บทที่ 2

แนวคิดและทฤษฎีที่เกี่ยวข้อง

การศึกษาวิจัยเรื่องแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ผู้วิจัยดำเนินการทบทวนวรรณกรรมที่เกี่ยวข้องกับแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ สรุปสาระสำคัญตามลำดับ ดังนี้

1. การรักษาความมั่นคงปลอดภัยสารสนเทศ
    1.1 ความหมายของความมั่นคงปลอดภัยสารสนเทศ
    1.2 คุณลักษณะของความมั่นคงปลอดภัยสารสนเทศ
2. ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ
    2.1 ความหมายภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ
    2.2 ประเภทของภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ
3. การจัดการความมั่นคงปลอดภัยสารสนเทศ
    3.1 ความหมายของการจัดการความมั่นคงปลอดภัยสารสนเทศ
    3.2 มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ
    3.3 กระบวนการการจัดการความมั่นคงปลอดภัยสารสนเทศ
    3.4 มาตรการการจัดการความมั่นคงปลอดภัยสารสนเทศ
4. ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ
5. บริบทกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร
    5.1 ประวัติความเป็นมาของการโรงพยาบาล
    5.2 นโยบายด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ
6. งานวิจัยที่เกี่ยวข้อง
    6.1 งานวิจัยภายในประเทศ
    6.2 งานวิจัยต่างประเทศ

การรักษาความมั่นคงปลอดภัยสารสนเทศ

1. ความหมายของความมั่นคงปลอดภัยสารสนเทศ

จากการวรรณกรรมที่เกี่ยวข้อง มีความหมายของความมั่นคงปลอดภัยสารสนเทศ ดังนี้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (2553) ให้ความหมายไว้ว่า ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability)ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

วิภาวรรณ คุ้มศิริ (2552) ได้ให้ความหมายไว้ว่า การรักษาความมั่นคงปลอดภัยทางสารสนเทศ (Information Security) หมายถึง การป้องกันระบบข้อมูลข่าวสารที่เกิดจากการเข้าใช้โดยไม่ได้รับอนุญาต หรือมีการเปลี่ยนแปลงข้อมูล ในการเก็บ การประมวลผล หรือการสื่อสาร ซึ่งรวมถึงการวัดผล ในเรื่องการตรวจตรา และ ต่อต้านต่อภัยคุกคาม

พิรมล เก่งคุมพล (2555, หน้า 7) ได้ให้ความหมายไว้ว่า การรักษาความมั่นคงปลอดภัยสารสนเทศมีจุดมุ่งหมายเพื่อปกป้องข้อมูล และระบบสารสนเทศขององค์กรจากผู้ที่ไม่มีสิทธิในการเข้าถึง ในการอ่านหรือการใช้งาน การเปิดเผยข้อมูลระบบสารสนเทศ การขัดขวางการใช้งานหรือการให้บริการ รวมไปถึงการแก้ไขเปลี่ยนแปลงข้อมูล และการทำสาเนาข้อมูลอีกด้วย

ความปลอดภัยสารสนเทศตามคำจำกัดความของ U.S. National Information System Security Glossary ได้กำหนดไว้ คือ การป้องกันระบบข้อมูลในการเข้าถึงหรือแก้ไขข้อมูลที่ไม่ได้รับอนุญาต ไม่ว่าจะอยู่ในที่จัดเก็บข้อมูลหรืออยู่ระหว่างกระบวนการ โดยจะต้องไม่อนุญาตให้ผู้ที่ไม่มีสิทธิ์เข้ามาใช้บริการได้ รวมถึงการตรวจวัดระบบการจัดทำเอกสารและการตอบสนองต่อภัยคุกคามเหล่านั้น

อัครา วัฒนโยธิน (2553) ได้ให้ความหมายของการรักษาความมั่นคงปลอดภัยสารสนเทศ ไว้ว่า ความหมายของระบบรักษาความปลอดภัยข้อมูลข่าวสาร คือ มาตรการหรือแนวทางการป้องกัน และรักษาความปลอดภัยของข้อมูลข่าวสาร เพื่อสร้างความมั่นใจต่อความถูกต้องของข้อมูลรวมถึงการรักษาความลับของข้อมูลสำคัญต่างๆ และความพร้อมของข้อมูลสำหรับการปฏิบัติงาน ดังนั้นสิ่งที่ต้องคำนึงถึง หรือจุดประสงค์สำหรับระบบการรักษาความมั่นคงปลอดภัย คือ 1) การรักษาความปลอดภัยจากผู้ใช้ข้อมูล 2) การรักษาความลับของข้อมูลข่าวสาร 3) การคงสภาพของข้อมูลข่าวสาร และ 4) การรักษาสภาพของระบบเพื่อความสามารถของการใช้งาน

ซึ่งหลักการทั้ง 4 ข้อเป็นพื้นฐานสำคัญของเหตุผลและความจำเป็นในการสร้างระบบรักษาความปลอดภัยและลดความเสี่ยงของข้อมูลข่าวสาร

ว่าที่ร้อยตรี ภูมินทร์ ภูดวงสี (2550) ได้ให้ความหมายของการรักษาความปลอดภัยสารสนเทศซึ่งสอดคล้องกับแนวคิดของ อัครา วัฒนโยธิน (2553) ไว้ว่า การรักษาความมั่นคงปลอดภัยสารสนเทศ คือ การคงคุณสมบัติของความมั่นคงปลอดภัยสารสนเทศ ได้แก่ 1) การรักษาความลับของสารสนเทศ 2) การรักษาความสมบูรณ์ถูกต้องของสารสนเทศ และ 3) การรักษาความพร้อมใช้ของสารสนเทศ

จตุชัย แพงจันทร์ (2553, หน้า 4) การรักษาความมั่นคงปลอดภัยสารสนเทศ หมายถึง มาตรการที่ใช้สำหรับป้องกันผู้ที่ไม่ได้รับอนุญาตในการเข้าถึง ลบ แก้ไข หรือขัดขวางไม่ให้ผู้ที่ได้รับอนุญาตใช้งานความรู้ แนวคิด และข้อเท็จจริง

จากแนวคิดการรักษาความมั่นคงปลอดภัยสารสนเทศ ผู้วิจัยสรุปความหมายของการรักษาความมั่นคงปลอดภัยสารสนเทศ หมายถึง การป้องกันระบบสารสนเทศ ข้อมูลสารสนเทศ ไม่ให้ผู้ที่ไม่ได้รับอนุญาต สามารถเข้าถึง หรือเข้ามาทำการเปลี่ยนแปลง ไม่ว่าสถานะของข้อมูลนั้นจะถูกจัดเก็บอยู่ หรืออยู่ในกระบวนการต่างๆ โดยมีจุดประสงค์เพื่อรักษาคุณลักษณะของความมั่นคงปลอดภัยสารสนเทศ ได้แก่ 1) การรักษาความลับของข้อมูล, 2) การรักษาความสมบูรณ์ ความคงสภาพของข้อมูล และ 3) การรักษาความพร้อมใช้ของข้อมูล

2. คุณลักษณะความมั่นคงปลอดภัยสารสนเทศ

คุณลักษณะความมั่นคงปลอดภัยสารสนเทศมีนักวิชาการให้ความหมายไว้หลายท่านดังนี้

เฉลิม สุวรรณะ (2554, หน้า 17 – 18) คุณลักษณะพื้นฐานความปลอดภัยของข้อมูลหลักๆ มีอยู่ 3 อย่าง ซึ่งใช้ตัวย่อ CIA มาจากคำว่า Confidentiality Integrity Availability และยังมีองค์ประกอบอื่นๆ เพิ่มเติม คือ Authentication Authorization และ Non–repudiation (หรืออาจเรียกรวมได้ว่า CIAAAN)

ความลับของข้อมูล (Confidentiality) หมายถึง การปกป้องข้อมูล โดยมีเงื่อนไขว่าข้อมูลนั้นใครมีสิทธิ์ที่จะล่วงรู้ เข้าถึง ใช้งานได้ และการทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น อาทิเช่น ข้อมูลอีเมล์ในเมลล์บ็อกซ์ (Mail Box) ของผู้ใช้ ผู้ที่มีสิทธิ์เข้าถึงเมลล์บ็อกซ์และเปิดอ่านจดหมายได้จะต้องเป็นเจ้าของเมลล์บ็อกซ์นั้น เพียงคนเดียวเท่านั้นที่สามารถเข้าถึงและเปิดอ่านจดหมายได้

ความคงสภาพของข้อมูล (Integrity) หมายถึง การปกป้องเพื่อให้ข้อมูลไม่ถูกแก้ไข เปลี่ยนแปลง หรือถูกทำลาย ถ้าเราสามารถรักษาสภาพของข้อมูลได้ จะทำให้ข้อมูลเหล่านั้นเกิดความน่าเชื่อถือ อาทิเช่น เมื่อมีการส่งไฟล์จากผู้ใช้ต้นทางไปยังผู้ใช้ปลายทาง ไฟล์นั้นจะต้องไม่ถูกแก้ไขหรือเปลี่ยนแปลงโดยบุคคลอื่นในระหว่างทางที่ส่งมา

การรักษาความคงสภาพของข้อมูลนั้นสามารถทำได้หลายวิธี เช่นการ checksum ตัวอย่างเช่น การตรวจสอบไฟล์ที่ดาวน์โหลดมาจากเว็บไซต์ว่าตรงกับต้นฉบับหรือไม่ โดยเราสามารถทำได้โดยตรวจสอบจากค่า checksum โดยใช้ MD5 เป็นต้น

ความพร้อมใช้งานของข้อมูล (Availability) หมายถึง ข้อมูลจะต้องมีสภาพพร้อมใช้งานอยู่ตลอดเวลา อาทิเช่น เมล์เซิร์ฟเวอร์ถูกโจมตีจนไม่สามารถเข้าไปขอรับบริการจากเมล์เซิร์ฟเวอร์นั้นได้ ต้องรอจนกว่าผู้ดูแลระบบจะแก้ไขเพื่อให้ระบบสามารถกลับมาให้บริการได้เหมือนเดิม แต่ถ้าหากระบบเมล์นี้ออกแบบให้มีระบบสำรอง (Mail Backup) ที่สามารถทำงานแทนเมล์เซิร์ฟเวอร์ตัวหลักได้ทันที ผู้ใช้ก็จะสามารถใช้บริการระบบสำรองนี้ได้ทันที

การพิสูจน์ทราบตัวตนที่แท้จริง (Authentication) เนื่องจากการระบุตัวบุคคลนั้นจะต้องใช้กระบวนการพิสูจน์ตัวตนที่แท้จริงเพื่อให้ทราบว่าบุคคลผู้นั้นเป็นตัวจริงหรือไม่ อาทิเช่น การล็อกอินเข้าสู่ระบบลงทะเบียนวิชาของนักศึกษา สมาชิก (นักศึกษา) จะต้องใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเป็นการพิสูจน์ทราบว่า

เป็นผู้ใช้คนนั้นจริงๆ และการพิสูจน์ทราบตัวตนก็มีอยู่หลากหลายวิธี เช่น สิ่งที่คุณรู้ (What you know ?) เช่น การใช้ยูสเซอร์เนม และ พาสเวิร์ด เป็นต้น, สิ่งที่คุณมี (What you have ?) เช่น การใช้บัตรประจำตัว เป็นต้น, สิ่งที่คุณเป็น (What you are ?) เช่น การสแกนลายนิ้วมือ, เสียงพูด เป็นต้น

อาจผสมผสานวิธีการพิสูจน์ทราบตัวตนมากกว่า 1 วิธีเพื่อประสิทธิภาพในการพิสูจน์ตัวตน เช่น การกดเงินจากเครื่องกดเงินอัตโนมัติ (ATM) ที่จะต้องใช้ “สิ่งที่คุณมี” คือ บัตรสำหรับกดเงินอัตโนมัติ และต้องใช้ “สิ่งที่คุณรู้” นั่นคือรหัสผ่าน หรือการใช้บริการโอนเงินผ่านอินเทอร์เน็ต เพื่อการโอนเงิน คุณจะต้องใช้ “สิ่งที่คุณรู้” คือ ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเข้าใช้งานเว็บไซต์ และต้องใช้ “สิ่งที่คุณมี” คือ โทรศัพท์มือถือ เพื่อใช้รับรหัสผ่านสำหรับใช้ครั้งเดียว (OPT: One Time Password) เพื่อใช้กรอกในเว็บไซต์เพื่อยืนยันการทำรายการ

การอนุญาตให้เข้าใช้งานและลำดับสิทธิในการเข้าถึง (Authorization)

หลังจากได้มีการพิสูจน์ตัวตนแล้ว ระบบจะทำการอนุญาตให้ผู้ใช้คนนั้นๆเข้าใช้งานตามสิทธิของผู้ใช้งานคนนั้นๆ ซึ่งการให้สิทธิ์สามารถแบ่งได้เป็นหลายระดับ อาทิเช่น ผู้ใช้ระดับสูง เช่น ผู้แลระบบ (Administrator) สามารถเปลี่ยนแปลง/แก้ไขข้อมูลได้ทั้งหมด ผู้ใช้งานที่เป็นสมาชิกไปอาจจะแก้ไขข้อมูลได้บางส่วน หรือ ผู้ใช้ระดับ Guest สามารถอ่านข้อมูลได้อย่างเดียว เป็นต้น

การไม่สามารถปฏิเสธความรับผิดชอบ (Non–repudiation)

คือการปฏิเสธไม่ได้ถึงความรับผิดชอบ เช่น ปฏิเสธไม่ได้ว่าข้อความนี้ถูกส่งโดยผู้ใช้งานคนนี้ อาทิเช่น สมาชิกในเว็บบอร์ดที่มีการโพสต์ (Post) ข้อความว่าร้ายผู้อื่นลงไปในระบบเว็บบอร์ด จะต้องมีการบันทึกและแสดงชื่อผู้ใช้ซึ่งจะได้จากการพิสูจน์ตัวตน พร้อมกับข้อความที่โพสต์เพื่อใช้ยืนยันว่าข้อความดังกล่าวถูกโพสต์โดยผู้ใช้ผู้นั้นไม่สามารถปฏิเสธความรับผิดชอบได้

แนวคิดของ พิรมล เก่งคุมพล (2555, หน้า 7) เกี่ยวกับคุณลักษณะความมั่นคงปลอดภัย สอดคล้องกับแนวคิด เฉลิม สุวรรณะ (2554, หน้า 17 – 18) ในหัวข้อ Confidentiality Integrity Availability แต่ไม่มีหัวข้อ Authentication, Authorization, Non–repudiation มีรายละเอียดดังนี้

ความลับของข้อมูล (Confidentiality) หมายถึง การรักษาความลับของข้อมูลโดยจะอนุญาตให้เข้าถึงและเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ซึ่งเป็นการ

ปกป้องข้อมูลจากผู้ที่ไม่ได้รับอนุญาตโดยมีกลไกที่ใช้ในการรักษาความลับ เช่น กลไกการเข้ารหัสข้อมูล (Cryptography หรือ Encryption) เป็นกลไกในการรักษาความลับของข้อมูลนั้นๆ เพื่อจัดข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านหรือเข้าใจได้ถ้าไม่รู้วิธีการและกุญแจ (Key) หรือรหัสผ่าน (Password) ที่ใช้ในการเข้ารหัสและถอดรหัสนั้น ซึ่งการรักษากุญแจหรือรหัสผ่านจะต้องใช้กลไกการควบคุมการเข้าถึง (Access Control) เป็นกลไกควบคุมการเข้าถึงระบบ เพื่อให้พิสูจน์ทราบตัวตนของผู้ที่เข้ามาใช้งานระบบว่าเป็นคนที่ได้รับอนุญาตหรือไม่ และทั้งสองกลไกนี้ สามารถใช้งานพร้อมกันได้ หากกลไกควบคุมการเข้าถึงทำงานผิดพลาดหรือล้มเหลว ก็ยังมีกลไกการเข้ารหัสข้อมูลรักษาความลับของข้อมูลนั้นๆ ได้

ความคงสภาพของข้อมูล (Integrity) หมายถึง การรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความเชื่อถือได้ ซึ่งข้อมูลนั้นจะต้องไม่ถูกแก้ไขเปลี่ยนแปลงจากแหล่งที่มา และแหล่งที่มาของข้อมูลนั้นต้องเชื่อถือได้ ความคงสภาพของข้อมูลแบ่งออกเป็น 2 แบบ ได้แก่ ความสมบูรณ์ของข้อมูล (Data Integrity) และความสมบูรณ์ของระบบ (System Integrity) ความสมบูรณ์ของข้อมูล หมายถึง ข้อมูลสารสนเทศและโปรแกรมการใช้งานขององค์กรจะต้องไม่ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ความสมบูรณ์ของระบบหมายถึง ระบบจะต้องไม่ถูกแก้ไขเปลี่ยนแปลงด้วยประการใดๆ โดยไม่ได้รับอนุญาต เช่น การเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต, การแก้ไขเปลี่ยนแปลงหรือลบข้อมูลโดยไม่สามารถตรวจสอบตัวบุคคลที่เป็นผู้กระทำการได้

