 การโอนย้ายระบบงานเพื่อใช้งานจริง

ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

5.6 การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ version ของระบบงานที่ได้รับการพัฒนา

5.6.1 ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่ผ่านมา

5.6.2 ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และ program specification เป็นต้น และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

5.6.3 ต้องจัดเก็บโปรแกรม version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

5.7 การทดสอบหลังการใช้งาน (post- implementation test)

ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

5.8 การสื่อสารการเปลี่ยนแปลง

ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

6. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉินโดยมีรายละเอียดและแนวปฏิบัติดังนี้

6.1 การสำรองข้อมูลและระบบคอมพิวเตอร์

6.1.1 ทำการ Backupไปยังพื้นที่เก็บข้อมูลภายในองค์กร (Local Storage) และส่งไปยังพื้นที่เก็บข้อมูลภายนอกองค์กร (Cloud Storage) ในเวลาเดียวกัน ซึ่งมีความถี่อย่างน้อยวันละ 2 ครั้ง หรือเมื่อ Software ที่ใช้ เช่น Formula และ Humano มีการปรับปรุงเวอร์ชั่น.

6.1.2 Replace เวลา 12.30น. และ 21.00น. on local drive และ on cloud พร้อมกัน.

6.1.3 เก็บ File backup on cloud อย่างน้อยอาทิตย์ละ 1 ครั้ง (ทุกวันศุกร์ หรือวันสุดท้ายในการทำงานของแต่ละสัปดาห์) ทั้ง 2 ช่วงเวลา

6.1.4 ตรวจสอบว่าข้อมูลที่ได้รับการ Backup สมบูรณ์ โดยดูจากขนาดของไฟล์หลังการ Backup หรือ ดูจากเครื่องหมายสถานะการ upload to cloud เป็นเครื่องหมายถูก

6.1.5 หลังจากสำรองข้อมูลแบบถาวรอย่างน้อยอาทิตย์ละ 1 ครั้งเรียบร้อย เมื่อขึ้นเดือนใหม่จะทำการลบไฟล์ Backup บนพื้นที่เก็บข้อมูลภายในองค์กร (Local Storage) และพื้นที่เก็บข้อมูลภายนอกองค์กร (Cloud Storage) ก่อนหน้าเดือนปัจจุบัน

6.2 การทดสอบ

6.2.1 ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 2 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

6.2.2 ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

6.3 การเก็บรักษา

6.3.1 ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในข้อ Physical Security ด้วย

6.3.2 ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

6.4 การเตรียมพร้อมกรณีฉุกเฉิน

6.4.1 ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุดโดยแผนฉุกเฉินต้องมีรายละเอียด ดังนี้

(ก) ต้องจัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงาน

(ข) ต้องกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

(ค) ต้องมีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

(ง) ต้องกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

(จ) ต้องมีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะ ของเครื่องคอมพิวเตอร์ (specification) ขั้นต่ำ ค่า configuration และอุปกรณ์เครือข่าย เป็นต้น

(ฉ) ในกรณีที่บริษัทมี บริษัทสำรอง ก็ต้องระบุรายละเอียดเกี่ยวกับ บริษัทสำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น

(ช) ต้องปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่

(ซ) ต้องทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 2 ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย

(ฌ) ควรสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น

(ญ) ในกรณีเกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย สามารถดูรายละเอียดเพิ่มเติมได้ที่ คู่มือขั้นตอนการสำรองข้อมูล (Backup)

7. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้องต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่างๆ ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk และ availability risk โดยมีรายละเอียดและแนวปฏิบัติดังนี้

7.1 การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

ต้องมีขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็น แนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (computer operator) เช่น ขั้นตอนในการเปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ.

7.2 การติดตามการทำงานของระบบคอมพิวเตอร์ (monitoring)

ควรบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่างๆ ให้อยู่ในสภาพที่ดีและพร้อมใช้งานอยู่เสมอ

7.3 การจัดการปัญหาต่างๆ

7.3.1 ต้องจัดให้มีช่องทางการติดต่อ[แผนกเทคโนโลยีสารสนเทศ]โดยกำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน เช่น กำหนดผู้รับผิดชอบในการแก้ไขปัญหาระบบ FORMULA เป็นต้น รวมถึงเบอร์โทรศัพท์ของผู้ที่เกี่ยวข้องเพื่อใช้ติดต่อในกรณีที่มีปัญหา และต้องปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

7.3.2 ควรมีระบบจัดเก็บบันทึกปัญหาและเหตุการณ์ผิดปกติที่เกิดขึ้น และรายงานให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหาและตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาต่อไป

8. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงต่อบริษัทในรูปแบบที่แตกต่างไปจากการดำเนินงานปกติโดยบริษัทเอง เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (access risk) ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลและการประมวลผลของระบบงาน (integrity risk) ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น ดังนั้น การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นจึงมีวัตถุประสงค์เพื่อให้บริษัทใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการโดยมีรายละเอียดและแนวปฏิบัติดังนี้

8.1 การคัดเลือกผู้ให้บริการ

8.1.1 ควรมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ

8.1.2 ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

8.2 การควบคุมผู้ให้บริการ

8.2.1 ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่บริษัทควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่บริษัท (onsite service) และให้เจ้าหน้าที่บริษัทตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ remote access และปิด modem ทันทีที่การให้บริการเสร็จสิ้น เป็นต้น

8.2.2 ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

8.3 ระเบียบการควบคุมความปลอดภัยเกี่ยวกับการใช้สื่อบันทึกข้อมูลด้านกายภาพ

8.3.1 “สื่อบันทึกข้อมูลด้านกายภาพ” คือ อุปกรณ์ที่ใช้ในการบันทึกข้อมูลโดยใช้วิธีการเชื่อมต่อกับคอมพิวเตอร์โดยตรง เช่น Flash Drive, External Hard Disk, USB หรือ CD เป็นต้น.

8.3.2 ต้องควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล โดยผู้เป็นเจ้าของหรือผู้ได้รับมอบหมายต้องลงทะเบียนการใช้งานสื่อบันทึกข้อมูลเป็นลายลักษณ์อักษร และต้องผ่านการตรวจสอบและสแกนไวรัสจากแผนกเทคโนโลยีสารสนเทศเท่านั้น.

8.3.3 ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำการเปลี่ยน หรือทดแทนอุปกรณ์.

8.3.4 ต้องลบหรือฟอร์แมต (Format) ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อน ทำลายหรือเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์.

8.3.5 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อ การรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ.

8.3.6 โปรแกรมต่างๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัทเป็นโปรแกรมที่ บริษัทได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรม และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานเพราะเป็น การกระทำที่ผิดกฎหมาย.

8.3.7 ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

9. ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

9.1 การกำหนดความเสี่ยงที่สามารถยอมรับได้

พิจารณาถึงระดับความเสี่ยงที่บริษัทสามารถยอมรับได้เมื่อมีความเสี่ยงนั้น ๆ เกิดขึ้น โดยควรมีการกำหนดระดับความเสี่ยงที่สามารถยอมรับได้ (Risk Appetite) โดยอาจพิจารณาจากระดับความเสี่ยงที่บริษัทสามารถยอมรับได้ รวมถึงวัฒนธรรมองค์กร หรือระดับการยอมรับความเสี่ยงของคณะกรรมการตรวจสอบและ/หรือคณะกรรมการบริษัท

9.2 การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เมื่อบริษัทระบุความเสี่ยงที่เป็นไปได้ทั้งหมดกำหนดสถานการณ์ความเสี่ยง และกำหนดปัจจัยความเสี่ยง ที่เหมาะสม รวมทั้งกำหนดความเสี่ยงที่สามารถยอมรับได้แล้ว จึงประเมินถึงโอกาสเกิดและผลกระทบของเหตุการณ์ ความเสี่ยงที่กำหนดไว้ โดยอาจจัดทำในรูปแบบของแผนภาพความเสี่ยง (Risk Map) เพื่อนำเสนอระดับของโอกาสเกิดและผลกระทบของแต่ละเหตุการณ์ความเสี่ยง และทะเบียนความเสี่ยง (Risk Register) เพื่อบรรยายข้อมูลรายละเอียดของ ความเสี่ยง จากนั้นจึงจัดทำโครงร่างของความเสี่ยง (Risk Profile) เพื่อรวบรวมความเสี่ยงที่เกี่ยวข้องทั้งหมด โดยโครงร่างรวบรวมความเสี่ยงเหตุการณ์ ประเภท และ ปัจจัยความเสี่ยงระบุความเสี่ยงที่เกี่ยวข้องระบุความเสี่ยงที่เกี่ยวข้องอันอาจมีผลกระทบต่อการดำเนินงานบันทึกข้อมูลความเสี่ยงรวบรวมข้อมูลความเสี่ยง ปัจจัยภายใน และปัจจัยภายนอกที่เกี่ยวข้องสำรวจข้อมูลเหตุการณ์ในอดีตรวบรวมข้อมูลเหตุการณ์ความเสี่ยง และ ผลกระทบในอดีต ทั้งภายในองค์กร แนวโน้มอุตสาหกรรม เป็นต้นเชื่อมโยงเหตุการณ์ความเสี่ยง เชื่อมโยงเหตุการณ์ที่เคยเกิดขึ้น เงื่อนไขของเหตุการณ์ ปัจจัยที่มีผลต่อผลกระทบของเหตุการณ์ปรับปรุงข้อมูลเหตุการณ์ความเสี่ยง ปรับปรุง วิเคราะห์ และทบทวนเหตุการณ์ความเสี่ยงอย่างสม่ำเสมอ

