CIVIL ENGINEERING

บริษัท ซีวิลเอนจีเนียริง จำกัด (มหาชน)

ระเบียบบริษัท

เรื่อง

การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

จัดทำโดย :	อนุมัติโดย :
(นายฤทธิกร ทวีเจริญสิน) ผู้จัดการแผนกเทคโนโลยีสารสนเทศ	(นายปิยะดิษฐ์ อัศวศิริสุข) ประธานเจ้าหน้าที่บริหาร

ประวัติการแก้ไขเอกสาร

ครั้งที่	ผู้ดำเนินการ	วันที่บังคับใช้	รายละเอียดการแก้ไข
0	นายฤทธิกร ทวีเจริญสิน	01 ตุลาคม 2561	จัดทำเอกสารเป็นครั้งแรก

สารบัญ

หน้า

การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท 3

หมวดที่ 1 การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ 4

หมวดที่ 2 การแบ่งแยกหน้าที่ 6

หมวดที่ 3 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย 8

หมวดที่ 4 การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย 9

หมวดที่ 5 การใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานจากภายนอกบริษัท 14

หมวดที่ 6 การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ 16

หมวดที่ 7 การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน 18

หมวดที่ 8 การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ 20

หมวดที่ 9 การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น 22

การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

เพื่อประสิทธิภาพสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของบริษัท ซีวิลเอนจีเนียริง จำกัด (มหาชน) จึงเห็นควรให้มีการกำหนดระเบียบบริษัท เรื่อง การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยมีวัตถุประสงค์ ดังนี้

1. เพื่อเป็นแนวปฏิบัติของบุคลากร ซึ่งรวมทั้งพนักงานและผู้บริหารในการใช้งาน ดูแลรักษา และควบคุมระบบสารสนเทศและคอมพิวเตอร์ของบริษัท
2. เพื่อเป็นแนวทางในการกำหนดมาตรฐานการทำงานที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศ ของบริษัท ตลอดจนกระบวนการการทำงานที่ถูกต้องและเป็นมาตรฐานเดียวกันในการบริหารจัดการข้อมูล และกำหนดระดับชั้นความมั่นคงปลอดภัยของข้อมูล
3. เพื่อสร้างความเชื่อมั่นในระบบรักษาความปลอดภัยของข้อมูลธุรกิจต่อบุคลากรซึ่งเป็นผู้ใช้บริหาร และผู้มีส่วนเกี่ยวข้องในการดำเนินธุรกิจของบริษัท

สาระสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ มีดังนี้

1. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
2. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
3. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
4. การใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานจากภายนอกบริษัท (Mobile Device and Teleworking)
5. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบคอมพิวเตอร์ (Change Management)
6. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
7. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)
8. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

ระบบข้อมูลสารสนเทศ เป็นระบบคอมพิวเตอร์ ระบบโครงข่าย และอุปกรณ์โครงข่ายสำคัญของระบบข้อมูลทางการบริหารจัดการของบริษัท การจัดทำ จัดเก็บ นำไปใช้ และควบคุมดูแลรักษาระบบความมั่นคงความปลอดภัยของข้อมูลทางธุรกิจของบริษัท จะสามารถปกป้องคุ้มครองข้อมูลและความลับทางธุรกิจของบริษัท มิให้รั่วไหล และก่อให้เกิดความเสียหายต่อธุรกิจได้ ดังนั้น ความสำเร็จทางธุรกิจของบริษัทส่วนหนึ่งจึงขึ้นอยู่กับประสิทธิภาพในการใช้งาน และการป้องกันให้เกิดความมั่นคงปลอดภัยของระบบคอมพิวเตอร์อย่างถูกต้องและเหมาะสมอยู่เสมอ

หมวดที่ 1 การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

การจัดให้มีระเบียบบริษัทฯ เกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งาน และบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่ ความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำระเบียบบริษัทฯ รายละเอียดของระเบียบบริษัทฯ และการปฏิบัติตามระเบียบบริษัทฯ