สภาพความพร้อมใช้ของข้อมูล (Availability) หมายถึง การรักษาระบบให้อยู่ในสภาพที่มีความพร้อมต่อการใช้งานและสามารถให้บริการได้ตลอดเวลา หรือหากมีช่วงหยุดให้บริการ เช่น การหยุดการให้บริการเนื่องจากการตรวจสอบ การเปลี่ยนแปลง หรือการบำรุงรักษาระบบ ก็ต้องอยู่ในช่วงเวลาหรือช่วงระยะเวลาตามหลักเกณฑ์ที่ยอมรับได้ แต่หากเป็นการหยุดให้บริการซึ่งมีสาเหตุจากความล้มเหลวหรือข้อผิดพลาดในการทำงานของฮาร์ดแวร์หรือซอฟต์แวร์ รวมไปถึงการที่ระบบไม่สามารถทำงานได้เนื่องจากการถูกโจมตีต่างๆ อันเป็นการทำให้ระบบสูญเสียสภาพความพร้อมใช้ไป ก็ไม่สามารถนับเป็นสภาพความพร้อมใช้ได้ เป็นต้น

แนวความคิดของ วราภรณ์ ธวิทย์ชัยพร (2549, หน้า 9–10) เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ สอดคล้องกับแนวคิดของ พิรมล เก่งคุมพล (2555, หน้า 7) ซึ่งกล่าวไว้ว่า

การรักษาความปลอดภัยสารสนเทศนั้นจัดทำขึ้นเพื่อให้เกิดเป็นคุณสมบัติของความปลอดภัยสารสนเทศ 3 ประการ ได้แก่ 1) ความมั่นใจในการเข้าถึงข้อมูลได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หรือความสามารถในการที่จะรักษาข้อมูลให้เป็นความลับ (Confidentiality) 2) การรักษาและปกป้องความสมบูรณ์ถูกต้องของข้อมูลและกระบวนการ (Integrity) 3) การจัดการความสะดวกและความพร้อมในการใช้ข้อมูลสำหรับผู้ที่ได้รับการอนุญาต (availability)

จตุชัย แพงจันทร์ (2553, หน้า 8 –13) ได้ให้แนวคิดของคุณลักษณะของความมั่นคงปลอดภัยสารสนเทศซึ่งสอดคล้องกับ เฉลิม สุวรรณะ แต่มีการใช้คำที่แตกต่างกันคือ การไม่สามารถปฏิเสธความรับผิดชอบ (Non–repudiation) ซึ่งมีความหมายใกล้เคียงกับคำว่าการระบุตัวตน (Identification) และมีเนื้อหาที่เพิ่มขึ้น ได้แก่ ความเป็นส่วนตัว (Privacy) การตรวจสอบได้ (Accountability) โดยมีรายละเอียดดังนี้

ความลับ (Confidentiality) หมายถึง การทำให้สารสนเทศสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาต กลไกที่ใช้ในการรักษาความลับ คือ การเข้ารหัสข้อมูล (Cryptography หรือ Encryption) ซึ่งเป็นการจัดข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านหรือเข้าใจได้ถ้าไม่รู้วิธีการและคีย์ในการเข้ารหัส และยังมีกลไกอื่นที่ใช้สำหรับปกป้องความลับของสารสนเทศที่จัดเก็บไว้ คือ กลไกการควบคุมการเข้าถึง (Access Control) กลไกการควบคุมนี้จะพิสูจน์ทราบตัวตนของผู้ที่เข้ามาใช้งานระบบว่าเป็นผู้ที่ได้รับอนุญาตหรือไม่

ความถูกต้อง (Integrity) หมายถึง การรักษาความคงสภาพสารสนเทศจากแหล่งที่มา หรือไม่ได้ถูกแก้ไข โดยผู้ที่ไม่ได้รับอนุญาต กลไกในการรักษาความถูกต้องของข้อมูลนั้นประกอบด้วย 2 ส่วน คือ การป้องกัน (Prevention) และ การตรวจสอบ (Detection) โดยกลไกในการป้องกันนี้มีจุดหมายเพื่อรักษาความถูกต้องของข้อมูล ซึ่งทำได้โดยการป้องกันความพยายามที่จะเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต หรือความพยายามที่จะเปลี่ยนแปลงข้อมูลในรูปแบบที่ไม่ถูกต้อง หรือได้รับอนุญาต ข้อแตกต่างระหว่างความพยายามทั้งสองประเภทนี่สำคัญ โดยในความพยายามข้อแรกนั้นเป็นความพยายามที่จะแก้ไข หรือเปลี่ยนแปลงข้อมูลโดยที่ผู้ที่พยายามนั้นไม่ได้รับอนุญาต แต่ความพยายามอีกข้อหนึ่งนั้นเกิดจากการที่ผู้ที่ได้รับอนุญาตพยายามที่จะแก้ไขข้อมูลนอกเหนือจากขอบเขตที่ตัวเองมีสิทธิ์ กลไกในการป้องกันผู้ที่ไม่ได้รับอนุญาตคือ การพิสูจน์ตัวตน (Authentication) และการควบคุมการเข้าถึง (Access Control) ส่วนกลไกที่ใช้ป้องกันการกระทำเกินกว่าสิทธิ์ที่ได้รับ คือ การตรวจสอบสิทธิ์ (Authorization)

ความพร้อมใช้งาน (Availability) หมายถึง การทำให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงสารสนเทศได้ ส่วนหนึ่งของความพร้อมใช้ที่เกี่ยวข้องกับการรักษาความปลอดภัยคือ อาจมีผู้ไม่ประสงค์ดีพยายามที่จะทำให้ไม่สามารถเข้าถึงสารสนเทศได้โดยการทำให้ระบบไม่สามารถใช้งานได้ การออกแบบระบบนั้นส่วนใหญ่จะใช้ข้อมูลทางด้านสถิติเกี่ยวกับรูปแบบหรือพฤติกรรมในการใช้งานระบบของผู้ใช้ ระบบจะถูกออกแบบเพื่อให้เหมาะกับสภาพแวดล้อมดังกล่าว ดังนั้น กลไกในการรักษาความพร้อมใช้งานนั้นจะทำงานในกรณีที่ระบบไม่ได้ทำงานในสภาพที่ปกติหรือที่ออกแบบไว้ ซึ่งถ้ากลไกนี้ไม่ทำงานส่วนใหญ่จะส่งผลให้ระบบล่ม หรือไม่พร้อมใช้งาน

ความเป็นส่วนตัว (Privacy) ข้อมูลที่องค์กรรวบรวม จัดเก็บ และใช้งานนั้นควรถูกใช้เพื่อจุดประสงค์ที่เจ้าของข้อมูลระบุตอนที่เก็บรวบรวมเท่านั้น แต่ถ้าใช้เพื่อจุดประสงค์อื่นก็แสดงว่าเป็นการละเมิดสิทธิส่วนบุคคลของเจ้าของข้อมูลนั้น บางองค์กรใช้ข้อมูลส่วนบุคคลในทางที่ผิด หรือบางทีอาจขายข้อมูลเหล่านี้ให้กับบุคคลหรือองค์กรอื่นโดยที่เจ้าของข้อมูลไม่รับรู้ ปัจจุบันข้อมูลส่วนบุคคลนั้นสามารถค้นหาและรวบรวมได้จากหลายๆ แหล่ง และเมื่อรวบรวมได้แล้วอาจถูกใช้ในทางที่เจ้าของนั้นไม่เห็นด้วย หรือไม่พึงประสงค์

การระบุตัวตน (Identification) ระบบสารสนเทศนั้นจะต้องสามารถระบุตัวตนของผู้ใช้แต่ละคนที่ใช้งานระบบได้ การระบุตัวตนเป็นขั้นแรกในการที่จะสามารถเข้าถึงข้อมูลในขั้นความลับ และเป็นพื้นฐานสำหรับขั้นตอนต่อไปคือการพิสูจน์ทราบตัวตน (Authentication) และการพิสูจน์สิทธิ์ (Authorization) เมื่อใช้การระบุตัวตนร่วมกันเป็นส่วนสำคัญในการสร้างระดับในการเข้าถึงระบบ หรือการอนุญาตสิทธิ์มากน้อยแค่ไหนในการใช้งานระบบ รูปแบบของการระบุตัวตนที่นิยมใช้ในระบบคอมพิวเตอร์มากที่สุดคือการใช้ยูสเซอร์เนม (Username)

การพิสูจน์ทราบตัวตน (Authentication) การพิสูจน์ทราบตัวตนนั้นเกิดขึ้นเมื่อระบบควบคุมพิสูจน์ว่าผู้ใช้คือคนที่ผู้ใช้บอกหรือไม่ เช่น ถ้าผู้ใช้ระบุยูสเซอร์เนมแล้วก็ต้องสามารถระบุรหัสผ่านที่คู่กับยูสเซอร์เนมนั้นได้ หรืออีกตัวอย่างหนึ่งคือ การใช้ใบรับรองอิเล็กทรอนิกส์ในการสร้างการเชื่อมต่อแบบ SSL (Secure Socket Layer) เพื่อพิสูจน์ว่าเซิร์ฟเวอร์ที่เชื่อมต่ออยู่นั้นใช่เครื่องที่ต้องการเชื่อมต่อจริงๆ

การอนุญาตใช้งาน (Authorization) การอนุญาตใช้งานเป็นขั้นตอนหลังจากที่มีการพิสูจน์ทราบตัวตนแล้ว ขั้นตอนต่อไปคือ การตรวจสอบสิทธิ์ของผู้ใช้หรือ

ไคลเอนท์ (Client) นั้นว่าได้มีการกำหนดสิทธิ์ให้ใช้งานระบบได้ในระดับไหน ซึ่งสิทธิ์นั้นประกอบด้วย การเข้าถึงหรืออ่าน การแก้ไข และการลบข้อมูล เช่น การใช้ ACL (Access Control List) หรือการจัดกลุ่มของผู้ใช้ในระบบ เช่น กลุ่มผู้ใช้ในระดับผู้ดูแลระบบ (Administrator หรือ Root) นั้นมีสิทธิ์สูงสุด แต่ถ้าเป็นผู้ใช้ทั่วไปก็จะมีสิทธิ์ที่ต่ำลงมาแล้วแต่จะกำหนด อีกตัวอย่างหนึ่งคือ ระบบฐานข้อมูล หลังจากระบบพิสูจน์ทราบตัวตนแล้ว ขั้นตอนต่อไปก็เป็นการตรวจสอบสิทธิ์ว่าผู้ใช้คนนั้นมีสิทธิ์ในการอ่าน เขียน สร้าง และลบหรือไม่

การตรวจสอบได้ (Accountability) ความสามารถในการตรวจสอบการใช้งานระบบได้ ก็เป็นอีกส่วนที่สำคัญเพราะเป็นการรับรองว่าทุกๆ กิจกรรมหรือทุกเหตุการณ์ที่เกิดขึ้นนั้นสามารถตรวจสอบได้ว่าเกิดขึ้นเพราะใครหรือเกิดขึ้นจากโพรเซสไหน ยกตัวอย่างเช่น การเก็บล็อก (Logs) เกี่ยวกับกิจกรรมต่างๆ ที่ผู้ใช้แต่ละคนใช้งานระบบเป็นต้น

จากแนวคิดเกี่ยวกับคุณลักษณะความมั่นคงปลอดภัยสารสนเทศ ผู้วิจัยสรุปคุณลักษณะความมั่นคงปลอดภัยสารสนเทศประกอบด้วย 8 ด้าน ดังนี้

การรักษาความลับ (Confidentiality) การรักษาความลับ หมายถึง การปกป้องสารสนเทศจากผู้ที่ไม่ได้รับอนุญาตให้เข้าถึง และเปิดเผยได้เฉพาะผู้ที่ได้รับการอนุญาตเท่านั้น โดยกลไกที่ใช้ในการรักษาความลับคือ การเข้ารหัสข้อมูล (Encryption) ซึ่งเป็นการจัดข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถทำความเข้าใจได้หากไม่ทราบวิธีการ (Algorithm) และคีย์ (Key) ในการเข้ารหัส และมีอีกกลไกคือ กลไกการควบคุมการเข้าถึง (Access Control) โดยกลไกนี้จะอนุญาตให้เข้าถึงสารสนเทศได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

การคงสภาพของข้อมูล (Integrity) ความคงสภาพของข้อมูล (Integrity) หมายถึง การรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความเชื่อถือได้ ไม่ถูกแก้ไขเปลี่ยนแปลงจากแหล่งที่มา หรือไม่ได้ถูกแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต โดยกลไกในการป้องกันการแก้ไขจากผู้ที่ไม่ได้รับอนุญาต คือ การพิสูจน์ตัวตน (Authentication) และการควบคุมการเข้าถึง (Access Control) ส่วนกลไกที่ใช้ป้องกันการกระทำเกินกว่าสิทธิ์ที่ได้รับ คือ การตรวจสอบสิทธิ์ (Authorization)

ความพร้อมใช้งาน (Availability) ความพร้อมใช้งาน (Availability) หมายถึง การรักษาข้อมูลให้อยู่ในสภาพที่มีความพร้อมต่อการใช้งาน และสามารถให้บริการแก่ผู้ที่ได้รับอนุญาตได้ตลอดเวลา

การระบุตัวตน (Identification) การระบุตัวตน (Identification) หมายถึง ระบบสารสนเทศจะต้องสามารถระบุตัวตนของผู้ใช้แต่ละคนที่ใช้งานระบบได้

การพิสูจน์ทราบตัวตน (Authentication) การพิสูจน์ทราบตัวตน (Authentication) หมายถึง การพิสูจน์เพื่อให้ทราบว่าบุคคลนั้นเป็นตัวจริงหรือไม่ โดยการพิสูจน์ทราบตัวตนมีอยู่หลายวิธี เช่น 1) สิ่งที่คุณรู้ (What you know ?) เช่น การใช้ยูสเซอร์เนม และ พาสเวิร์ด 2) สิ่งที่คุณมี (What you have ?) เช่น การใช้บัตรประจำตัว 3) สิ่งที่คุณเป็น (What you are ?) เช่น การสแกนลายนิ้วมือ เสียงพูด

การอนุญาตใช้งาน (Authorization) การอนุญาตใช้งาน (Authorization) หมายถึง การตรวจสอบสิทธิ์ของผู้ใช้ว่าได้มีการกำหนดสิทธิ์ให้ใช้งานสารสนเทศได้ในระดับใด และจะต้องอนุญาตให้ใช้งานได้ตามสิทธิ์นั้นเท่านั้น

การตรวจสอบได้ (Accountability) ความสามารถในการตรวจสอบการใช้งานระบบ เป็นการรับรองว่าทุกๆ กิจกรรมหรือทุกเหตุการณ์ที่เกิดขึ้นนั้นสามารถตรวจสอบได้ว่าเกิดขึ้นเพราะแหล่งที่มาใด ยกตัวอย่างเช่น การเก็บล็อก (Logs) การใช้งานระบบสารสนเทศ เป็นต้น

ความเป็นส่วนตัว (Privacy) สารสนเทศที่ถูกรวบรวม จัดเก็บ และใช้งานนั้นควรถูกใช้เพื่อจุดประสงค์ที่เจ้าของสารสนเทศระบุตอนที่เก็บรวบรวมเท่านั้น แต่ถ้าใช้เพื่อจุดประสงค์อื่นก็แสดงว่าเป็นการละเมิดสิทธิส่วนบุคคลของเจ้าของสารสนเทศนั้น

ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ

การทบทวนวรรณกรรมเกี่ยวกับภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ผู้วิจัยแบ่งเป็นหัวข้อย่อย คือ ความหมายของภัยคุกคามความมั่นคงปลอดภัย และประเภทของภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ

1. ความหมายภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ

จากการทบทวนวรรณกรรมที่เกี่ยวข้อง มีนักวิชาการหลายท่านได้ให้ความหมายของภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ไว้ดังนี้

จตุชัย แพง จันทร์ (2553, หน้า 13) ให้ความหมายของภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ หมายถึง สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อคุณลักษณะของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน ภัยคุกคามความมั่นคงอาจจะไม่เกิดขึ้นหากมีการป้องกันที่ดี หรือถ้ามีการเตรียมการที่ดีเมื่อมีเหตุการณ์เกิดขึ้นก็จะช่วยลดความเสียหายได้ การกระทำที่อาจก่อให้เกิดความเสียหาย เรียกว่า การโจมตี (Attack) ส่วนผู้ที่ทำการโจมตี หรือผู้ที่เป็นเหตุให้เหตุการณ์ดังกล่าวเกิดขึ้นจะเรียกว่าผู้โจมตี (Attacker) หรือเรียกว่าแฮคเกอร์ (Hacker) หรือแคร็คเกอร์ (Cracker)