9.3 การระบุความเสี่ยง

เพื่อกำหนดความเสี่ยงที่เป็นไปได้ทั้งหมด เพื่อใช้ในการบริหารจัดการให้ความเสี่ยง ที่เกี่ยวข้องอยู่ในระดับที่ยอมรับได้ และยังช่วยบริษัทเปรียบเทียบโอกาสเกิด และผลกระทบของแต่ละความเสี่ยง และใช้ในการจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

9.4 การบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

เพื่อให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปตามระดับความสำคัญ และตอบสนองต่อเป้าหมายขององค์กร บริษัทควรมีกระบวนการในการบริหารและจัดการต่อความเสี่ยง ดังนี้

9.4.1 ควรนำระดับความเสี่ยงที่สามารถยอมรับได้มาเปรียบเทียบกับผลการประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่ได้ดำเนินการไว้ข้างต้น ซึ่งในกระบวนการนี้ บริษัทอาจประเมินการควบคุมและความเสี่ยงที่ยังหลงเหลืออยู่ โดยในกรณีที่ความเสี่ยงที่หลงเหลืออยู่เกินกว่าระดับที่องค์กรยอมรับได้ ควรมีการกำหนดวิธีการบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงนั้น

9.4.2 การบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ (Risk Response) อาจพิจารณาจากระดับความสำคัญของความเสี่ยง ประสิทธิภาพและประสิทธิผลของการจัดการความเสี่ยง และความสามารถของบริษัทในการดำเนินกิจกรรมเพื่อจัดการความเสี่ยง โดยการบริหารจัดการเพื่อตอบสนองต่อความเสี่ยงสามารถดำเนินการได้ใน 4 ลักษณะ อันได้แก่ การหลีกเลี่ยงความเสี่ยง (Risk Avoidance), การยอมรับความเสี่ยง(Risk Acceptance), การร่วมรับความเสี่ยง/ถ่ายโอน (Risk Sharing/Transfer) และการลดความเสี่ยง (Risk Mitigation)

9.5 การกำหนดตัวชี้วัดระดับความเสี่ยง (IT Risk Indicator) และจัดให้มีการติดตามรายงานผลตัวชี้วัดดังกล่าว

9.5.1 บริษัทควรกำหนดตัวชี้วัดระดับความเสี่ยง (IT Risk Indicator) เพื่อสามารถชี้วัดและติดตามความเสี่ยงได้อย่างรวดเร็ว รวมทั้งสามารถติดตามแนวโน้มของความเสี่ยงที่อาจเกิดขึ้น

9.5.2 ควรมีการรายงานผลการประเมินความเสี่ยงที่มีผลต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งหมดในรูปแบบที่สามารถนำไปประกอบการตัดสินใจได้ รวมถึงรายงานผลการบริหารจัดการความเสี่ยง ประสิทธิผลของการควบคุมข้อตรวจพบ หรือข้อปรับปรุง รวมทั้งผลกระทบจากรายการความเสี่ยง

9.6 การกำหนดหน้าที่และความรับผิดชอบของบุคลากรผู้ทำหน้าที่บริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

9.6.1 คณะกรรมการของบริษัทเป็นผู้รับผิดชอบในการให้แนวทางและอนุมัติเห็นชอบในนโยบายการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศโดยคณะกรรมการตรวจสอบเป็นผู้สอบทานการกำกับดูแลด้านการปฏิบัติงานและด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยของข้อมูลและแผนรองรับในกรณีฉุกเฉินที่มีประสิทธิผล รวมทั้งติดตามผลการปฏิบัติตามนโยบายการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและรายงานต่อคณะกรรมการบริษัท

9.6.2 ผู้บริหารซึ่งมีหน้าที่ในการบริหารความเสี่ยงตามที่ได้รับมอบหมายจากคณะกรรมการบริษัท เป็นผู้ทำหน้าที่ในการกำหนดกรอบและกระบวนการการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ รวมทั้งสนับสนุนให้มีการดำเนินงานดังกล่าวโดยผู้บริหารซึ่งมีหน้าที่ในการบริหารความเสี่ยงนี้จะเป็นผู้รับผิดชอบ (Accountable person) ในผลการบริหารจัดการความเสี่ยงทุกรูปแบบทั่วทั้งองค์กร รวมถึงรับผิดชอบให้มีการจัดทำและปรับปรุงรายการความเสี่ยงและกิจกรรมการบริหารความเสี่ยง