แนวทางปฏิบัติ

1. เกี่ยวกับการจัดทำระเบียบบริษัทฯ
   1) ระเบียบบริษัทฯ เกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศนี้ ได้จัดทำเป็นลายลักษณ์อักษรโดยผู้บริหารสูงสุดด้านเทคโนโลยีสารสนเทศ และนำเสนอกรรมการผู้จัดการพิจารณาอนุมัติ
   2) ระเบียบบริษัทฯ นี้ต้องทบทวนและปรับปรุง ให้เป็นปัจจุบันอยู่เสมอ โดยต้องมีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง ซึ่งต้องมีการกำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง
   3) ต้องจัดเก็บระเบียบบริษัทฯ ที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้อง สามารถเข้าถึงได้โดยง่าย

2. รายละเอียดของระเบียบบริษัทฯ

   ต้องระบุวัตถุประสงค์ และขอบเขตอย่างชัดเจน และมีเนื้อหาครอบคลุมอย่างน้อยในเรื่องต่อไปนี้

   1) การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
   2) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และป้องกันความเสียหาย (Physical Security)
   3) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
   4) การใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานจากภายนอกบริษัท (Mobile Device and Teleworking)
   5) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)
   6) การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
   7) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)
   8) การควบคุมการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

3. การปฏิบัติตามระเบียบบริษัทฯ
   1) จัดให้มีการประกาศใช้และสื่อสารระเบียบบริษัทฯ ให้แก่บุคคลที่เกี่ยวข้องอย่างทั่วถึง เพื่อให้สามารถปฏิบัติตามได้ เช่น จัดการฝึกอบรม เป็นต้น
   2) จัดให้มีระบบติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามระเบียบบริษัทฯ อย่างเคร่งครัด
   3) จัดให้มีการตรวจสอบ รวมทั้งประเมินความเพียงพอของระเบียบบริษัทฯ และระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศ โดยหน่วยงานที่เป็นอิสระอย่างน้อยปีละ 1 ครั้ง ซึ่งอาจเป็นหน่วยงานตรวจสอบภายในของบริษัทเอง หรือผู้ตรวจสอบภายนอก
   4) จัดให้มีการแจ้งแผนกแผนกเทคโนโลยีสารสนเทศโดยเร็ว เมื่อมีกรณีที่ส่งผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ
   5) จัดให้มีกระบวนการเพื่อรองรับให้มีการปฏิบัติตามระเบียบบริษัทฯ ที่ได้กำหนดไว้
   6) จัดให้มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ใช้งานและบุคคลที่เกี่ยวข้องอย่างชัดเจน เช่น หน้าที่ของผู้ใช้งานในกรณีที่พบว่าเครื่องคอมพิวเตอร์มีการติดไวรัส หน้าที่และความรับผิดชอบของเจ้าหน้าที่รักษาความปลอดภัยระบบเครือข่าย หน้าที่และความรับผิดชอบของลูกจ้างชั่วคราว เป็นต้น

หมวดที่ 2 การแบ่งแยกหน้าที่ (Segregation of Duties)

วัตถุประสงค์

การแบ่งแยกหน้าที่มีวัตถุประสงค์เพื่อให้มีการถ่วงดุลการปฏิบัติงานภายในของแผนกแผนกเทคโนโลยีสารสนเทศ