Whiteman Micheal E., Mattord Herbert J. (2011, pp. 42–43) ได้ให้ความหมายของภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ดังนี้ ภัยคุกคาม คือ วัตถุ สิ่งของ ตัวบุคคล หรือสิ่งอื่นใดที่เป็นตัวแทนของการกระทำอันตรายต่อทรัพย์สิน

จากการทบทวนวรรณกรรมที่เกี่ยวข้อง ผู้วิจัยสรุปว่า ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ หมายถึง วัตถุ สิ่งของ หรือสิ่งใดๆ ที่ก่อให้เกิดความเสียหายต่อคุณลักษณะความมั่นคงปลอดภัยสารสนเทศด้านใดด้านหนึ่ง หรือมากกว่าหนึ่งด้าน

2. ประเภทของภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ

จากการศึกษาค้นคว้าเอกสารงานวิจัยที่เกี่ยวข้อง มีผู้อธิบายถึงประเภทของภัยคุกคามความมั่นคงปลอดภัยระบบสารสนเทศ ไว้ดังนี้

จตุชัย แพงจันทร์ (2553, หน้า 13) ได้ให้แนวความคิดเกี่ยวกับประเภทภัยคุกคามความมั่นคงปลอดภัยของข้อมูลสามารถแบ่งได้ 4 ประเภท คือ 1) การเปิดเผย (Disclosure) คือ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือข้อมูลนั้นถูกเปิดเผยให้กับผู้ที่ไม่ได้รับอนุญาต 2) การหลอกลวง (Deception) คือ การให้ข้อมูลที่เป็นเท็จ 3) การขัดขวาง (Disruption) คือ การทำลายข้อมูล หรือกันไม่ให้กระทำต่อข้อมูลอย่างถูกต้อง และ 4) การควบคุมระบบ (Usurpation) คือ การเข้าควบคุมบางส่วนหรือทั้งระบบโดยไม่ได้รับอนุญาต

Whiteman Micheal E., Mattord Herbert J. (2011, pp. 44–65) ให้แนวคิดเกี่ยวกับประเภทของภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ไว้ดังนี้

การละเมิดทรัพย์สินทางปัญญา (Compromises to intellectual property) ทรัพย์สินทางปัญญา (IP) เป็นส่วนหนึ่งของการดำเนินธุรกิจ ซึ่งทรัพย์สินทางปัญญาเป็นผลงานของผู้ที่เป็นเจ้าของความคิด และเป็นทรัพย์สินอีกชนิดหนึ่ง ได้แก่ ลิขสิทธิ์ เครื่องหมายการค้าและสิทธิบัตร คุณสมบัติของทรัพย์สินทางปัญญาอย่างหนึ่งคือ มีการระบุรหัสบ่งชี้ไว้อย่างเหมาะสม บ่อยครั้งที่องค์กรซื้อหรือทำสัญญาเช่าทรัพย์สินทางปัญญา

จากองค์กรอื่น ต้องปฏิบัติตามข้อตกลงที่ได้ทำไว้เพื่อความยุติธรรมและความรับผิดชอบในการนำไปใช้ ส่วนใหญ่การละเมิดทรัพย์สินทางปัญญาจะเป็นการทำสำเนาซอฟต์แวร์ที่มีลิขสิทธิ์

การโจมตีด้วยซอฟต์แวร์ (Deliberate Software Attacks) การโจมตีซอฟต์แวร์ เกิดขึ้นโดยการออกแบบซอฟต์แวร์ให้โจมตีระบบจากคนๆ เดียวหรือจากกลุ่มคนที่มีซอฟต์แวร์ที่ก่อความเสียหาย ทำลาย หรือ ปฏิเสธการบริการของระบบเป้าหมาย ซอฟต์แวร์ที่นิยมคือ Malicious Code หรือ Malicious Software มักจะเรียกว่า มัลแวร์ (Malware) มีมากมาย อาทิ ไวรัส (Viruses) เวิร์ม (Worms) ม้าโทรจัน (Trojan Horses) Logic bombs และ ช่องทางลับ (Back doors)

คุณภาพของผู้ให้บริการที่ไม่เพียงพอ (Deviations in Quality of Service) ระบบสารสนเทศขององค์กรจะประสบความสำเร็จได้นั้นต้องได้รับการสนับสนุนจากระบบงานอื่นๆ ร่วมด้วย เช่น โรงไฟฟ้า เครือข่ายโทรคมนาคม ผู้จัดจำหน่าย ผู้ให้บริการ เจ้าหน้าที่ด้านต่างๆ ซึ่งระบบสนับสนุนเหล่านี้อาจหยุดการให้บริการได้หากเกิดเหตุการณ์ พายุ พนักงานป่วย หรือเหตุฉุกเฉินใดๆ ส่งผลให้การให้บริการระบบสารสนเทศขององค์กรไม่สามารถให้บริการได้ตามปกติ

การจารกรรมหรือการบุกรุก (Espionage or Trespass) การจารกรรมและการบุกรุกระบบสารสนเทศเป็นที่รู้จักอย่างแพร่หลาย ทั้งในรูปแบบในอิเล็กทรอนิกส์และกระทำโดยมนุษย์ที่สามารถเข้าถึงข้อมูลที่เป็นความลับ เมื่อมีบุคคลที่ไม่ได้รับอนุญาตได้ทำการรุกล้ำและพยายามเข้าถึงข้อมูลขององค์กรที่มีการป้องกัน ซึ่งพฤติกรรมดังกล่าวเป็นการจารกรรมหรือการบุกรุกโดยเจตนา ผู้บุกรุกระบบสารสนเทศสามารถที่จะใช้วิธีการต่างๆ ในการเข้าถึงข้อมูลที่เก็บรักษาอยู่ภายในระบบสารสนเทศได้

ภัยธรรมชาติ (Forces of Nature) ภัยธรรมชาติเป็นภัยคุกคามที่อันตรายมาก เพราะเป็นสิ่งที่มนุษย์ไม่สามารถควบคุมได้ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว และฟ้าผ่า รวมถึงภูเขาไฟระเบิด ทั้งหมดนี้ไม่เพียงแต่สร้างความยุ่งยากในการใช้ชีวิตประจำวัน ยังสร้างปัญหาให้กับระบบคอมพิวเตอร์ทั้งหน่วยเก็บข้อมูล สัญญาณการสื่อสารต่างๆ ส่งผลเสียโดยรวมต่อระบบสารสนเทศขององค์กร

ข้อผิดพลาดจากการกระทำของมนุษย์ (human error or failure) ภัยคุกคามประเภทนี้มีการกระทำโดยไม่มีเจตนา หรือ มีเจตนามุ่งร้ายต่อสารสนเทศขององค์กร โดยเมื่อเข้าใช้ระบบสารสนเทศแล้ว ผู้ใช้ระบบอาจทำงานผิดพลาด เนื่องจากขาด

ความชำนาญ ขาดการฝึกอบรม และการสันนิษฐานด้วยตนเองอย่างไม่ถูกต้อง สิ่งเหล่านี้สามารถสร้างความเสียหายให้แก่สารสนเทศขององค์กร

การกรรโชกข้อมูลสารสนเทศ (Information Extortion) การขู่กรรโชกในการเปิดเผยข้อมูลที่เป็นความลับ เกิดขึ้นจากการที่ข้อมูลที่เป็นความลับที่จัดเก็บอยู่ในระบบถูกขโมยไปอาจจะเป็นผู้บุกรุกจากภายนอกหรือผู้ที่มีหน้าที่ดูแลรักษาข้อมูลภายในองค์กร โดยมีการเรียกร้องค่าตอบแทนหรือค่าไถ่ (Ransom) แลกกับการที่จะไม่เปิดเผยข้อมูลความลับที่ได้ขโมยมา (Black Mail)

การจัดทำแผนและนโยบายขององค์กรที่ไม่สมบูรณ์ (Missing, Inadequate, or Incomplete Organizational Policy or Planning) การจัดทำนโยบายระบบสารสนเทศขององค์กรที่ไม่สมบูรณ์ ไม่เพียงพอ หรือตกหล่น ส่งผลให้ระบบสารสนเทศขององค์กรมีช่องโหว่ที่จะก่อให้เกิดการสูญเสีย ถูกโจมตี หรือถูกเปิดเผยสารสนเทศขององค์กร และยังเป็นการเปิดช่องโหว่ทำให้ภัยคุกคามอื่นๆ เข้ามาคุกคามระบบสารสนเทศขององค์กร

มาตรการควบคุมที่ไม่สมบูรณ์ (Missing, Inadequate, or Incomplete Controls) มาตรการควบคุมที่ไม่สมบูรณ์ ไม่เพียงพอ หรือตกหล่น เช่น มาตรการควบคุมที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย เป็นต้น ส่งผลให้เกิดการสูญเสียเมื่อมีการคุกคามระบบสารสนเทศขององค์กร

การก่อวินาศกรรมหรือการทำลาย (Sabotage or Vandalism) ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศจากการก่อวินาศกรรมหรือการทำลาย เป็นการก่อวินาศกรรมต่อระบบสารสนเทศหรือธุรกิจ หรือการทำลายทรัพย์สินซึ่งก่อให้เกิดความเสียหาย โดยการสร้างความเสียหายนั้นไม่จำเป็นต้องเป็นความเสียหายต่อทรัพย์สินเพียงอย่างเดียว การทำลายภาพพจน์ที่ดีขององค์กร ก็เป็นการสร้างความเสียหายร้ายแรงต่อองค์กรเช่นกัน

การโจรกรรม (Theft) ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศจากการโจรกรรม เป็นการครอบครองทรัพย์สินผู้อื่นโดยผิดกฎหมาย ซึ่งทรัพย์สินที่สามารถถูกโจรกรรมได้ คือ ทรัพย์สินทางกายภาพ (Physical Property) ทรัพย์สินที่อยู่ในลักษณะอิเล็กทรอนิกส์ (Electronic Property) และทรัพย์สินทางปัญญา (Intellectual Property)

ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (Technical Hardware Failures or Errors) ภัยคุกคามจากข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ เกิดจากที่ผู้ผลิตนำอุปกรณ์ที่มีปัญหาออกมาจำหน่ายสู่ตลาด ทำให้องค์กรที่นำอุปกรณ์เหล่านั้นไปใช้งาน ได้รับผล

กระทบจากการทำงานผิดพลาดของอุปกรณ์ ส่งผลให้ระบบสารสนเทศไม่สามารถให้บริการได้ตามปกติ

ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ (Technical Software Failures or Errors) การจำหน่ายซอฟต์แวร์ก่อนที่จะตรวจพบจุดบกพร่อง ทำให้การนำซอฟต์แวร์นั้นไปใช้งานเกิดความผิดพลาด ส่งผลต่อการให้บริการระบบสารสนเทศขององค์กร หรือในบางครั้งข้อผิดพลาดของซอฟต์แวร์เกิดจากโปรแกรมเมอร์สร้างช่องทางลับไว้ เป็นเหตุให้เกิดความเสียหายโดยสามารถเข้าสู่โปรแกรมได้โดยปราศจากการตรวจสอบด้านความมั่นคงปลอดภัย เป็นการฝ่าฝืนแนวทางในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร

เทคโนโลยีล้าสมัย (Technological Obsolescence) โครงสร้างพื้นฐานของระบบสารสนเทศที่ล้าสมัย ทำให้ระบบสารสนเทศไม่น่าเชื่อถือและมีความเสี่ยง โดยเทคโนโลยีที่ล้าสมัยจะไม่ได้รับการปรับปรุงจากผู้จำหน่ายทำให้เสี่ยงต่อภัยคุกคามที่มีต่อระบบสารสนเทศ ซึ่งส่งผลต่อการให้บริการของระบบสารสนเทศขององค์กร

เศรษฐพงศ์ มะลิสุวรรณ (2552, หน้า 5-19) ได้ให้แนวคิดเกี่ยวกับประเภทของภัยคุกคามความมั่นคงปลอดภัยสารสนเทศไว้ 12 ประเภท ดังนี้

ข้อผิดพลาดจากการกระทำของมนุษย์ (Acts of human error or failure) ภัยคุกคามประเภทนี้อาจเป็นการกระทำโดยไม่มีเจตนา หรือมีเจตนามุ่งร้ายโดยผู้ใช้ที่มีสิทธิเข้าใช้ระบบสารสนเทศ เมื่อผู้ใช้ระบบทำงานผิดพลาด เนื่องจากขาดความชำนาญ ขาดการฝึกอบรม และการสันนิษฐานคาดเดาที่ไม่ถูกต้อง สิ่งเหล่านี้สามารถสร้างความเสียหายอย่างมาก การคุกคามที่อันตรายที่สุดต่อความปลอดภัยของสารสนเทศองค์กร คือ พนักงานขององค์กรเองเพราะพนักงานใช้สารสนเทศในการดำเนินกิจกรรมทางธุรกิจขององค์กรอยู่เสมอ

การละเมิดทรัพย์สินทางปัญญา (Compromises to intellectual property) ทรัพย์สินทางปัญญา (IP) เป็นส่วนหนึ่งของการดำเนินธุรกิจ ซึ่งทรัพย์สินทางปัญญา และเป็นทรัพย์อีกชนิดหนึ่ง ได้แก่ ลิขสิทธิ์ เครื่องหมายการค้า และสิทธิบัตร ส่วนใหญ่การละเมิดทรัพย์สินทางปัญญาจะเป็นการทำสำเนาซอฟต์แวร์ที่มีลิขสิทธิ์ ซึ่งเป็นการกระทำที่ผิดกฎหมาย

การบุกรุก (Deliberate Acts of Trespass) การบุกรุกจากภายนอกเป็นสิ่งที่ได้รับการกล่าวถึงอย่างมาก ทั้งในรูปแบบที่เป็นอิเล็กทรอนิกส์ และกระทำโดย

คนที่สามารถเข้าถึงข้อมูลที่เป็นความลับโดยทางกายภาพ ซึ่งพฤติกรรมดังกล่าวเป็นการบุกรุกโดยเจตนา ผู้บุกรุกสามารถที่จะใช้วิธีการต่างๆ ในการเข้าถึงข้อมูลที่เก็บรักษาอยู่ภายในระบบสารสนเทศ

การกรรโชกข้อมูลสารสนเทศ (Deliberate Acts of Information Extortion) การขู่กรรโชกในการเปิดเผยข้อมูลที่เป็นความลับเกิดขึ้นจากการที่ข้อมูลที่เป็นความลับที่จัดเก็บอยู่ในระบบถูกขโมยไปอาจจะเป็นผู้บุกรุกจากภายนอกหรือผู้ที่มีหน้าที่ดูแลรักษาข้อมูลภายในองค์กร โดยมีการเรียกร้องค่าตอบแทนหรือค่าไถ่ (Ransom) แลกกับการที่จะไม่เปิดเผยข้อมูลความลับที่ได้ขโมยมา

การก่อวินาศกรรมหรือการทำลาย (Deliberate Acts of Sabotage or Vandalism) การก่อวินาศกรรมระบบคอมพิวเตอร์หรือธุรกิจ เป็นการทำลายทรัพย์สินหรือสารสนเทศขององค์กรก่อให้เกิดความเสียหาย เช่น การทำลายทรัพย์สิน หรือ การทำลายภาพพจน์ที่ดีขององค์กร เป็นต้น ในบางครั้งการสร้างความเสียหายไม่จำเป็นต้องเป็นตัวเงินเสมอไป การทำลายภาพพจน์ที่ดีขององค์กรก็เป็นเรื่องร้ายแรงเช่นเดียวกัน การทำลายเว็บไซต์ขององค์กร ส่งผลกระทบต่อความเชื่อมั่นของลูกค้าทำให้ยอดขายและมูลค่าขององค์กร รวมถึงชื่อเสียงก็ลดลงเช่นกัน

การโจรกรรม (Deliberate Acts of Theft) การคุกคามโดยการโจรกรรมเกิดจากบุคคลที่ได้มีการไตร่ตรองไว้ล่วงหน้า โดยมีเจตนายึดทรัพย์สินของผู้อื่นไปครอบครองโดยผิดกฎหมาย ซึ่งภายในองค์กรสามารถถูกโจรกรรมทรัพย์สิน ได้ 2 ลักษณะ คือ ทรัพย์สินทางกายภาพ (Physical Property) เช่น เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เป็นต้น และทรัพย์สินทางอิเล็กทรอนิกส์ (Electronic Property) เช่น ข้อมูล หรือสารสนเทศขององค์กร เป็นต้น โดยทรัพย์สินทางอิเล็กทรอนิกส์มีความซับซ้อนในการจัดการและควบคุม ซึ่งเป็นปัญหาหาขององค์กร ซึ่งต่างจากการโจรกรรมทรัพย์สินทางกายภาพสามารถตรวจพบได้ง่ายกว่า