9.6.3 ผู้บริหารหน่วยงานที่ปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ อาทิ หัวหน้าแผนกเทคโนโลยีสารสนเทศ เป็นผู้ทำหน้าที่ในการบริหารจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

10. การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

เพื่อให้มีการใช้ทรัพยากรสารสนเทศอย่างคุ้มค่า ลดความเสี่ยงที่อาจเกิดขึ้นและตอบสนองต่อความต้องการทางด้านธุรกิจอย่างมีประสิทธิภาพและมีประสิทธิผล โดยมีต้นทุนในระดับที่ยอมรับได้ คณะกรรมการบริษัทจึงกำหนดแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศหรือแผนด้านเทคโนโลยีสารสนเทศ เพื่อใช้เป็นแนวทางในการจัดสรรและบริหารทรัพยากรสารสนเทศ รวมถึงงบประมาณด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับแผนกลยุทธ์โดยรวมขององค์กร และเพียงพอต่อความต้องการใน

ปัจจุบันและอนาคต รวมทั้งทางเลือกเกี่ยวกับแหล่งที่มาของทรัพยากรสารสนเทศ และกลยุทธ์ในการจัดหาทรัพยากรโดยคำนึงถึงถึงปัจจัยดังต่อไปนี้

10.1 ความต้องการของผู้มีส่วนได้ส่วนเสีย และประเด็นที่เกี่ยวข้องกับกลยุทธ์ อาทิ ระดับการพึ่งพิงการใช้ระบบสารสนเทศ ความสามารถและความรู้ความเข้าใจในระบบสารสนเทศขององค์กร เพื่อที่จะประเมินระดับความสำคัญของเทคโนโลยีสารสนเทศในปัจจุบันและแนวโน้มที่เป็นไปได้ในอนาคตต่อแผนกลยุทธ์โดยรวมขององค์กร

10.2 ความน่าเชื่อถือ ความปลอดภัย และความคุ้มค่าในการใช้งานทรัพยากรสารสนเทศที่มีอยู่ และการจัดหาทรัพยากรสารสนเทศเพิ่มเติม

10.3 ความสอดคล้องของกลยุทธ์ทางด้านเทคโนโลยีสารสนเทศและกลยุทธ์ขององค์กรในภาพรวม เพื่อที่จะตอบสนองเป้าหมายขององค์กร โดยอาจพิจารณาจากเป้าหมายผลตอบแทนในการลงทุน (Return on investment) หรือความคาดหวังจากการลงทุนทางด้านเทคโนโลยีสารสนเทศ

10.4 ประโยชน์หรือโอกาส รวมทั้งความท้าทายที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศที่มีอยู่ในปัจจุบันและเทคโนโลยีที่มีการพัฒนาขึ้นใหม่มาใช้สำหรับการดำเนินงาน

10.5 การพิจารณากำหนดบทบาทหน้าที่ ความรับผิดชอบ และโครงสร้างการตัดสินใจในการดำเนินงานทางด้านเทคโนโลยีสารสนเทศที่เหมาะสม ที่ทำให้การตัดสินใจและการลงทุนทางด้านเทคโนโลยีสารสนเทศสร้างคุณค่าให้แก่องค์กร

10.6 เงื่อนไขในการจัดระดับความสำคัญหรือเงื่อนไขที่ใช้ในการตัดสินใจเกี่ยวกับการดำเนินงานที่สำคัญ หรือการลงทุนที่สำคัญทางด้านเทคโนโลยีสารสนเทศ โดยอาจพิจารณาจากความเสี่ยงที่เกี่ยวข้อง แผนการใช้งานระบบงานใหม่ งบประมาณ รวมถึงผลตอบแทนที่ได้รับ

10.7 ในการจัดทำงบประมาณทางด้านเทคโนโลยีสารสนเทศ ควรพิจารณาครอบคลุมทุกรายการที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น ทรัพย์สินสารสนเทศ การใช้ทรัพยากรส่วนกลางขององค์กร บุคลากรทางด้านสารสนเทศ ผู้ให้บริการภายนอกทางด้านเทคโนโลยีสารสนเทศ ค่าใช้จ่ายในการประกันภัย และค่าลิขสิทธิ์ที่เกี่ยวข้อง

10.8 นอกจากนี้อาจมีการประเมินต้นทุนทางตรง และต้นทุนทางอ้อมของบริการทางด้านเทคโนโลยีสารสนเทศเพื่อใช้เป็นข้อมูลในการจัดทำงบประมาณทางด้านเทคโนโลยีสารสนเทศ

ประกาศ ณ วันที่ 25 มีนาคม พ.ศ. 2564

.....

(นายประเสริฐ บุญสัมพันธ์)

ประธานกรรมการบริษัท