แนวทางปฏิบัติ

1. แผนกเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบดำเนินการและควบคุมให้เกิดการปฏิบัติตามระเบียบบริษัท เรื่อง การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท ฉบับนี้ และให้มีการรายงานตามโครงสร้างการบังคับบัญชาตามปกติ ทั้งนี้ แผนกแผนกเทคโนโลยีสารสนเทศมีบทบาท หน้าที่ และความรับผิดชอบ (IT, Security, Roles and Responsibilities) ดังนี้
   1) มีการแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production Environment)
   2) จัดให้มี Job Description ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายในแผนกแผนกเทคโนโลยีสารสนเทศอย่างชัดเจนเป็นลายลักษณ์อักษร
   3) ดูแลรักษาข้อมูลสารสนเทศอันเป็นทรัพย์สินของบริษัท ให้มีความมั่นคง ปลอดภัยอยู่เสมอ
   4) กำหนดคุณสมบัติของทรัพย์สินใหม่ หรืออะไหล่ที่ใช้ในการซ่อมแซมกรณีที่ต้องเปลี่ยนอะไหล่ ส่วนการจัดซื้อให้เป็นไปตามระเบียบปฏิบัติเกี่ยวกับการคัดเลือกและประเมินซัพพลายเออร์ การจัดซื้อ/จัดจ้าง และการเบิกจ่ายให้ปฏิบัติตามระเบียบปฏิบัติ เรื่อง การจ่ายเงินชำระค่าสินค้า บริการ และค่าใช้จ่ายอื่น ๆ

2. แผนกเทคโนโลยีสารสนเทศรับผิดชอบกำหนดคุณสมบัติที่เหมาะสมของอุปกรณ์คอมพิวเตอร์ ซอฟท์แวร์ และให้ฝ่ายบัญชี (ทรัพย์สิน) เป็นผู้รับผิดชอบในการตรวจสอบและจัดทำทะเบียนทรัพย์สินประเภทเครื่องคอมพิวเตอร์ เครื่องพิมพ์ และซอฟท์แวร์คอมพิวเตอร์ โดยแต่ละหน่วยงานจะเป็นผู้รับผิดชอบอุปกรณ์ของตนเอง ทั้งนี้ ในทะเบียนทรัพย์สิน จะต้องมีการตรวจสอบอย่างน้อยปีละ 1 ครั้ง ซึ่งอุปกรณ์ที่ต้องการจัดทำทะเบียน ได้แก่
   1) เครื่องคอมพิวเตอร์ (Personal Computer, Laptop/Notebook, และอุปกรณ์อื่น ๆ ที่จัดอยู่ในหมวดโปรแกรมคอมพิวเตอร์)
   2) เครื่องพิมพ์และอุปกรณ์ต่อพ่วงคอมพิวเตอร์
   3) ซอฟท์แวร์คอมพิวเตอร์
   4) Router / Access Point / Firewall / UPS

รายละเอียดของผู้ใช้งานในทะเบียน จะต้องระบุรายละเอียดให้ครบถ้วน ดังนี้

1) ชื่อผู้ใช้งาน
2) ชื่อ ฝ่าย หรือ แผนก
3) ชื่อเครื่อง รุ่นเครื่อง และตราผลิตภัณฑ์ (Brand)
4) หมายเลขไอพี (IP Address)

3. แผนกทรัพยากรบุคคล เป็นผู้รับผิดชอบในการดำเนินการดังนี้
   1) แจ้งให้แผนกเทคโนโลยีสารสนเทศทราบในทันที เมื่อมีการเปลี่ยนแปลงสภาพของผู้ใช้งาน เช่น การลาพักงาน การโอนย้าย การเปลี่ยนแปลงหน้าที่ การลาออก เพื่อให้แผนกเทคโนโลยีสารสนเทศทำการระงับการใช้งาน เปลี่ยนแปลง หรือลบสิทธิการใช้งานภายใน 30 วัน หรือวันที่ผู้บังคับบัญชาเห็นสมควร
   2) ร่วมกับหน่วยงานต้นสังกัดจัดทำ Job Description ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายในฝ่ายต่าง ๆ อย่างชัดเจน เป็นลายลักษณ์อักษร
   3) พนักงานบริษัททุกคนต้องลงนามในสัญญาข้อตกลงว่าด้วยการรักษาความลับข้อมูลทางกับบริษัทก่อนเริ่มงาน และหลังจากประกาศใช้ระเบียบบริษัทฉบับนี้ และให้ถือเป็นส่วนหนึ่งของสัญญาว่าจ้าง