การโจมตีโดยซอฟต์แวร์ (Deliberate Software Attacks) การโจมตีโดยซอฟต์แวร์ เกิดขึ้นโดยการออกแบบซอฟต์แวร์ให้โจมตีระบบจากคนๆ เดียวหรือจากกลุ่มคน โดยเป้าหมายคือ ก่อความเสียหาย ทำลาย หรือ ปฏิเสธการบริการของระบบเป้าหมาย ซอพต์แวร์ที่อยู่ในกลุ่มนี้ คือ Malicious Code หรือ Malicious Software มักจะเรียกว่า มัลแวร์(Malware) เช่น ไวรัส (Viruses) เวิร์ม (Worms)

ภัยธรรมชาติ (Forces of Nature) ภัยธรรมชาติเป็นภัยคุกคามที่อันตรายมาก เพราะเป็นสิ่งที่เกินกว่ามนุษย์จะควบคุมได้ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว ฟ้าผ่า รวมถึงภูเขาไฟระเบิด เป็นต้น ทั้งหมดนี้ไม่เพียงแต่สร้างความยุ่งยากต่อการใช้ชีวิตของแต่ละคนเท่านั้น แต่ยังสร้างปัญหาให้กับระบบสารสนเทศทั้งหน่วยเก็บข้อมูล สัญญาณการสื่อสารต่างๆ

คุณภาพของบริการ (Deviations in Quality of Service) ระบบสารสนเทศขององค์กรจะสามารถให้บริการได้นั้นต้องได้รับการสนับสนุนจากระบบอื่นๆ ร่วมด้วย เช่น โรงไฟฟ้า เครือข่ายโทรคมนาคม ผู้จัดจำหน่าย ผู้ให้บริการอินเตอร์เน็ต เป็นต้น ซึ่งระบบสนับสนุนเหล่านี้อาจหยุดชะงักได้หากเกิดพายุ พนักงานป่วย หรือเหตุฉุกเฉิน หากเกิดภัยคุกคามเหล่านี้ ทำให้คุณภาพของผู้ให้บริการคลาดเคลื่อน ไม่สมบูรณ์ และสร้างความเสียหายต่อระบบสารสนเทศขององค์กรได้

ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (Technical Hardware Failures or Errors) ความผิดพลาดทางเทคนิคของฮาร์ดแวร์ หรือความผิดพลาดที่การผลิตอุปกรณ์เกิดข้อบกพร่องเป็นเหตุให้การทำงานของอุปกรณ์โดยรวมไม่เป็นไปอย่างที่ออกแบบไว้ ส่งผลเสียต่อระบบสารสนเทศขององค์กรที่นำอุปกรณ์ที่มีข้อผิดพลาดเหล่านี้ไปใช้งาน

ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ (Technical Software Failures or Errors) ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ เกิดจากขั้นตอนในการพัฒนาซอฟต์แวร์แล้วไม่สามารถตรวจพบข้อผิดพลาดของซอฟต์แวร์ได้ ส่งผลเสียต่อหน่วยงานหรือองค์กรที่นำซอฟต์แวร์ที่มีข้อผิดพลาดนี้ไปใช้งาน ทำให้ระบบสารสนเทศขององค์กรไม่สามารถให้บริการได้อย่างปกติได้

เทคโนโลยีล้าสมัย (Technological Obsolescence) การใช้เทคโนโลยีที่ล้าสมัย ที่ผู้ให้บริการไม่สนับสนุนแล้ว ทำให้ข้อผิดพลาดต่างๆ ที่เกิดขึ้นภายหลังไม่ได้รับแก้ไขปรับปรุงก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัย ส่งผลเสียต่อองค์กรที่ใช้เทคโนโลยีล้าสมัยเหล่านั้น

ผู้วิจัยวิเคราะห์ประเภทของภัยคุกคามความมั่นคงปลอดภัยสารสนเทศจากนักวิชาการที่กล่าวมาข้างต้น ได้ดังตาราง 1

ตาราง 1 สรุปประเภทของภัยคุกคาม

ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ	Whiteman et. Al.(2011)	จตุชัย แพงจันทร์ (2553)	เศรษฐพงศ์ มะลิสุวรรณ (2552)
1) การละเมิดทรัพย์สินทางปัญญา (Compromises to intellectual property)	✓		✓
2) การโจมตีด้วยซอฟต์แวร์ (Deliberate Software Attacks)	✓	✓	✓
3) คุณภาพของผู้ให้บริการที่ไม่เพียงพอ (Deviations in Quality of Service)	✓		✓
4) การจารกรรมหรือการบุกรุก (Espionage or Trespass)	✓	✓	✓
5) ภัยธรรมชาติ (Forces of Nature)	✓		✓
6) ข้อผิดพลาดจากการกระทำของมนุษย์ (human error or failure)	✓		✓
7) การกรรโชกข้อมูลสารสนเทศ (Information Extortion)	✓	✓	✓
8) การจัดทำแผนและนโยบายขององค์กรที่ไม่สมบูรณ์ (Missing, Inadequate, or Incomplete Organizational Policy or Planning)	✓		
9) มาตรการควบคุมที่ไม่สมบูรณ์ (Missing, Inadequate, or Incomplete Controls)	✓		
10) การก่อวินาศกรรมหรือการทำลาย (Sabotage or Vandalism)	✓	✓	✓
11) การโจรกรรม (Theft)	✓		✓
12) ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (Technical Hardware Failures or Errors)	✓		✓
13) ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ (Technical Software Failures or Errors)	✓		✓
14) เทคโนโลยีล้าสมัย (Technological Obsolescence)	✓		✓

จากตาราง 1 ผู้วิจัยขอสรุปว่า ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ มี 14 ประเภท คือ

1. การละเมิดทรัพย์สินทางปัญญา (Compromises to intellectual property) ทรัพย์สินทางปัญญา (IP) เป็นทรัพย์สินชนิดหนึ่ง เช่น ลิขสิทธิ์ เครื่องหมายทางการค้าและสิทธิบัตร ส่วนใหญ่การละเมิดทรัพย์สินทางปัญญาจะเป็นการทำสำเนาซอฟต์แวร์ที่มีลิขสิทธิ์

2. การโจมตีด้วยซอฟต์แวร์ (Deliberate Software Attacks) การโจมตีด้วยซอฟต์แวร์ เป็นการโจมตีระบบสารสนเทศจากคนๆ เดียวหรือจากกลุ่มคนโดยใช้ซอฟต์แวร์ที่สามารถสร้างความเสียหาย ทำลาย หรือทำให้ระบบสารสนเทศของของเป้าหมายที่โจมตีปฏิเสธการให้บริการได้ ซึ่งซอฟแวร์ที่ใช้โจมตีเรียกว่า Malicious Code หรือ Malicious Software นิยมเรียกว่า มัลแวร์ (Malware) ตัวอย่างของมัลแวร์ เช่น ไวรัส (Viruses) เวิร์ม (Worms) ม้าโทรจัน (Trojan Horses) Logic bombs และ ช่องแบ็คดอร์(Back doors) เป็นต้น

3. คุณภาพของผู้ให้บริการที่ไม่เพียงพอ (Deviations in Quality of Service) ระบบสารสนเทศขององค์กรต้องได้รับการสนับสนุนจากส่วนอื่นๆ ร่วมกัน เช่น ระบบไฟฟ้า เครือข่ายโทรคมนาคม ผู้จัดจำหน่าย ผู้ให้บริการอินเทอร์เน็ต เจ้าหน้าที่ด้านต่างๆ ซึ่งส่วนที่สนับสนุนเหล่านี้อาจให้บริการได้ไม่เต็มความสามารถ หากส่วนสนับสนุนนั้นประสบเหตุการณ์ที่ส่งผลต่อการให้บริการ เช่น พายุ พนักงานป่วย หรือเหตุฉุกเฉินใดๆ เป็นต้น ส่งผลให้การให้บริการของระบบสารสนเทศขององค์กรไม่สามารถให้บริการได้สมบูรณ์ปกติ

4. การจารกรรมหรือการบุกรุก (Espionage or Trespass) การจารกรรมและการบุกรุกระบบสารสนเทศ ทั้งในรูปแบบอิเล็กทรอนิกส์และกระทำโดยบุคคลสามารถเข้าถึงสารสนเทศที่เป็นความลับทางกายภาพ โดยผู้บุกรุกระบบสารสนเทศใช้ทุกวิธีการเพื่อให้สามารถเข้าถึงสารสนเทศที่เก็บรักษาอยู่ภายในระบบสารสนเทศ

5. ภัยธรรมชาติ (Forces of Nature) ภัยธรรมชาติเป็นภัยคุกคามที่ควบคุมได้ยาก เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว และฟ้าผ่า รวมถึงภูเขาไฟระเบิด เป็นต้น ภัยธรรมชาติสร้างความยุ่งยาก และสร้างปัญหาให้กับระบบสารสนเทศทั้งหน่วยเก็บข้อมูล สัญญาณการสื่อสารต่างๆ ส่งผลเสียโดยรวมต่อระบบสารสนเทศขององค์กร

6. ข้อผิดพลาดจากการกระทำของมนุษย์ (human error or failure) ภัยคุกคามจากความผิดพลาดของการกระทำของมนุษย์ ครอบคลุมการกระทำทั้งที่เจตนาและไม่เจตนามุ่งร้ายต่อสารสนเทศขององค์กร โดยผู้ใช้ระบบสารสนเทศอาจทำงาน

ผิดพลาด เนื่องจากขาดความชำนาญ ขาดการฝึกอบรม หรือตั้งใจทำให้เกิดข้อมูลที่ผิดพลาด ซึ่งสร้างความเสียหายให้แก่สารสนเทศขององค์กร

7. การกรรโชกข้อมูลสารสนเทศ (Information Extortion) การกรรโชกข้อมูลสารสนเทศ เกิดจากการที่ข้อมูลที่เป็นความลับที่จัดเก็บอยู่ในระบบสารสนเทศถูกขโมยไปอาจจะเป็นผู้บุกรุกจากภายนอกหรือผู้ที่มีหน้าที่ดูแลรักษาข้อมูลภายในองค์กรเอง โดยมีการเรียกร้องค่าตอบแทนหรือค่าไถ่ (Ransom) แลกกับการที่ไม่เปิดเผยข้อมูลความลับที่ได้ขโมยมา (Black Mail)

8. การจัดทำแผนและนโยบายขององค์กรที่ไม่สมบูรณ์ (Missing, Inadequate, or Incomplete Organizational Policy or Planning) การจัดทำนโยบายระบบสารสนเทศขององค์กรที่ไม่สมบูรณ์ ไม่เพียงพอ หรือตกหล่น ส่งผลให้ระบบสารสนเทศขององค์กรมีช่องโหว่ที่จะก่อให้เกิดการสูญเสีย ถูกโจมตี หรือถูกเปิดเผยสารสนเทศที่เป็นความลับขององค์กร และการจัดทำนโยบายระบบสารสนเทศที่ไม่สมบูรณ์ยังเป็นการเปิดช่องโหว่ทำให้ภัยคุกคามอื่นๆ เข้ามาคุกคามระบบสารสนเทศขององค์กรได้อีกด้วย

9. มาตรการควบคุมที่ไม่สมบูรณ์ (Missing, Inadequate, or Incomplete Controls) มาตรการควบคุมเป็นมาตรการสำหรับแก้ปัญหาช่องโหว่ที่เกิดขึ้นในระบบสารสนเทศ หากมาตรการควบคุมไม่สมบูรณ์ ไม่เพียงพอ หรือตกหล่น เช่น มาตรการควบคุมที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย เป็นต้น ส่งผลให้มีโอกาสที่สารสนเทศเกิดความเสียหายเมื่อมีภัยคุกคามระบบสารสนเทศขององค์กร

10. การก่อวินาศกรรมหรือการทำลาย (Sabotage or Vandalism) ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศจากการก่อวินาศกรรมหรือการทำลาย เป็นการก่อวินาศกรรมต่อระบบสารสนเทศหรือธุรกิจ หรือการทำลายทรัพย์สินซึ่งก่อให้เกิดความเสียหาย สามารถสร้างความเสียหายต่อทรัพย์สิน หรือการทำลายภาพพจน์ที่ดีขององค์กรก็เป็นการสร้างความเสียหายร้ายแรงต่อองค์กรเช่นกัน

11. การโจรกรรม (Theft) ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศจากการโจรกรรม เป็นการครอบครองทรัพย์สินผู้อื่นโดยผิดกฎหมาย ซึ่งทรัพย์สินที่สามารถถูกโจรกรรมได้ คือ ทรัพย์สินทางกายภาพ (Physical Property) ทรัพย์สินที่ในรูปแบบอิเล็กทรอนิกส์ (Electronic Property) และทรัพย์สินทางปัญญา (Intellectual Property)

12. ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ (Technical Hardware Failures or Errors) ภัยคุกคามจากข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ เกิดจากที่ผู้ผลิตนำอุปกรณ์ที่มีปัญหาออกมาจำหน่ายสู่ตลาด ทำให้องค์กรที่นำอุปกรณ์เหล่านั้นไปใช้งาน ได้รับผลกระทบจากการทำงานผิดพลาดของอุปกรณ์ ส่งผลให้ระบบสารสนเทศไม่สามารถให้บริการได้ตามปกติ

13. ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ (Technical Software Failures or Errors) การจำหน่ายซอฟต์แวร์ก่อนที่จะตรวจพบจุดบกพร่อง ทำให้องค์กรที่นำซอฟแวร์ที่มีข้อบกพร่องนี้ไปใช้งาน ได้รับผลกระทบทำให้การให้บริการระบบสารสนเทศขององค์กรเกิดอุปสรรคติดขัดไม่สามารถให้บริการได้อย่างสมบูรณ์

14. เทคโนโลยีล้าสมัย (Technological Obsolescence) เทคโนโลยีที่ล้าสมัยจะไม่ได้รับการพัฒนาปรับปรุงจากผู้จำหน่ายทำให้จุดบกพร่องต่างๆ ที่ตรวจพบภายหลังไม่ได้รับการแก้ไข ทำให้เสี่ยงต่อภัยคุกคามที่มีต่อระบบสารสนเทศ ซึ่งส่งผลต่อการให้บริการของระบบสารสนเทศขององค์กร

การจัดการความมั่นคงปลอดภัยสารสนเทศ

การทบทวนวรรณกรรมเกี่ยวกับการจัดการความมั่นคงปลอดภัยสารสนเทศ ผู้วิจัยแบ่งเป็นหัวข้อย่อย คือ ความหมายของการจัดการความมั่นคงปลอดภัยสารสนเทศ, มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ, กระบวนการจัดการความมั่นคงปลอดภัย, มาตรการการจัดการความมั่นคงปลอดภัย

1. ความหมายของการจัดการความมั่นคงปลอดภัยสารสนเทศ

การจัดการความมั่นคงปลอดภัยสารสนเทศ มีผู้ให้ความหมายไว้ดังนี้

วศิน รำพึงกิจ (2552, หน้า 8) กล่าวว่า การจัดการความมั่นคงปลอดภัยสารสนเทศ เป็นการป้องกันการสูญเสียทรัพย์สินสารสนเทศ ลดผลกระทบและลดความเสี่ยงต่างๆ ที่อาจเกิดขึ้นที่จะทำให้การดำเนินการทางธุรกิจหรือความต่อเนื่องของงานเป็นไปอย่างราบรื่น

จิระ จิตสุภา และคณะ (2555, ไม่ปรากฏเลขหน้า) การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศเป็นการระบุรายละเอียดการดำเนินการของทรัพย์สินด้านความมั่นคงปลอดภัยและการพัฒนาระบบ การจัดทำเอกสาร นโยบาย มาตรฐาน

ขั้นตอนการปฏิบัติและแนวปฏิบัติ ซึ่งต้องยึดกรอบดำเนินการที่ประกอบด้วยการเก็บรักษาข้อมูลไว้เป็นความลับ (Confidentiality), ความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้ของข้อมูล (Availability) โดยการดำเนินการควรประกอบไปด้วยการแบ่งชั้นความสำคัญและความลับข้อมูล การสร้างความตระหนัก การฝึกอบรมและการให้ความรู้ด้วยการเรียนรู้แก่ผู้มีส่วนได้ส่วนเสีย

จากที่ได้กล่าวมา ผู้วิจัยสรุปว่า การจัดการความมั่นคงปลอดภัยสารสนเทศ หมายถึง การป้องกันการสูญเสียทรัพย์สินสารสนเทศ ลดผลกระทบและลดความเสี่ยงต่างๆ ที่อาจเกิดขึ้นที่จะทำให้การดำเนินการทางธุรกิจหรือความต่อเนื่องของงานเป็นไปอย่างราบรื่น โดยมีขั้นตอน ระบุรายละเอียดการดำเนินการของทรัพย์สินด้านความมั่นคงปลอดภัยและการพัฒนาระบบ การจัดทำเอกสาร นโยบาย มาตรฐาน ขั้นตอนการปฏิบัติและแนวปฏิบัติ ซึ่งต้องยึดกรอบดำเนินการที่ประกอบด้วยการเก็บรักษาข้อมูลไว้เป็นความลับ (Confidentiality) ความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้ของข้อมูล (Availability) การแบ่งชั้นความสำคัญและความลับข้อมูล การสร้างความตระหนัก การฝึกอบรมและการให้ความรู้ด้วยการเรียนรู้แก่ผู้มีส่วนได้ส่วนเสีย

2. มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ

จากการทบทวนวรรณกรรมที่เกี่ยวข้องกับมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ มีผู้ให้ความหมายของมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ ไว้ดังนี้

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นมาตรการสำหรับใช้ในการควบคุมให้ระบบสารสนเทศมีความมั่นคงปลอดภัย ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและสารสนเทศในระบบ (สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, 2555)

จิระ จิตสุภา และคณะ (2555) กล่าวว่า มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ คือ กระบวนการดำเนินการ ซึ่งทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย ช่วยสร้างความมั่นใจในการบริหารจัดการความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้สามารถดำเนินไปอย่างต่อเนื่อง มีประสิทธิภาพ และเป็นที่ยอมรับ

จากที่ได้กล่าวมา ผู้วิจัยสรุปว่า มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ คือ มาตรการ กระบวนการ สำหรับควบคุมให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและสารสนเทศในระบบ ช่วยสร้างความมั่นใจในการบริหารจัดการความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้สามารถดำเนินไปอย่างต่อเนื่อง มีประสิทธิภาพ และเป็นที่ยอมรับ

จากการทบทวนวรรณกรรมที่เกี่ยวข้องกับมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ มีมาตรฐานเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ และนิยมใช้แพร่หลายดังนี้

2.1 ISO/IEC 27001 เป็นมาตรฐานที่เกี่ยวกับการจัดการในเรื่องความปลอดภัยของข้อมูล ได้รับการพัฒนามาจาก Information Security Management Standard BS7799 Part 2 ออกโดย British Standard Institute (BSI) จากนั้นจึงได้รับการพิจารณาจาก International Standard Organization) International Organizational for Standard (ISO) และ International Electrotechnical Commission (IEC) ประกาศให้เป็นมาตรฐานสากล มาตรฐาน ISO/IEC 27001:2005 เป็นมาตรฐานเกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information Security Management Systems: ISMS) ซึ่งจะกำหนดความต้องการ (Set of Requirements) ในการจัดทำระบบ ISMS เพื่อช่วยให้องค์กรสามารถสร้างระบบ ISMS ขึ้นมาได้อย่างมีประสิทธิภาพ ซึ่งระบบ ISMS นี้ถือเป็นส่วนหนึ่งของระบบบริหารจัดการขององค์กรที่มีพื้นฐานมาจากแนวทางการบริหารจัดการความเสี่ยงของธุรกิจ (Business Risk Approach) โดยมีวัตถุประสงค์เพื่อรักษาไว้ซึ่งความลับ (Confidentiality) บูรณภาพ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศและทรัพย์สินอื่นๆ ขององค์กร เพื่อให้องค์กรสามารถรอดพ้นจากภัยคุกคามต่างๆ ได้ มาตรฐาน ISO/IEC 27001:2005 ประกอบไปด้วยข้อกำหนดและแนวทางในการจัดตั้งระบบ ISMS ขึ้นภายในองค์กรตั้งแต่การริเริ่มทำระบบ การนำระบบไปใช้ การดำเนินงานของระบบ การวัดผลและการทบทวนการดำเนินงานของระบบ การบำรุงรักษาระบบและการปรับปรุงระบบอย่างสม่ำเสมอ รวมถึงแนวทางในการออกใบรับรอง (Certification) ให้กับระบบโดยที่หัวใจสำคัญของระบบ ISMS นั้นอยู่ที่การทำการตรวจประเมินความเสี่ยงและการเลือกวิธีการควบคุมให้เหมาะสมกับการปฏิบัติงานและระดับความเสี่ยงที่ยอมรับได้ขององค์กรนอกจากนั้น มาตรฐานนี้ยังได้ถูกปรับปรุงเพื่อให้มีความเข้ากันได้กับ

มาตรฐาน ISO9001 และISO14001 และมาตรฐาน ISO/IEC27001 ยังได้มีการอ้างอิงมาตรการของการควบคุมทางด้านการจัดการความปลอดภัยของข้อมูลทั้ง 11 หมวด 133 มาตรการตามมาตรฐาน ISO/IEC 17799:2005 โดยระบุไว้ในส่วนของ Annex A ด้วย (หนึ่งฤทัย เตชะรัตนประเสริฐ, 2552, หน้า 14–18; ศรีสุรางค์ เบญจสัตย์กุล, 2553, หน้า 31)

2.2 ISO/IEC 17799 มีจุดเริ่มต้นมาจากมาตรฐาน BS7799 Part1 ซึ่งถูกพัฒนาขึ้นครั้งแรกในปี ค.ศ. 1995 โดย British Standard Institute (BSI) ของประเทศอังกฤษ มาตรฐานดังกล่าวเกิดจากการรวบรวมมาตรการพื้นฐาน (Baseline) ทางอุตสาหกรรมที่หลายๆ องค์กรยึดถือร่วมกันและถูกนำไปใช้อย่างแพร่หลายทั่วโลก แม้แต่องค์กรที่ไม่ได้อยู่ในภาคอุตสาหกรรม และได้ถูกแก้ไขปรับปรุงหลายครั้ง จนกระทั่งได้รับการพิจารณาจาก International Organizational for Standard (ISO) และ International Electrotechnical Commission (IEC) ประกาศให้เป็นมาตรฐานสากล ISO/IEC 17799:2000 – Code of Practice for Information Security Management ซึ่งในฉบับล่าสุดที่เปลี่ยนชื่อเป็น ISO/IEC 17799:2005 – Security Technique – Code of Practice for Information Security Management นั้นจะประกอบไปด้วยหัวข้อ (Domain) และวัตถุประสงค์ (Control Objectives) ที่ใช้ในการควบคุมทางด้านการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ปรับปรุงใหม่แล้ว ทั้งหมด 11 หัวข้อ ใน 39 วัตถุประสงค์ รวมเป็นมาตรการ (Controls) ทั้งสิ้น 133 มาตรการ (หนึ่งฤทัย เตชะรัตนประเสริฐ, 2552, หน้า 9–10)

2.3 Control Objectives for Information and Related Technology (COBIT) มาตรฐานนี้เกิดจากความร่วมมือของ IT Governance Institute (ITGI) และ Information Systems Audit and Control Association (ISACA) ได้ร่วมกันจัดทำมาตรฐาน COBIT ขึ้นมา ไม่เพียงแต่จุดประสงค์ด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเท่านั้น แต่ยังมุ่งหวังสร้างการบริหารจัดการที่ดีทางเทคโนโลยีสารสนเทศ (IT governance) อีกทางหนึ่งด้วย มาตรฐาน COBIT เป็นแนวคิดและแนวทางการปฏิบัติ เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่างๆ ที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี ซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยโครงสร้างของมาตรฐาน COBIT ได้ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจแบ่งได้เป็น 4 กระบวนการหลัก ได้แก่ 1) การวางแผนและการจัดการองค์กร 2) การจัดหาและติดตั้ง 3) การส่งมอบและบำรุงรักษา และ 4) การติดตามผลโดยในแต่ละกระบวนการหลัก

จะมีวัตถุประสงค์ของการควบคุมหลัก 34 หัวข้อ และในแต่ละหัวข้อจะประกอบด้วยวัตถุประสงค์ของการควบคุมย่อยลงไปอีกขั้นหนึ่ง รวม 318 หัวข้อย่อย พร้อมทั้งแนวทางการตรวจสอบสำหรับแต่ละหัวข้อ (จิระ จิตสุภา และคณะ, 2555, หน้า 73; ศรีสุรางค์ เบญจสัตย์กุล, 2553, หน้า 37–38)

2.4 Information Technology Infrastructure Library (ITIL) เป็นแนวทางปฏิบัติที่ว่าด้วยเรื่องเกี่ยวกับโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เป็นมาตรฐานด้านความมั่นคงปลอดภัยจากประเทศอังกฤษ The British Office of Government Commerce (OGC) มีวัตถุประสงค์ในการสร้าง Best Practices สำหรับกระบวนการของ IT Service Delivery และSupport แต่ไม่ได้เป็นการกำหนด Framework ของการควบคุม เน้นการพัฒนากระบวนการเพื่อรองรับการให้บริการต่อลูกค้าและธุรกิจเป็นหลัก เช่นการออกแบบการติดตั้ง การกระจาย การดูแลรักษาและการปรับปรุง เป็นต้น ITIL เป็นแนวทางปฏิบัติที่ดีเยี่ยมในการบริหารจัดการด้าน IT Service ให้แก่ลูกค้าแนวทางปฏิบัตินี้เหมาะกับองค์กรทุกขนาดโดยเฉพาะอย่างยิ่งองค์กรที่เน้นเรื่องของการบริการด้าน IT Service (จิระ จิตสุภา และคณะ, 2555, หน้า 72; วราภรณ์ ธวิทย์ชัยพร, 2549)

2.5 มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ สำหรับประเทศไทยนั้น คณะอนุกรรมการด้านความมั่นคงภายใต้คณะอนุกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งถูกจัดตั้งขึ้นตามพระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้นำเอามาตรฐาน ISO/IEC 17799:2000 มาเป็นแนวทางในการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 1) ประจำปี พ.ศ. 2547 หลังจากที่ได้พัฒนามาตรฐานในเวอร์ชัน 1 แล้ว จึงได้นำเอามาตรฐาน ISO/IEC 17799:2005 มาเป็นแนวทางในการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2) ประจำปี พ.ศ. 2549 โดยได้มีการปรับเปลี่ยนในสาระสำคัญสองประการ ประการแรก คือ มีการเพิ่มมาตรการที่เห็นว่ามีความเหมาะสมกับสภาพแวดล้อมและสถานการณ์ทางด้านเทคโนโลยีสารสนเทศในประเทศไทยรวมเป็นจำนวนทั้งสิ้น 144 มาตรการ ประการที่สองคือ มีการแบ่งระดับของมาตรการเป็นระดับ 1 – 3 เพื่อช่วยให้องค์กรค่อยๆ นำมาตรการแต่ละระดับไปปรับใช้ด้วยวิธีค่อยเป็นค่อยไป ในกรณีที่องค์กรเห็นว่าการนำมาตรการทั้งหมดไปปฏิบัตินั้นเป็นเรื่องที่ทำได้ยาก คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้มอบหมายให้คณะอนุกรรมการด้านความมั่นคงปลอดภัยทำการพัฒนามาตรฐานด้าน

ความมั่นคงปลอดภัยดังกล่าวขึ้น โดยหน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ในฐานะฝ่ายเลขานุการของคณะอนุกรรมการชุดดังกล่าว เป็นหน่วยงานซึ่งทำการศึกษา วิจัย และพัฒนามาตรฐานดังกล่าวโดยอ้างอิงกับมาตรฐาน ISO/IEC 27001:2005 และ ISO/IEC 17799:2005 ทั้งนี้ เพื่อให้มาตรฐานความมั่นคงปลอดภัยที่พัฒนาขึ้นนั้นสอดคล้องกับมาตรฐานสากล พัฒนามาเป็น มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี พ.ศ. 2550 จากนั้นคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ก็ได้พิจารณาให้ความเห็นชอบร่างมาตรฐานดังกล่าว เพื่อให้มีการดำเนินการตามขั้นตอนเพื่อประกาศให้ร่างมาตรฐานด้านความมั่นคงปลอดภัยที่จัดทำขึ้นนั้นเป็นมาตรฐานของประเทศไทยต่อไป (ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ, 2550; หนึ่งฤทัย เตชะรัตนประเสริฐ, 2552, หน้า 14)

จากการทบทวนวรรณกรรมที่เกี่ยวข้อง มีการเลือกใช้หรืออ้างอิงมาตรฐานสากลเพื่อใช้เป็นแนวทางในการจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งสามารถสรุปได้ดังตาราง 2

ตาราง 2 มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ

วรรณกรรม	ISO27001	ISO17799	COBIT	ITILL	BS 7799	ISMF
1. การรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษาศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี (เฉลิม สุวรรณะ, 2554)	✓					
2. การศึกษาระบบความมั่นคงปลอดภัยด้านสารสนเทศสำหรับบริการทางการเงินผ่านอินเทอร์เน็ต กรณีศึกษา: ธนาคารพาณิชย์แห่งหนึ่ง (หนึ่งฤทัย เตชะรัตนประเสริฐ, 2552)	✓	✓				

ตาราง 2 (ต่อ)

วรรณกรรม	ISO27001	ISO17799	COBIT	ITILL	BS 7799	ISMF
3. การสำรวจภัยคุกตามทางคอมพิวเตอร์และการรักษาความปลอดภัยข้อมูลสารสนเทศ ของธนาคารพาณิชย์ในประเทศไทย (วศิน รำพึงกิจ, 2552)	✓					
4. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสำหรับส่วนงานความมั่นคงสารสนเทศ กระทรวงการต่างประเทศ (ชูเกียรติ ประเสริฐสุข, 2551)	✓	✓				
5. การศึกษาแนวทางการพัฒนานโยบายความมั่นคงปลอดภัยสารสนเทศภายในองค์กร กรณีศึกษา บริษัท NEC Corporation (Thailand) Ltd. (ภูมินทร์ ภูดวงสี, 2550)	✓					
6. แนวทางการนำ Information Security Management มาใช้ในการจัดระเบียบการบริหารจัดการด้านความปลอดภัยสารสนเทศ กรณีศึกษา: บริษัทให้คำปรึกษาด้านสารสนเทศแห่งหนึ่ง (วรากรณ์ ธวิทย์ชัยพร, 2549)				✓		✓
7. การสร้างมาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้ และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550: กรณีศึกษาองค์กรกระจายเสียงและแพร่ภาพแห่งสาธารณะแห่งประเทศไทย (วิภาวรรณ คุ้มศิริ, 2552)	✓					✓

ตาราง 2 (ต่อ)

วรรณกรรม	ISO27001	ISO17799	COBIT	ITILL	BS 7799	ISMF
8. แนวทางในการวางระบบความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก (ผกากรอง บ่ายสว่าง และคณะ, 2552)	✓					
9. การสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO27001 ขององค์กร กรณีศึกษา บริษัท บิ๊กฟิช เอ็นเตอร์ไพร์ส จำกัด (พิรมล เก่งคุมพล, 2555)	✓					
10. การสังเคราะห์เนื้อหาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศตามมาตรฐานสากล (จิระ จิตสุภา และคณะ, 2555)	✓		✓			
11. คู่มือการรักษาความมั่นคงปลอดภัยICT (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2550)	✓					
12. การจัดทำแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศด้วยมาตรฐาน ISO/IEC 27001 กรณีศึกษา : สำนักงานรัฐบาลอิเล็กทรอนิกส์ (มหาชน) (สรอ.) (รัชชาภรณ์ สุภาพ และคณะ, 2557)	✓					
13. การศึกษาแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ ด้วยมาตรฐาน ISO/IEC 27001 และเกณฑ์ด้านสารสนเทศ COBIT กรณีศึกษา บริษัท วิทยุการบินแห่งประเทศไทย จำกัด (ศรีสุรางค์ เบญจสัตย์กุล, 2553)	✓		✓			

จากตารางสรุปได้ว่า มาตรฐาน ISO/IEC27001 เป็นมาตรฐานที่งานวิจัยใช้เป็นกรอบในการจัดการความมั่นคงปลอดภัยสารสนเทศอย่างแพร่หลาย และคณะอนุกรรมการด้านความมั่นคงปลอดภัยภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งถูกจัดตั้งขึ้นตามพระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้นำเอามาตรฐาน ISO/IEC 27001 และมาตรฐาน ISO/IEC17799 มาใช้เป็นแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550 (ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ, 2550) เพื่อเป็นมาตรฐานความมั่นคงปลอดภัยของประเทศ ดังนั้นเพื่อให้มาตรฐานของงานวิจัยสอดคล้องกับบริบทและมาตรฐานของประเทศไทย ผู้วิจัยจึงเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบทำธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550 ของคณะอนุกรรมการด้านความมั่นคงภายใต้คณะอนุกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นมาตรฐานในการวิจัยครั้งนี้