หมวดที่ 3 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์ (Data Center) มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (Access Risk) แก้ไขเปลี่ยนแปลง (Integrity Risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (Availability Risk) ส่วนการป้องกันความเสียหาย มีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูล และระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ (Availability Risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และระบบป้องกันความเสียหายต่าง ๆ ที่บริษัทควรจัดให้มีภายในศูนย์คอมพิวเตอร์

แนวทางปฏิบัติ

1. การควบคุมศูนย์คอมพิวเตอร์
   1) ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น เจ้าหน้าที่เทคโนโลยีสารสนเทศ เป็นต้น
   2) ต้องมีระบบเก็บบันทึกการเข้า - ออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
   3) ควรจัดศูนย์คอมพิวเตอร์ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงาน และยังทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญๆ มีประสิทธิภาพมากขึ้น
2. การป้องกันความเสียหาย
   1) ระบบป้องกันไฟไหม้
      - ระบบป้องกันไฟไหม้ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น
      - ศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรอง อย่างน้อยต้องมีถังดับเพลิงที่เหมาะสำหรับการใช้งานในห้องคอมพิวเตอร์ เพื่อใช้สำหรับการดับเพลิงในเบื้องต้น
   2) ระบบป้องกันไฟฟ้าขัดข้อง
      - ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ
      - ต้องมีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์สำคัญ เพื่อให้การดำเนินงานมีความต่อเนื่อง
   3) ระบบควบคุมอุณหภูมิและความชื้น
      - ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศ และตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์

หมวดที่ 4 การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

วัตถุประสงค์

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious Code ต่าง ๆ ไม่ให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

แนวทางปฏิบัติ

1. การบริหารจัดการข้อมูล
   1) ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีการปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
   2) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น
   3) ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) นอกจากนี้ ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน
   4) ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

2. การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)
   1) ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบคอมพิวเตอร์ (Application System) สิทธิการใช้งานอินเตอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจเป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
   2) ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิพิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม แผนกเทคโนโลยีสารสนเทศจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม
      2.1) ควรได้รับความเห็นชอบจากผู้มีอำนาจ

2.2) ควรควบคุมการใช้งาน User ที่มีสิทธิพิเศษอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งาน User โดยให้เก็บซอง Password ไว้ในตู้เซฟ เป็นต้น และจำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

2.3) ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

2.4) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสผ่านทุก 180 วัน เป็นต้น

3) ในกรณีที่ไม่มีการปฏิบัติงานอยู่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

4) ในกรณีที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญ มีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึง หรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

5) ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉิน หรือชั่วคราว ต้องมีการขออนุมัติจากผู้มีอำนาจทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3. การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

1) ต้องมีระบบตรวจสอบตัวตนจริง และสิทธิการเข้าใช้งานของผู้ใช้งานก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดา และการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น บริษัทฯ จะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณา

1.1) ควรกำหนดให้รหัสผ่านประกอบด้วย ตัวเลข และตัวอักษร รวมกันให้มีความยาวขั้นต่ำ 8 ตัวอักษร

1.2) สำหรับผู้ใช้งานทั่วไป และผู้ใช้งานที่มีสิทธิพิเศษ ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 180 วัน ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

1.3) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น abcdef, aaaaaa, 123456 เป็นต้น

1.4) ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น

1.5) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งบริษัทกำหนดให้ผิดได้ไม่เกิน 3 ครั้ง

1.6) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้น โดยทันที

1.7) ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

2) ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อพนักงานที่ลาออกไปแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยน Password เป็นต้น

4. การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

1) ต้องมีกระบวนการในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

2) ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

3) ต้องดำเนินการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติงาน DBMS และ Web Server เป็นต้น อย่างสม่ำเสมอ

4) ควรทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

5) ควรมีแนวทางปฏิบัติในการใช้งาน Software Utility เช่น Personal Firewall Password Cracker เป็นต้น และตรวจสอบการใช้งาน Software Utility อย่างสม่ำเสมอ

6) ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของโปรแกรมระบบอย่างชัดเจน

5. การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)

1) ต้องแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก ส่วน DMZ เป็นต้น

2) ต้องมีระบบป้องกันการบุกรุก เช่น Firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก

3) ต้องมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ

3.1) ความพยายามในการบุกรุกผ่านระบบเครือข่าย

3.2) การใช้งานในลักษณะที่ผิดปกติ

3.3) การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

4) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
5) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า Parameter ต่าง ๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Physical Disconnect) และจุดเชื่อมต่อ (Disable Port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง
6) ในกรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ Remote Access หรือการเชื่อมต่อเครือข่ายภายนอกโดยผ่านระบบ Internet ต้องได้รับการอนุมัติจากผู้มีอำนาจและมีการควบคุมอย่างเข้มงวด เช่น การใช้ระบบ, VPN การควบคุมการเปิด-ปิดระบบ Remote การตรวจสอบตัวตนจริงและสิทธิของผู้ใช้งาน การบันทึกรายละเอียดการใช้งาน และในกรณีหยุดการเชื่อมต่อก็ควรตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อออกจากระบบเครือข่ายภายใน เป็นต้น รวมทั้งต้องตัดการเชื่อมต่อการเข้าถึงดังกล่าวเมื่อไม่ใช้งานแล้ว
7) ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่าย และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละ 1 ครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ก็ควรแจ้งบุคคลที่เกี่ยวข้องได้รับทราบทุกครั้ง
8) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจเช็คระบบเครือข่าย ควรได้รับการอนุมัติจากผู้มีอำนาจและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6. การบริหารการเปลี่ยนแปลงระบบคอมพิวเตอร์ (Configuration Management)
   1) ก่อนการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์ ควรมีการประเมินผลกระทบที่เกี่ยวข้องและบันทึกการเปลี่ยนแปลงให้เป็นปัจจุบันอยู่เสมอ รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ
   2) ควรติดตั้งซอฟต์แวร์เท่าที่จำเป็นแก่การใช้งาน และถูกต้องตามลิขสิทธิ์

7. การวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (Capacity Planning)

   ต้องประเมินการใช้งานระบบคอมพิวเตอร์สำคัญไว้ล่วงหน้า เพื่อรับรองการใช้งานในอนาคต

8. การป้องกันไวรัส และ Malicious Code
   1) ต้องมีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น

2) ควรควบคุมมิให้ผู้ใช้งานระงับใช้งาน (disable) ระบบป้องกันไวรัสที่ได้ติดตั้งไว้ และควรแจ้งบุคคลที่เกี่ยวข้องทันทีที่พบว่ามีไวรัส

9. บันทึกเพื่อการตรวจสอบ (Audit Logs)

1) ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ (login-logout logs) บันทึกการพยายามเข้าสู่ระบบ (login attempts) บันทึกการใช้ command line และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน

2) ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

3) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกต่าง ๆให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่ 5 การใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานจากภายนอกบริษัท (Mobile Device and Teleworking)

วัตถุประสงค์

เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับการปฏิบัติงานของบริษัทจากระยะไกล รวมทั้ง การใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา จึงกำหนดแนวปฏิบัติ ดังนี้

แนวทางปฏิบัติ

1. ในกรณีการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพาสำหรับการปฏิบัติงานที่มีการเชื่อมต่อกับระบบงานภายในบริษัท ทั้งนี้ ไม่รวมถึงระบบ mail service บริษัทได้มีมาตรการป้องกันข้อมูลสารสนเทศที่สำคัญ โดยพิจารณาถึงแนวทางดังต่อไปนี้
   1) กำหนดให้มีการลงทะเบียนอุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น ยี่ห้อ รุ่น ระบบปฏิบัติการรหัสประจำเครื่อง (serial number) และหมายเลขอ้างอิงอุปกรณ์เครือข่าย (MAC address) เป็นต้น อย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนอุปกรณ์ เพื่อให้มั่นใจได้ว่าการใช้งานอุปกรณ์ดังกล่าวมีความสอดคล้องเป็นไปตามระเบียบบริษัท การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
   2) มีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) กรณีที่อุปกรณ์คอมพิวเตอร์ประเภทพกพาสูญหาย เช่น การกำหนดให้ใส่รหัสผ่านก่อนใช้งานอุปกรณ์ (lock screen) หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น
   3) กำหนดประเภทบริการการใช้งาน (application service) ที่อนุญาตให้ใช้งานผ่านอุปกรณ์คอมพิวเตอร์ประเภทพกพา และกำหนดมาตรการควบคุมการเข้าถึงบริการการใช้งานดังกล่าวโดยคำนึงถึงความปลอดภัยของการเชื่อมต่อกับเครือข่าย เช่น จำกัดให้เข้าถึงบริการการใช้งานบางประเภทหากเป็นการเชื่อมต่อกับเครือข่ายภายนอก เป็นต้น
   4) กำหนดให้มีการเข้ารหัสข้อมูลสารสนเทศที่สำคัญบนอุปกรณ์พกพาและที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์
   5) กำหนดให้มีการอบรมผู้ใช้งานเพื่อตระหนักและทราบถึงความเสี่ยงจากการใช้งาน และแนวทางการควบคุมความเสี่ยงดังกล่าว
   6) ควบคุมให้มีการติดตั้งเฉพาะซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์ และโปรแกรมเพื่อปิดช่องโหว่ (patches) ที่เหมาะสม
   7) กำหนดมาตรการป้องกันโปรแกรมไม่ประสงค์ดี (malware)
   8) กำหนดให้มีการดำเนินการเพื่อลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศเช่น ตัดการเชื่อมต่อโดยทันทีที่ทราบเหตุ เป็นต้น

ทั้งนี้ หากอุปกรณ์คอมพิวเตอร์ประเภทพกพาเป็นทรัพย์สินของพนักงาน บริษัทได้เข้มงวดให้มีการปฏิบัติตามแนวทางในข้อ 1) - 5) เป็นอย่างน้อย พร้อมทั้งกำหนดให้มีมาตรการควบคุมที่เทียบเคียงหรือทดแทนแนวทาง ในข้อ 6) - 8) เพิ่มเติม เช่น กำหนดให้มีการตรวจสอบอุปกรณ์คอมพิวเตอร์ประเภทพกพาอย่างสม่ำเสมอ กำหนดบทลงโทษหรือตัดสิทธิการใช้งาน application service ในกรณีที่พนักงานละเมิดข้อกำหนด เป็นต้น

2. ในกรณีที่มีการปฏิบัติงานของบริษัทจากระยะไกล (teleworking site) บริษัทได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลสารสนเทศที่ถูกเข้าถึง ประมวลผลและจัดเก็บในพื้นที่ปฏิบัติงาน โดยพิจารณาถึง
   1) การควบคุมสิทธิการใช้งานและการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งานอย่างเหมาะสม
   2) การรักษาความมั่นคงปลอดภัยกรณีมีการเชื่อมต่อระบบงานที่สำคัญ หรือรับส่งข้อมูลที่เป็นความลับหรือมีความสำคัญจากระยะไกล (remote access)
   3) การป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิในการใช้งาน เช่น ญาติพี่น้อง และเพื่อน เป็นต้น
   4) การป้องกันโปรแกรมไม่ประสงค์ดี (malware)

หมวดที่ 6 การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่ การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงใช้งานจริง