3. กระบวนการจัดทำระบบการจัดการความมั่นคงปลอดภัย

กระบวนการจัดทำระบบการจัดการความมั่นคงปลอดภัยสารสนเทศตามแนวทางของมาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ประจำปี 2550 มีรายละเอียดโดยสรุปดังนี้

องค์กรจะต้องกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ได้กำหนดไว้เป็นลายลักษณ์อักษร ภายในกรอบกิจกรรมการดำเนินการทางธุรกิจต่างๆ รวมทั้งความเสี่ยงที่เกี่ยวข้อง แนวทางที่ใช้ในมาตรฐานฉบับนี้จะใช้กระบวนการ Plan–Do–Check–Act หรือ P–D–C–A

Plan กำหนดนโยบายความมั่นคงปลอดภัย และจัดทำระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) โดยต้องกำหนดขอบเขตของระบบการจัดการความมั่นคงปลอดภัย กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศโดยพิจารณาจากบริบทขององค์กร จัดทำระบบการจัดการความเสี่ยง ระบุความเสี่ยงที่เหลืออยู่ในระบบ และกำหนดมาตรการในการจัดการกับเสี่ยง

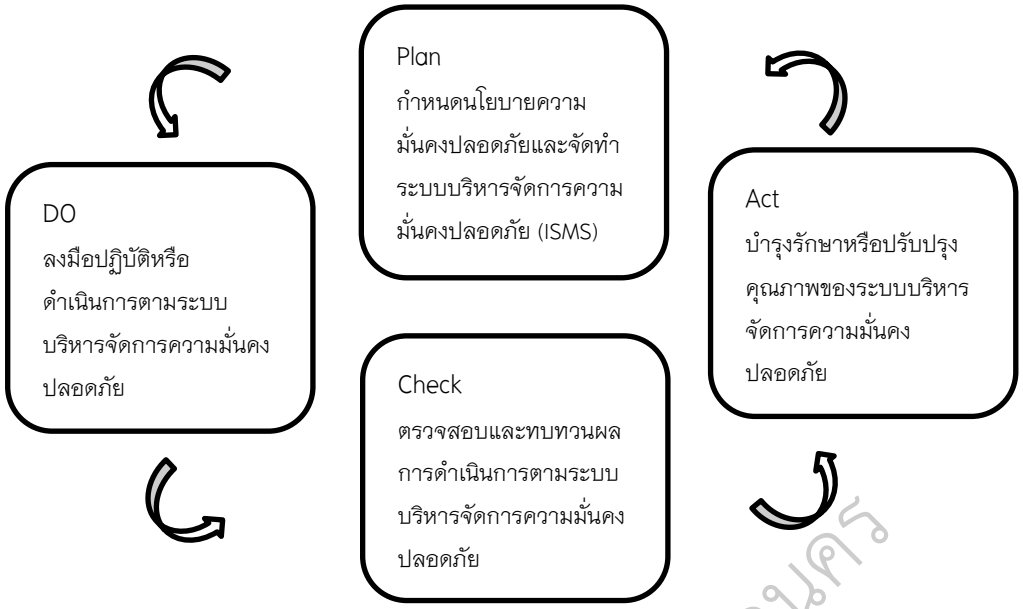
Do ลงมือปฏิบัติและดำเนินการระบบการจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร จัดทำแผนจัดการความเสี่ยงและลงมือปฏิบัติตามแผนการจัดการ

ความเสี่ยง ดำเนินการตามมาตรการการจัดการความเสี่ยงที่ได้เลือกไว้ ฝึกอบรมบุคลากร สร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

Check ตรวจสอบและทบทวนผลการดำเนินการตามระบบการจัดการความมั่นคงปลอดภัย ตรวจสอบข้อผิดพลาดจากการประมวลผล ระบุการละเมิดความมั่นคงปลอดภัย ระบุกิจกรรมทางด้านความมั่นคงปลอดภัยที่มอบหมายให้กับบุคลากรเป็นไปตามที่คาดหมายไว้หรือไม่ ตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และตรวจสอบการดำเนินการเพื่อแก้ไขการละเมิดด้านความมั่นคงปลอดภัยว่ามีสัมฤทธิผลหรือไม่ ทบทวนความสัมฤทธิผลของระบบการจัดการความมั่นคงปลอดภัย ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้ และทบทวนความเสี่ยงที่ยังเหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ ดำเนินการพิจารณาทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหารอย่างสม่ำเสมอ

Act บำรุงรักษาหรือปรับปรุงคุณภาพของระบบบริหารจัดการความมั่นคงปลอดภัย ดำเนินการแก้ไขและปรับปรุงตามที่ระบุไว้ในขั้นตอนการสอบและทบทวนผลการดำเนินการตามระบบการจัดการความมั่นคงปลอดภัย แจ้งการปรับปรุงและการดำเนินการให้ทุกหน่วยงานที่เกี่ยวข้องโดยให้รายละเอียดที่เหมาะสมต่อสถานการณ์ที่เกิดขึ้น

แสดงวงจรการจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan Do Check Act ตามดังภาพประกอบ 2



ภาพประกอบ 2 แผนภาพแสดงวงจรการจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan–Do–Check–Act (ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ, 2550, หน้า 10)

4. มาตรการการจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

จากการศึกษาค้นคว้างานวิจัยที่เกี่ยวข้อง มีการอธิบายมาตรการการจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ดังนี้

หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (2550, หน้า 26 – 56) และวิภาวรรณ คุ้มสิริ (2552, หน้า 16–42) เห็นสอดคล้องกัน โดยมีรายละเอียดดังนี้

มาตรการการจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศประกอบไปด้วย 11 หมวด ดังต่อไปนี้

4.1 หมวดที่ 1 นโยบายความมั่นคงปลอดภัย (Security policy)

4.1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)

มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจกฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

4.1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)

(ผู้บริหารองค์กร) ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษร เอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งาน และต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

4.1.1.2. การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)

(ผู้บริหารองค์กร) ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

4.2 หมวดที่ 2 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

4.2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)

มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

4.2.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)

(ผู้บริหารองค์กร) ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

4.2.1.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคง

ปลอดภัยให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้นจะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน

4.2.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)

(ผู้บริหารสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน

4.2.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities)

(ผู้บริหารสารสนเทศ) ต้องกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

4.2.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)

(หัวหน้างานบุคคล) ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างพนักงานนั้น) รวมทั้งเงื่อนไขหรือข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับจะต้องได้รับการปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร

4.2.1.6 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with authorities)

(ผู้บริหารสารสนเทศ) ต้องมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่นสำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ บมจ. ทศท คอร์ปอเรชัน บมจ. กสทโทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

4.2.1.7 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)

(ผู้บริหารองค์กรและหัวหน้างานสารสนเทศ) ต้องมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่มีความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ หรือสมาคมต่างๆ ในอุตสาหกรรมที่องค์กรมีส่วนร่วม

4.2.1.8 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent review of information security)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กร

4.2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)

มีจุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

4.2.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

4.2.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers)

(หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

4.2.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)

(หัวหน้างานสารสนเทศ) ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์กรและหน่วยงานภายนอก เมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กรก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

4.3 หมวดที่ 3 การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

4.3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) มีจุดประสงค์เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

4.3.1.1 การจัดทำบัญชีทรัพย์สิน (Inventory of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ

4.3.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดให้มีการระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ ตามที่กำหนดไว้ในบัญชีทรัพย์สิน

4.3.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) จะต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้นเช่น อันเกิดจากการขาดความระมัดระวัง การขาดการดูแลและเอาใจใส่ เป็นต้น

4.3.2 การจัดหมวดหมู่สารสนเทศ (Information classification)

มีจุดประสงค์เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

4.3.2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines)

(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม

4.3.2.2 การจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ (Information labeling and handling)

(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว

4.4 หมวดที่ 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

4.4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง (เช่น เพื่อการบำรุงรักษาอุปกรณ์ต่างๆ ขององค์กร) และหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

4.4.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับพนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และ/หรือหน่วยงานภายนอกที่องค์กรต้องการว่าจ้างมาปฏิบัติงานให้องค์กร และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

4.4.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องทำการตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) โดยละเอียด เช่น ตรวจสอบจาก

จดหมายรับรอง ประวัติการทำงานวุฒิการศึกษา บุคคลหรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และจะต้องพิจารณากฎหมาย ระเบียบ จริยธรรม ชั้นความลับของทรัพย์สินสารสนเทศ และระดับความเสี่ยงในการเข้าถึง ประกอบการคัดเลือกด้วย

4.4.1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment)

(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องกำหนดเงื่อนไขการจ้างงาน (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) ซึ่งรวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และบุคลากรที่จะได้รับการว่าจ้างดังกล่าวจะต้องเห็นชอบและลงนามในเงื่อนไขการจ้างงานนั้นด้วย

4.4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

4.4.2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)

(ผู้บริหารองค์กร) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

4.4.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education, and training)

(หัวหน้างานบุคคลและหัวหน้างานที่เกี่ยวข้อง) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงาน และผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอก ได้รับการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความ

มั่นคงปลอดภัยอย่างสม่ำเสมอ การอบรมควรครอบคลุมถึงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กรตามลักษณะงานที่พนักงานต้องรับผิดชอบด้วย

4.4.2.3 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary process)

(ผู้บริหารองค์กร) ต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

4.4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or change of employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

4.4.3.1 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination responsibilities)

(หัวหน้างานบุคคล) ต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่องค์กรเลิกการจ้างงานหรือองค์กรเปลี่ยนลักษณะการจ้างงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว

4.4.3.2 การคืนทรัพย์สินขององค์กร (Return of assets)

(หัวหน้างานบุคคลและหัวหน้างานพัสดุ) ต้องกำหนดให้ผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน

4.4.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)

(หัวหน้างานสารสนเทศและหัวหน้างานอาคาร) ต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน

4.5 หมวดที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

4.5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

4.5.1.1 การจัดทำบริเวณล้อมรอบ (Physical security perimeter)

(หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องมีการจัดสรรพื้นที่ กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า–ออกที่มีการควบคุม ตั้ง โต๊ะทำการของ รปภ. บริเวณทางเข้า–ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

4.5.1.2 การควบคุมการเข้า–ออก (Physical entry controls)

(หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องจัดให้มีการควบคุมการเข้า–ออก ในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า–ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

4.5.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing offices, rooms and facilities)

(หัวหน้างานอาคาร) ต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงานห้องทำงานและทรัพย์สินอื่นๆ

4.5.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)

(หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

4.5.1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)

(หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

4.5.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)

(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ควรจัดเป็นบริเวณแยกออกมาต่างหาก

4.5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)

มีจุดประสงค์เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่างๆขององค์กรเกิดการติดขัดหรือหยุดชะงัก

4.5.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)

(พนักงาน) ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

4.5.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบน้ำประปา ระบบควบคุมอุณหภูมิระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรอง ระบบสายสื่อสารสำรอง เป็นต้น

4.5.2.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)

(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องกำหนดให้เดินสายไฟฟ้าสายสื่อสาร และสายเคเบิ้ลอื่นๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย

4.5.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

4.5.2.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้นการป้องกันให้พิจารณาจากความเสี่ยงต่างๆ ที่มีต่ออุปกรณ์เหล่านั้น

4.5.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)

(พนักงาน) ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้งหรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

4.5.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)

(หัวหน้างานอาคาร) ต้องไม่อนุญาตการนำทรัพย์สินขององค์กร ได้แก่ อุปกรณ์สารสนเทศ หรือซอฟต์แวร์ ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น

4.6. หมวดที่ 6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)

4.6.1. การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)

มีจุดประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

4.6.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

(หัวหน้างานสารสนเทศ) ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงานปรับปรุงตามระยะเวลาอันสมควร และแจกจ่ายให้กับผู้ที่เกี่ยวข้อง

4.6.1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ (Change management)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือ แก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ

4.6.1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)

(ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจ) ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาตหรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร

4.6.1.4 การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต

4.6.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management)

มีจุดประสงค์เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

4.6.2.1 การให้บริการโดยหน่วยงานภายนอก (Service delivery)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการและระดับของการให้บริการ

4.6.2.2 การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and review of third party services)

(หัวหน้างานสารสนเทศ) ต้องตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่น การดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆ ที่กำหนดให้บันทึกไว้ เป็นต้น

4.6.2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changes to third party services)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยการเปลี่ยนเทคโนโลยีใหม่ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

4.6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System planning and acceptance)

มีจุดประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

4.6.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)

(หัวหน้างานสารสนเทศ) ต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน

4.6.3.2 การตรวจรับระบบ (System acceptance)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน

4.6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code)

มีจุดประสงค์เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

4.6.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)

(ผู้ดูแลระบบ) ต้องมีมาตรการสำหรับการตรวจจับ การป้องกันและการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย

4.6.4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code)

(ผู้ดูแลระบบ) ต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่(โปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่งเพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง) ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้

4.6.5 การสำรองข้อมูล (Back-up/Housekeeping)

มีจุดประสงค์เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

4.6.5.1 การสำรองข้อมูล (Information back-up)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร

4.6.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)

มีจุดประสงค์เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

4.6.6.1 มาตรการทางเครือข่าย (Network controls)

(ผู้ดูแลระบบ) ต้องบริหารและจัดการเครือข่าย กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอพพลิเคชั่นที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่าย

4.6.6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

(หัวหน้างานสารสนเทศ) ต้องกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่าย โดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก

4.6.7.การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling and security)

มีจุดประสงค์เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ

4.6.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

4.6.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว การทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย

4.6.7.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information handling procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์

4.6.7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

4.6.8 การแลกเปลี่ยนสารสนเทศ (Exchange of information)

มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

4.6.8.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ(Information exchange policies and procedures)

(ผู้บริหารองค์กร) ต้องกำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับ เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงานภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด

4.6.8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements)

(หัวหน้างานสารสนเทศ) ต้องจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ระหว่างองค์กร อย่างเป็นลายลักษณ์อักษร

4.6.8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical media in transit)

(หัวหน้างานสารสนเทศและหัวหน้างานธุรการ) ต้องป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร

4.6.8.4 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์

4.6.8.5 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems)

(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน

4.6.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน

4.6.9.1 การพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ที่มีการส่งผ่านทางเครือข่ายสาธารณะจากการฉ้อโกง การปฏิเสธ การเปิดเผย และการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

4.6.9.2 การทำธุรกรรมออนไลน์ (On-line transactions)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่งที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่าย

การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำลำเนาสารสนเทศโดยไม่ได้รับอนุญาต

4.6.9.3 สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly available information)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ

4.6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

มีจุดประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

4.6.10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย อย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

4.6.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

4.6.10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

4.6.10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ(Administrator and operator logs)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ

4.6.10.5 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้นและดำเนินการแก้ไขตามสมควร

4.6.10.6 การตั้ง เวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)

(ผู้ดูแลระบบ) ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

4.7 หมวดที่ 7 การควบคุมการเข้าถึง (Access control)

4.7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)

มีจุดประสงค์เพื่อควบคุมการเข้าถึงสารสนเทศ

4.7.1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ

4.7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)

มีจุดประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.7.2.1 การลงทะเบียนพนักงาน (User registration)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเปลี่ยนตำแหน่งงานภายในองค์กรเป็นต้น

4.7.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)

(ผู้ดูแลระบบ) ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

4.7.2.3 การบริหารจัดการรหัสผ่านผู้ใช้งาน (User password management)

(ผู้ดูแลระบบ) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย

4.7.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้

4.7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

4.7.3.1 การใช้งานรหัสผ่าน (Password use)

(ผู้ดูแลระบบ) ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน

4.7.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)

(พนักงาน) ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล

4.7.3.3 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)

(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย เช่นสามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น

4.7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

4.7.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)

(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายการใช้งานเครือข่าย ซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้

4.7.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

4.7.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)

(ผู้ดูแลระบบ) ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

4.7.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

(ผู้ดูแลระบบ) ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

4.7.4.5 การแบ่งแยกเครือข่าย (Segregation in networks)

(ผู้ดูแลระบบ) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ

4.7.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

(ผู้ดูแลระบบ) ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางธุรกิจได้ระบุไว้

4.7.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

(ผู้ดูแลระบบ) ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง

4.7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

4.7.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

(ผู้ดูแลระบบ) ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ

4.7.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)

(ผู้ดูแลระบบ) ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

4.7.5.3. ระบบบริหารจัดการรหัสผ่าน (Password management system)

(ผู้ดูแลระบบ) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

4.7.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)

(ผู้ดูแลระบบ) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว

4.7.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time out)

(ผู้ดูแลระบบ) ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้

4.7.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

(ผู้ดูแลระบบ) ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

4.7.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชันโดยไม่ได้รับอนุญาต

4.7.6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

(ผู้ดูแลระบบ) ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

4.7.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)

(หัวหน้างานสารสนเทศ) ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ

4.7.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

4.7.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)

(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้

4.7.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

(ผู้บริหารสนเทศ) ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

4.8 หมวดที่ 8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

4.8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information systems)

มีจุดประสงค์เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

4.8.1.1 การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย(Security requirements analysis and specification)

(ผู้พัฒนา และผู้เป็นเจ้าของระบบ) ต้องวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว

4.8.2 การประมวลผลสารสนเทศในแอพพลิเคชัน (Correct processing in applications)

มีจุดประสงค์เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์

4.8.2.1 การตรวจสอบข้อมูลนำเข้า (Input data validation)

(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับตรวจสอบข้อมูลนำเข้าของแอพพลิเคชันว่าข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป

4.8.2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of internal processing)

(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ เช่น อาจมีสาเหตุจากความผิดพลาดในการประมวลผล การกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น

4.8.2.3 การตรวจสอบความถูกต้องของข้อความ (Message integrity)

(ผู้พัฒนาระบบ) ต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอพพลิเคชัน (เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง)รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต

4.8.2.4 การตรวจสอบข้อมูลนำออก (Output data validation)

(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับการตรวจสอบข้อมูลนำออกจากแอพพลิเคชันเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม

4.8.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic controls)

มีจุดประสงค์เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการการเข้ารหัสข้อมูล

4.8.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้งานภายในองค์กร

4.8.3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key management)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานขององค์กร

4.8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับไฟล์ต่างๆ ของระบบที่ให้บริการ

4.8.4.1 การควบคุมการติดตั้ง ซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการนั้นเกิดความเสียหายทำงานผิดปกติ หรือไม่สามารถใช้งานได้

4.8.4.2 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of system test data)

(ผู้พัฒนาระบบ) ต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการสำหรับทำการทดสอบระบบ หากมีความจำเป็นต้องใช้ ต้องกำหนดให้มีการป้องกันและควบคุมการใช้งาน เช่น ควรลบทิ้งบางส่วนของข้อมูลที่เป็นความลับ ข้อมูลส่วนตัว หรือข้อมูลสำคัญ

4.8.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)

(หัวหน้างานสารสนเทศ) ต้องจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ ทั้งนี้เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาต หรือโดยไม่ได้เจตนา

4.8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in development and support processes)

มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

4.8.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้

4.8.5.2 การตรวจสอบการทำงานของแอพพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes)

(ผู้ดูแลระบบ) ต้องทำการตรวจสอบทางเทคนิคภายหลังจากที่ทำการเปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าแอพพลิเคชันที่ทำงานอยู่บนระบบปฏิบัติการนั้นทำงานผิดปกติ ไม่สามารถใช้งานได้ หรือมีปัญหาทางด้านความมั่นคงปลอดภัยเกิดขึ้นหรือไม่

4.8.5.3 การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต (Restrictions on changes to software packages)

(หัวหน้างานสารสนเทศ) ต้องหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นต้องแก้ไข ต้องแก้ไขตามความจำเป็นเท่านั้นและต้องมีการควบคุมการแก้ไขนั้นอย่างเข้มงวดด้วย

4.8.5.4 การป้องกันการรั่วไหลของสารสนเทศ (Information leakage)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กร หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป

4.8.5.5 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

4.8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

มีจุดประสงค์เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

4.8.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

4.9 หมวดที่ 9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

4.9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)

มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

4.9.1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events)

(พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้

4.9.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)

(พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

4.9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)

มีจุดประสงค์เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

4.9.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

4.9.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents)

(ผู้ดูแลระบบ) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

4.9.2.3 การเก็บรวบรวมหลักฐาน (Collection of evidence)

(หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้น นั้น มีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

4.10 หมวดที่ 10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

4.10.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร(Information security aspects of business continuity management)

มีจุดประสงค์เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

4.10.1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ กระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ

4.10.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)

(หัวหน้างานสารสนเทศ) ต้องระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้น ต่อความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

4.10.1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security)

(ผู้บริหารสารสนเทศ) ต้องจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินงานต่างๆ ให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงัก หรือล้มเหลว

4.10.1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ(Business continuity planning framework)

(ผู้บริหารสารสนเทศ) ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่างๆ ที่ต้องดำเนินการ

4.10.1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ(Testing, maintaining and re-assessing business continuity plans)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี

4.11 หมวดที่ 11 การปฏิบัติตามข้อกำหนด (Compliance)

4.11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)

มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ

4.11.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)

(หัวหน้างานนิติการ) ต้องระบุข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กร ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้น ให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

4.11.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights(IRP))

(หัวหน้างานนิติการ) ต้องกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา ขั้นตอนปฏิบัติดังกล่าวต้องกำหนดหรือควบคุมให้ปฏิบัติตามข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) รวมทั้งข้อกำหนดในการใช้งานผลิตภัณฑ์ซอฟต์แวร์จากผู้ขายด้วย

4.11.1.3 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of organizational records)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ จากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง

4.11.1.4 การป้องกันข้อมูลส่วนตัว (Data protection and privacy of personal information)

(หัวหน้างานนิติการ และหัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมาย ระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง

4.11.1.5 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์(Prevention of misuse of information processing facilities)

(หัวหน้างานสารสนเทศ) ต้องป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ประมวลผลสารสนเทศขององค์กรผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต

4.11.1.6 การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of cryptographic controls)

(หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องกำหนดให้ใช้มาตรการการเข้ารหัสข้อมูลโดยให้ยึดถือตาม หรือต้องสอดคล้องกับข้อตกลง กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

4.11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัย และข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance) มีจุดประสงค์เพื่อให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

4.11.2.1 การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย(Compliance with security policies and standards)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

4.11.2.2 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร(Technical compliance checking)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร

4.11.3 การตรวจประเมินระบบสารสนเทศ (Information systems audit considerations)

มีจุดประสงค์เพื่อให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

4.11.3.1 มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)

(หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ เช่นการหยุดชะงักของกระบวนการทางธุรกิจในระหว่างที่ทำการตรวจประเมิน

4.11.3.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ(Protection of information systems audit tools)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (เช่น ซอฟต์แวร์ที่ใช้ในการตรวจประเมิน) เพื่อป้องกันการใช้งานผิดวัตถุประสงค์ หรือการเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต

มาตราการณ์ในการรักษาความมั่นคงปลอดภัยสารสนเทศที่ได้กล่าวมานี้ ผู้วิจัยได้ใช้เป็นตัวแปรในการวิจัยครั้งนี้ โดยเป็นองค์ประกอบของมาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ดังนี้ 1) นโยบายความมั่นคงปลอดภัย 2) โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร 3) การบริหารจัดการทรัพย์สินขององค์กร 4) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร 5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม 6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร 7) การควบคุมการเข้าถึง 8) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ 9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร 10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร 11) การปฏิบัติตามข้อกำหนด

ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงระบบเทคโนโลยีสารสนเทศ

จากการศึกษาค้นคว้างานวิจัยที่เกี่ยวข้อง ปัจจัยที่ส่งผลต่อการจัดการความมั่นคงระบบเทคโนโลยีสารสนเทศ แสดงดังตาราง 3

ตาราง 3 ตัวแปรที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ

เอกสารและงานวิจัย	งบประมาณด้านระบบเทคโนโลยีขององค์กร	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	เทคโนโลยีด้านความมั่นคงปลอดภัยที่องค์กรเลือกใช้	การอัพเดทแพทช์ของซอฟแวร์และระบบปฏิบัติการที่ใช้งาน	ความตระหนักต่อความมั่นคงปลอดภัยสารสนเทศ	กฎหมาย	นโยบายของผู้บริหาร	ความสามารถของบุคลากรในการใช้งานระบบเทคโนโลยีสารสนเทศ	ความถี่ในการทบทวนแผน(ต่อปี)	ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ	การสร้างความมั่นใจให้ลูกค้า	การสร้างความได้เปรียบทางการแข่งขันทางธุรกิจ	ความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศ	การให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	การขาดแคลนผู้เชี่ยวชาญ	ความสำคัญของข้อมูล	ระบบเครือข่ายขององค์กร	สภาพแวดล้อมทางกายภาพของข้อมูล
การศึกษาสถานะปัจจุบันของภัยคุกคามในกลุ่มธุรกิจพาณิชย์อิเล็กทรอนิกส์ของประเทศไทย (ศักดิ์สิริ แจ่มศักดิ์, 2552)	✓		✓	✓	✓													
การสำรวจภัยคุกคามทางคอมพิวเตอร์และการรักษาความปลอดภัยข้อมูลสารสนเทศ ของธนาคารพาณิชย์ในประเทศไทย (วศิน รำพึงกิจ 2552)		✓	✓		✓	✓												

ตาราง 3 (ต่อ)

เอกสารและงานวิจัย	งบประมาณด้านระบบเทคโนโลยีขององค์กร	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	เทคโนโลยีด้านความมั่นคงปลอดภัยที่องค์กรเลือกใช้	การอัพเดทแพทช์ของซอฟแวร์และระบบปฏิบัติการที่ใช้งาน	ความตระหนักต่อความมั่นคงปลอดภัยสารสนเทศ	กฎหมาย	นโยบายของผู้บริหาร	ความสามารถของบุคลากรในการใช้งานระบบเทคโนโลยีสารสนเทศ	ความถี่ในการทบทวนแผน(ต่อปี)	ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ	การสร้างความมั่นใจให้ลูกค้า	การสร้างความได้เปรียบทางการแข่งขันทางธุรกิจ	ความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศ	การให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	การขาดแคลนผู้เชี่ยวชาญ	ความสำคัญของข้อมูล	ระบบเครือข่ายขององค์กร	สภาพแวดล้อมทางกายภาพของข้อมูล
การวิเคราะห์ปัจจัยที่มีผลต่อการบริหารเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันอุดมศึกษาไทย (บรรจง เขื่อนแก้ว และคณะ, 2553)	✓	✓					✓	✓					✓					
ความรู้เบื้องต้นเกี่ยวกับความมั่นคงปลอดภัย (สุชาดา สิทธิ์จงสถาพร, 2556)		✓			✓		✓	✓										
การศึกษาแนวทางการพัฒนานโยบายความมั่นคงปลอดภัยสารสนเทศภายในองค์กร กรณีศึกษา บริษัท NEC Corporation (Thailand) Ltd. (ภูมินทร์ ภูดวงสี, 2550)					✓				✓	✓	✓	✓						

ตาราง 3 (ต่อ)

เอกสารและงานวิจัย	งบประมาณด้านระบบเทคโนโลยีขององค์กร	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	เทคโนโลยีด้านความมั่นคงปลอดภัยที่องค์กรเลือกใช้	การอัพเดทแพทช์ของซอฟแวร์และระบบปฏิบัติการที่ใช้งาน	ความตระหนักต่อความมั่นคงปลอดภัยสารสนเทศ	กฎหมาย	นโยบายของผู้บริหาร	ความสามารถของบุคลากรในการใช้งานระบบเทคโนโลยีสารสนเทศ	ความถี่ในการทบทวนแผน(ต่อปี)	ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ	การสร้างความมั่นใจให้ลูกค้า	การสร้างความได้เปรียบทางการแข่งขันทางธุรกิจ	ความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศ	การให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	การขาดแคลนผู้เชี่ยวชาญ	ความสำคัญของข้อมูล	ระบบเครือข่ายขององค์กร	สภาพแวดล้อมทางกายภาพของข้อมูล
แนวทางการนำ Information Security Management มาใช้ในการจัดระเบียบการบริหารจัดการด้านความปลอดภัยสารสนเทศ กรณีศึกษา : บริษัทให้คำปรึกษาด้านสารสนเทศแห่งหนึ่ง (วราภรณ์ ธวิทย์ชัยพร, 2549)										✓	✓	✓				✓	✓	✓
การสร้างมาตรฐานทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้ และสอดคล้องกับ					✓		✓	✓	✓	✓			✓	✓				

ตาราง 3 (ต่อ)

เอกสารและงานวิจัย	งบประมาณด้านระบบเทคโนโลยีขององค์กร	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	เทคโนโลยีด้านความมั่นคงปลอดภัยที่องค์กรเลือกใช้	การอัพเดทแพทช์ของซอฟแวร์และระบบปฏิบัติการที่ใช้งาน	ความตระหนักต่อความมั่นคงปลอดภัยสารสนเทศ	กฎหมาย	นโยบายของผู้บริหาร	ความสามารถของบุคลากรในการใช้งานระบบเทคโนโลยีสารสนเทศ	ความถี่ในการทบทวนแผน(ต่อปี)	ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ	การสร้างความมั่นใจให้ลูกค้า	การสร้างความได้เปรียบทางการแข่งขันทางธุรกิจ	ความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศ	การให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	การขาดแคลนผู้เชี่ยวชาญ	ความสำคัญของข้อมูล	ระบบเครือข่ายขององค์กร	สภาพแวดล้อมทางกายภาพของข้อมูล
พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550: กรณีศึกษาองค์กรกระจายเสียง และแพร่ภาพสาธารณะแห่งประเทศไทย (วิภาวรรณ คุ้มศิริ, 2552)																		
การวิเคราะห์ปัจจัยและสร้างโมเดลทำนายความเสี่ยงของการเกิดภัยคุกคามความปลอดภัยของระบบสารสนเทศในองค์กรของประเทศไทย (ธนาวรรณ จันทรัตนไพบูล และคณะ, 2556)	✓	✓	✓		✓									✓	✓			

ตาราง 3 (ต่อ)

เอกสารและงานวิจัย	งบประมาณด้านระบบเทคโนโลยีขององค์กร	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	เทคโนโลยีด้านความมั่นคงปลอดภัยที่องค์กรเลือกใช้	การอัพเดทแพทช์ของซอฟแวร์และระบบปฏิบัติการที่ใช้งาน	ความตระหนักต่อความมั่นคงปลอดภัยสารสนเทศ	กฎหมาย	นโยบายของผู้บริหาร	ความสามารถของบุคลากรในการใช้งานระบบเทคโนโลยีสารสนเทศ	ความถี่ในการทบทวนแผน(ต่อปี)	ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ	การสร้างความมั่นใจให้ลูกค้า	การสร้างความได้เปรียบทางการแข่งขันทางธุรกิจ	ความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศ	การให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	การขาดแคลนผู้เชี่ยวชาญ	ความสำคัญของข้อมูล	ระบบเครือข่ายขององค์กร	สภาพแวดล้อมทางกายภาพของข้อมูล
การศึกษาระบบความมั่นคงปลอดภัยด้านสารสนเทศสำหรับบริการทางด้านการเงินผ่านอินเตอร์เน็ต กรณีศึกษา: ธนาคารพาณิชย์แห่งหนึ่ง (หนึ่งฤทัย เตชะรัตนประเสริฐ, 2552)						✓				✓								
การจัดทำแนวทางการปฏิบัติ ในการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศด้วยมาตรฐาน ISO/IEC 27001 กรณีศึกษา : สำนักงานรัฐบาลอิเล็กทรอนิกส์ (มหาชน) (สรอ.) (รัชชาภรณ์ สุภาพ, 2557)										✓								

จากตัวแปรปัจจัยที่ส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ ผู้วิจัยวิเคราะห์เนื้อหาและจัดกลุ่มปัจจัยตามปัจจัยภายในองค์กรและปัจจัยนอกองค์กร ดังนี้

รายละเอียดของแต่ละตัวแปรมีดังนี้

1. ปัจจัยภายในองค์กร

1.1 แผนงานและงบประมาณด้านระบบสารสนเทศขององค์กร การดำเนินการในภาคธุรกิจมักจะเริ่มต้นด้วยการวางแผนเสมอ เพราะการวางแผนถือเป็นส่วนประกอบสำคัญที่จะนำพาให้องค์กรไปสู่เป้าหมายด้วยวิธีการอย่างมีแบบแผน มีทิศทางกระบวนการทำงานอย่างมีระบบ โดยผลลัพธ์ที่ได้จากกระบวนการวางแผนคือแผนงาน (Plan) ซึ่งประกอบด้วยกิจกรรมในรูปแบบต่างๆ ที่มีความชัดเจน ทำให้ทีมงานยึดถือ และปฏิบัติตาม เพื่อให้บรรลุถึงผลสำเร็จตามเป้าหมาย ดังนั้นแผนงานจะนำไปสู่การลงมือปฏิบัติ การวางแผนระบบสารสนเทศ ประกอบด้วยขั้นตอนสร้างพันธกิจระดับองค์กรและพันธกิจทางระบบสารสนเทศ, กำหนดวิสัยทัศน์ที่ชัดเจนต่อการนำระบบสารสนเทศมาใช้กับองค์กร สร้างกลยุทธ์ทางไอทีและแผนยุทธวิธีขึ้นมา วางแผนการปฏิบัติงานเพื่อนำไปสู่เป้าหมายตามพันธกิจและวิสัยทัศน์ และขั้นตอนสุดท้ายเป็นการกำหนดงบประมาณด้านระบบสารสนเทศและการจัดหาทรัพยากรเพื่อนำไปสู่เป้าหมายตามพันธกิจและวิสัยทัศน์ (โอภาส เอี่ยมสิริวงศ์, 2554, หน้า 500–506)