แนวทางปฏิบัติ

1. การกำหนดกระบวนการปฏิบัติงาน
   1) ควรมีกระบวนการในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานที่เกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน
   2) ควรมีกระบวนการในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (emergency change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจทุกครั้ง
   3) ควรสื่อสารเกี่ยวกับรายละเอียดกระบวนการดังกล่าวให้ผู้ใช้งาน และบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

2. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน
   1) การร้องขอ
      1.1) การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร (อาจเป็น Electronic Transaction เช่น Email เป็นต้น) และได้รับอนุมัติจากผู้มีอำนาจ
      1.2) ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง
      1.3) ควรสอบทานกฎเกณฑ์ของทางบริษัทที่เกี่ยวข้อง เนื่องจากการแก้ไข เปลี่ยนแปลง ในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางบริษัท

2) การปฏิบัติงานพัฒนาระบบ

2.1) ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Development Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น

2.2) ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ

2.3) ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

3) การทดสอบ

3.1) ผู้ที่ร้องขอและแผนกเทคโนโลยีสารสนเทศรวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

3.2) ในระบบงานสำคัญควรมีหน่วยงานหรือทีมงานอิสระ เข้าตรวจสอบว่ามีการปฏิบัติตามกระบวนการพัฒนาและการทดสอบระบบ ก่อนที่จะโอนย้ายไปใช้งานจริง

4) การโอนย้ายระบบงานเพื่อใช้งานจริง ควรตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

5) การจัดทำเอกสารและรายละเอียดการพัฒนาระบบงาน และจัดเก็บ Version ของระบบงานที่ได้รับการพัฒนา

5.1) ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา

5.2) ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียด โครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน กระบวนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

6) การทดสอบหลังการใช้งาน (Post-Implementation Test) ควรกำหนดให้มีการทดสอบระบบที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

7) การสื่อสารการเปลี่ยนแปลง ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

หมวดที่ 7 การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

วัตถุประสงค์

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (Availability Risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

แนวทางปฏิบัติ

1. การสำรองข้อมูลและระบบคอมพิวเตอร์
   1) การสำรอง
      1.1) ต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง
      1.2) ควรมีกระบวนการในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้
         - ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
         - ประเภทสื่อบันทึก (Media)
         - จำนวนที่ต้องสำรอง (Copy)
         - วิธีการสำรอง
         - สถานที่ และวิธีการเก็บรักษาสื่อบันทึก
         - ควรมีการบันทึกการปฏิบัติงาน (Log Book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
   2) การทดสอบ
      2.1) ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูล รวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้
      2.2) ควรมีกระบวนการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน
   3) การเก็บรักษา
      3.1) ต้องจัดเก็บสื่อบันทึกข้อมูลสำรองไว้ในที่ปลอดภัย และมีระบบป้องกันความเสียหายตามที่กล่าวในข้อ Physical Security ด้วย

3.2) ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

3.3) ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

3.4) การขอใช้งานสื่อบันทึกข้อมูลสำรอง ควรได้รับอนุมัติจากผู้มีอำนาจ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา

3.5) ควรมีกระบวนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว

2. การเตรียมพร้อมกรณีฉุกเฉิน

1) ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินต้องมีรายละเอียดดังนี้

1.1) ต้องจัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงาน

1.2) ต้องกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

1.3) ต้องมีกระบวนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

1.4) ต้องกำหนดเจ้าหน้าที่รับผิดชอบและผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

1.5) ต้องมีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (specification) ขั้นต่ำ ค่า Configuration และอุปกรณ์เครือข่าย เป็นต้น

1.6) ในกรณีที่บริษัทมีศูนย์คอมพิวเตอร์สำรองก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจนเช่น สถานที่ตั้ง แผนที่ เป็นต้น

1.7) ต้องปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอและเก็บแผนฉุกเฉินไว้นอกสถานที่

2) ต้องทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย

3) ควรสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น

4) ในกรณีเกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ปัญหาไว้ด้วย

หมวดที่ 8 การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

วัตถุประสงค์

การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้มีการใช้งานคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพโดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่าง ๆ ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk และ availability risk

แนวทางปฏิบัติ

1. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์
   1) ต้องมีกระบวนการในการปฏิบัติงานประจำในด้านต่าง ๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่เทคโนโลยีสารสนเทศ เช่น ขั้นตอนในการเปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพในการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และปรับปรุงขั้นตอนและวิธีการปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ
   2) ควรกำหนดให้เจ้าหน้าที่เทคโนโลยีสารสนเทศ ปฏิบัติงานโดยผ่านเมนูและควรจำกัดการปฏิบัติงานเท่าที่จำเป็น

2. การติดตามการทำงานของระบบคอมพิวเตอร์ (monitoring)
   1) ต้องติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่อง และมีประสิทธิภาพ เช่น การรับส่งข้อมูลของระบบ การใช้งานฮาร์ดดิสก์ การใช้งานหน่วยประมวลผล (CPU) เป็นต้น เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพ (capacity) ของระบบ
   2) ควรบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์ต่าง ๆให้อยู่ในสภาพที่ดีและพร้อมใช้งานอยู่เสมอ

3. การจัดการปัญหาต่าง ๆ
   1) ต้องกำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน เช่น กำหนดผู้รับผิดชอบในการแก้ไขปัญหาระบบการใช้งานของบริษัท เป็นต้น รวมถึงเบอร์โทรศัพท์ของผู้ที่เกี่ยวข้องเพื่อใช้ติดต่อในกรณีที่มีปัญหา
   2) ควรมีระบบจัดเก็บบันทึกปัญหา และเหตุการณ์ผิดปกติที่เกิดขึ้นและรายงานให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหา และตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาต่อไป

4. การควบคุมการจัดทำรายงาน
   1) การขอให้จัดพิมพ์รายงานต่าง ๆ ควรได้รับความเห็นชอบจากผู้มีอำนาจ
   2) ควรมีทะเบียนคุมการพิมพ์ และการจัดส่งรายงานจัดเก็บรายงานต่าง ๆ ที่ได้จัดพิมพ์แล้วอย่างรัดกุม และกำหนดให้มีการลงลายมือชื่อเมื่อมีการรับรายงาน นอกจากนี้ควรทำลายรายงานที่ไม่ได้ใช้งานแล้ว

หมวดที่ 9 การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

วัตถุประสงค์

การใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น อาจก่อให้เกิดความเสี่ยงต่อบริษัทในรูปแบบที่แตกต่างไปจากการดำเนินงานปกติโดยบริษัทเอง เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (access risk) ความเสี่ยงเกี่ยวกับความถูกต้อง ครบถ้วนของข้อมูล และการประมวลผลของระบบงาน (integrity risk) ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น ดังนั้นการควบคุมการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น จึงมีวัตถุประสงค์เพื่อให้บริษัทใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกแบบควบคุมการปฏิบัติงานของผู้ให้บริการ

แนวทางปฏิบัติ

1. การคัดเลือกผู้ให้บริการ
   1) ควรมีการกำหนดเกณฑ์ในการเลือกผู้ให้บริการและคัดเลือกผู้ให้บริการที่มีกระบวนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ
   2) ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

2. การควบคุมผู้ให้บริการ
   1) ในกรณีที่ใช้บริการด้านการพัฒนาระบบงานต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่บริษัทควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิด ในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่บริษัท (onsite service) และให้เจ้าหน้าที่บริษัทตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ remote access และปิด modem ทันทีที่การให้บริการเสร็จสิ้น เป็นต้น
   2) ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ
   3) ควรกำหนดให้ผู้บริการรายงานการปฏิบัติงาน ปัญหาต่าง ๆ และแนวทางแก้ไข
   4) ควรมีกระบวนการตรวจรับงานของผู้ให้บริการ