1.2 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร นโยบาย คือ หลักการและวิธีปฏิบัติซึ่งถือเป็นแนวดำเนินการ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ คือ หลักการและวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรที่ดี ส่งผลให้ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศที่มี ส่งผลให้เกิดความเสียหายอยู่ในเกณฑ์ต่ำ เนื่องจากมีมาตรการในการตรวจสอบและควบคุมที่เหมาะสม การกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรยังเป็นการสร้างความมั่นใจให้แก่ผู้ที่มาใช้บริการขององค์กร ซึ่งเป็นการสร้างความได้เปรียบทางการแข่งขันทางธุรกิจ (วศิน รำพึงกิจ, 2552, หน้า 105; ภูมินทร์ ภูดวงสี, 2550, หน้า 129)

1.3 ฮาร์ดแวร์ (Hardware) ประกอบด้วยอุปกรณ์ทุกชนิดที่อยู่ในระดับกายภาพของระบบสารสนเทศ เป็นอุปกรณ์ที่เราสามารถมองเห็นและสัมผัสได้ ซึ่งประกอบด้วย ระบบคอมพิวเตอร์ อุปกรณ์รอบข้าง และอุปกรณ์เครือข่าย ซึ่งฮาร์ดแวร์จะ

ถูกควบคุมโดยซอฟต์แวร์ (โอภาส เอี่ยมสิริวงศ์, 2554, หน้า 25; O' Leary T. J. และ O'Leary L.6 I., 2013 หน้า 4)

1.4 ซอฟแวร์ คือกลุ่มของชุดคำสั่ง หรือโปรแกรมที่นำมาใช้ควบคุมการทำงานของอุปกรณ์ฮาร์ดแวร์ ด้วยการสั่งให้คอมพิวเตอร์รับข้อมูลเข้ามาอย่างไร ประมวลผลอย่างไร แสดงผลอย่างไร และจัดเก็บข้อมูลหรือแสดงผลสารสนเทศอย่างไร หน้าที่หลักของซอฟต์แวร์มีสามประการ คือ (1) บริหารจัดการทรัพยากรคอมพิวเตอร์ขององค์กร (2) จัดเตรียมเครื่องมือสำหรับให้ผู้ใช้สามารถใช้งานทรัพยากรได้อย่างสะดวก และ (3) ทำหน้าที่เป็นตัวกลางระหว่างองค์กรและสารสนเทศที่เก็บรักษาไว้ โดยซอฟแวร์มีสองประเภท ได้แก่ ซอฟต์แวร์ระบบ (System Software) คือซอฟต์แวร์ที่ออกแบบสำหรับการจัดการทรัพยากรของระบบคอมพิวเตอร์ และซอฟต์แวร์ประยุกต์ (Application Software) คือซอฟต์แวร์ที่สร้างขึ้นเพื่อใช้งานเฉพาะด้านใดด้านหนึ่ง (โอภาส เอี่ยมสิริวงศ์, 2554, หน้า 25; Laudon K. C., Laudon J. P, 2002, หน้า 114)

1.5 บุคลากร คือ บุคคลที่มีส่วนได้ส่วนเสียในระบบสารสนเทศ บุคลากรแบ่งได้เป็น 2 กลุ่ม คือ บุคลากรทั่วไป และบุคลากรฝ่ายเทคนิค บุคลากรทั่วไปเป็นผู้ใช้งานระบบสารสนเทศ และบุคลากรฝ่ายเทคนิคจะเป็นผู้ดูแลระบบสารสนเทศขององค์กร บุคลากรส่งผลต่อการจัดการความมั่นคงปลอดภัยสารสนเทศ บุคลากรทั่วไปขององค์กรได้รับการฝึกอบรมให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีความตระหนักต่อความมั่นคงปลอดภัยสารสนเทศ ทราบถึงความสำคัญของสารสนเทศขององค์กร อันส่งผลดีต่อความมั่นคงปลอดภัยสารสนเทศขององค์กร ส่วนบุคลากรฝ่ายเทคนิคต้องมีความชำนาญ มีความรู้ทางด้านสายงาน และมีความรู้ทางด้านความมั่นคงปลอดภัยสารสนเทศ และต้องมีการฝึกอบรมเพื่อเพิ่มความรู้ความชำนาญแก่บุคลากรฝ่ายเทคนิค (ภูมินทร์ ภูดวงศรี, 2550, หน้า 131; วิภาวรรณ คุ้มสิริ, 2552, หน้า 194; โอภาส เอี่ยมสิริวงศ์, หน้า 25)

1.6 ผู้บริหาร เป็นผู้ที่มีอำนาจหน้าที่ในการวางนโยบาย แผนงาน การบริหารจัดการ จัดสรรทรัพยากรมนุษย์และเงินทุน และประสานการทำงานเพื่อให้บรรลุวัตถุประสงค์ขององค์กร ผู้บริหารจำเป็นจะต้องเป็นบุคคลที่มีความรับผิดชอบสูงซึ่งจะต้องเป็นผู้นำที่สามารถบริหารงานช่วยให้องค์กรฟันฝ่าอุปสรรคทั้งหลายไปได้ บทบาทและความรับผิดชอบในการตัดสินใจของผู้บริหารในแต่ละระดับนั้นแตกต่างกัน ผู้บริหารอาวุโส (Senior manager) กำหนดแนวทางการผลิตสินค้าและบริการในระยะยาว ผู้บริหาร

ระดับกลาง (middle managers) พัฒนาแผนการปฏิบัติงานขึ้นมาเพื่อรองรับแผนการระยะยาวที่ผู้บริหารอาวุโสกำหนด ส่วนผู้บริหารระดับปฏิบัติการ (operation managers) ควบคุมรับผิดชอบการปฏิบัติงานที่เกิดขึ้นในแต่ละวันให้เป็นไปด้วยความเรียบร้อย ผู้บริหารแต่ละระดับจำเป็นต้องมีแนวทางในการพัฒนางานที่ตนเองรับผิดชอบ ส่วนงานด้านระบบสารสนเทศมีผู้บริหารสารสนเทศระดับสูง (Chief Information Officer: CIO) เป็นบุคคลผู้มีอำนาจสูงสุดในส่วนงาน เป็นผู้นำบทบาทของเทคโนโลยีสารสนเทศมาใช้กับองค์กร ด้วยการวางนโยบาย แผนงาน การบริหารจัดการ และการจัดหาระบบสารสนเทศ ส่วนงานด้านความมั่นคงปลอดภัยมีผู้บริหารความปลอดภัยระดับสูง (Chief Security Officer : CSO) เป็นผู้รับผิดชอบงานด้านความมั่นคงปลอดภัยสารสนเทศ เป็นผู้กำหนดนโยบาย และการจัดการความปลอดภัยด้านระบบสารสนเทศ (โอภาส เอี่ยมสิริวงศ์, 2554, หน้า 48–51; Laudon K. C., Laudon J. P, 2002, หน้า 10)

1.7 ผู้รับบริการ คือ ผู้ที่ได้รับบริการขององค์กร หรือในทางธุรกิจเรียกว่าลูกค้า ในการสร้างความเชื่อมั่นและสร้างความไว้วางใจให้กับลูกค้าทำให้องค์กรต้องมีการพัฒนาในหลายด้าน รวมถึงการจัดการความมั่นคงปลอดภัยสารสนเทศ (ภูมินทร์ ภูดวงสี (2550, หน้า 129; วราภรณ์ ธวิทย์ชัยพร, 2549)

1.8 ข้อมูล คือข้อเท็จจริง ที่ได้รับการรวบรวมและป้อนเข้าสู่ระบบข้อมูลมีหลายรูปแบบ เช่น ตัวอักษร ตัวเลข รูปภาพ วิดีโอ และเสียง ข้อมูลเหล่านี้อาจถูกจัดเก็บไว้ในลักษณะของรายละเอียด เรคอร์ด แฟ้มข้อมูล หรือฐานข้อมูล ซึ่งถือว่าเป็นข้อมูลที่ยังไม่สามารถนำมาใช้ประโยชน์ได้ทันที แต่จะเตรียมไว้เพื่อรอการประมวลผลซึ่งข้อมูลเมื่อได้รับการประมวลผลหรือปรับแต่งให้เป็นประโยชน์ต่อผู้ใช้ จะเรียกว่าสารสนเทศ (Information) (โอภาส เอี่ยมสิริวงศ์, 2554, หน้า 25; Laudon K. C and Laudon J. P, 2002, หน้า 6)

2. ปัจจัยภายนอกองค์กร

2.1 กฎหมาย กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ มีหลายฉบับ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550, พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 เป็นต้น การบังคับใช้กฎหมาย พระราชบัญญัติต่างๆ ที่เกี่ยวข้องทำให้องค์กรต้องปฏิบัติตาม ส่งผลให้องค์กรต้องทบทวนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเพิ่มระดับของการ

รักษาความมั่นคงปลอดภัยและสร้างความเชื่อมั่นแก่ผู้รับบริการ พร้อมทั้งยังเป็นการปฏิบัติตามกฎหมาย (วศิน รำพึงกิจ 2552, หน้า 54–58; หนึ่งฤทัย เตชะรัตนประเสริฐ, 2552)

2.2 ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ หมายถึง วัตถุ สิ่งของ หรือสิ่งใดๆ ที่ก่อให้เกิดความเสียหายต่อคุณลักษณะความมั่นคงปลอดภัยสารสนเทศด้านใดด้านหนึ่ง หรือมากกว่าหนึ่งด้าน ตัวอย่างของภัยคุกคามความมั่นคงปลอดภัย เช่น การโจมตีด้วยซอฟต์แวร์ที่ไม่หวังดี ภัยธรรมชาติ เป็นต้น

บริบทกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

1. ประวัติความเป็นมาของกลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร

กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร ประกอบด้วยโรงพยาบาลโคกศรีสุพรรณ ซึ่งเป็นโรงพยาบาลชุมชน คือ โรงพยาบาลโคกศรีสุพรรณ และโรงพยาบาลส่งเสริมสุขภาพตำบล 5 แห่ง คือ รพ.สต.ห้วยหีบรุ่งอรุณ รพ.สต.เหล่าโพนค้อ รพ.สต.ม่วงไข่น้อย รพ.สต.โคกนาดี รพ.สต.โพนทองวัฒนา รับผิดชอบบริการด้านการแพทย์แก่ประชาชนในอำเภอโคกศรีสุพรรณ กลุ่มเครือข่ายสุขภาพ อำเภอโคกศรีสุพรรณ มีกำลังหลักในการให้บริการทางด้านการแพทย์คือ โรงพยาบาลโคกศรีสุพรรณ ซึ่งเป็นโรงพยาบาลชุมชนขนาด 30 เตียง กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ ได้ประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศเพื่อให้บริการโดยการนำระบบ HoSxp สำหรับให้บริการในโรงพยาบาลชุมชน และ HoSxp PCU สำหรับให้บริการในโรงพยาบาลส่งเสริมสุขภาพตำบล โดยระบบ HoSxp และ HoSxp PCU เป็นระบบเวชระเบียนและยา การใช้งานระบบ HoSxp ครอบคลุมตั้งแต่ระบบคิว ระบบผู้ป่วยนอก ระบบผู้ป่วยใน รวมถึงระบบห้องตรวจต่างๆ ระบบห้องยา จนถึงระบบการออกใบเสร็จ รวมถึงการทำรายงานต่างๆ ส่งให้หน่วยงานต้นสังกัด (ผิน ฮ่มป่า, สัมภาษณ์, 22 มิถุนายน 2558)

2. นโยบายด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ

สำนักงานปลัดกระทรวงสาธารณสุข มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของกระทรวงสาธารณสุขขึ้น และประกาศที่ทุกหน่วยงานที่เกี่ยวข้องรับทราบ และนำไปปฏิบัติ ตามประกาศใน

หนังสือ ที่ สธ 0202.05/ว 473 เมื่อวันที่ 28 กรกฎาคม 2553 โดยมีวัตถุประสงค์เพื่อให้ระบบเทคโนโลยีสารสนเทศของกระทรวงสาธารณสุข เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กระทรวงสาธารณสุขและหน่วยงานในสังกัด และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายที่เกี่ยวข้อง

อาศัยความในมาตรา 5 และมาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 กระทรวงสาธารณสุขได้จัดทำร่างนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้หน่วยงานใช้เป็นแนวทางในการดำเนินการในทิศทางเดียวกัน ได้มีมติเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ในการประชุมครั้งที่ 10/2555 เมื่อวันอังคารที่ 11 ธันวาคม 2555 เห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารด้านสารสนเทศตามรายละเอียดในประกาศสำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ 0202.05/ว26 เมื่อวันที่ 9 มกราคม 2556

จากการสัมภาษณ์ผู้ดูแลระบบสารสนเทศของโรงพยาบาลโคกศรีสุพรรณ (ผิน ฮ่มป่า ,สัมภาษณ์, 22 มิถุนายน 2558) พบว่ากลุ่มเครือข่ายบริการสุขภาพไม่มีนโยบายความมั่นคงปลอดภัยระบบสารสนเทศที่เป็นลายลักษณ์อักษร แต่ทางกลุ่มเครือข่ายบริการสุขภาพ ได้ดำเนินการด้านความมั่นคงปลอดภัยระบบสารสนเทศ ดังนี้

2.1 การใช้งานระบบ HoSxp

2.1.1 เจ้าหน้าที่ของโรงพยาบาลเข้าใช้งานระบบ HoSxp ด้วย Account ของตนเองเท่านั้น

2.1.2 การเข้าถึงข้อมูลของผู้ป่วย จำกัดสิทธิ์ให้เข้าถึงได้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น โดยการกำหนดสิทธิ์การเข้าถึงข้อมูล ต้องกระทำโดยผู้ดูแลระบบเทคโนโลยีสารสนเทศที่ได้รับการแต่งตั้งจากโรงพยาบาลเท่านั้น

2.1.3 ห้ามเปิดเผยข้อมูลการรักษาผู้ป่วยแก่สาธารณะ

2.2 การใช้งานอินเตอร์เน็ต

2.2.1 เจ้าหน้าที่ของโรงพยาบาลเข้าใช้งานอินเตอร์เน็ตด้วย Account ของตนเองเท่านั้น

2.3 การใช้งานคอมพิวเตอร์

2.3.1 การติดตั้งซอฟแวร์บนเครื่องคอมพิวเตอร์ ต้องได้รับการติดตั้งโดยผู้ดูแลระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

งานวิจัยที่เกี่ยวข้อง

1. งานวิจัยในประเทศ

เฉลิม สุวรรณะ (2554) ได้ทำการศึกษาเรื่อง การรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา ศูนย์การแพทย์สมเด็จพระเทพรัตนราชสุดาฯสยามบรมราชกุมารี พบว่า การจัดการความมั่นคงของโรงพยาบาลหลังจากที่ได้ปรับปรุงตามมาตรฐาน ISO/IEC27001:2005 โดยการประเมินความเสี่ยง และดำเนินการแก้ไขเพื่อลดความเสี่ยงตามหัวข้อที่องค์กรให้ความสำคัญก่อนนั้น ผลการแก้ไข ทำให้ความเสี่ยงต่อภัยคุกคามความมั่นคงลดลงอยู่ในระดับกลางและต่ำ

วศิน รำพึงกิจ (2552) ได้ทำการศึกษาเรื่อง การสำรวจภัยคุกคามทางคอมพิวเตอร์และการรักษาความปลอดภัยข้อมูลสารสนเทศ ของธนาคารพาณิชย์ในประเทศไทย พบว่า จากการที่ได้ศึกษาสภาพปัญหาปัจจุบัน จากนั้นจึงได้อ้างอิงมาตรฐาน ISO/IEC27001:2005 เพื่อแนะแนวทางในการแก้ปัญหาในเชิงนโยบายการจัดการ และลดความเสี่ยงของภัยคุกคามความมั่นคงระบบเทคโนโลยีสารสนเทศให้อยู่ในระดับที่ต่ำลง

วิภาวรรณ คุ้มศิริ (2552) ที่ได้ทำการศึกษาเรื่อง การสร้างมาตรการด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC27001 มาประยุกต์ใช้ และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กรณีศึกษาองค์กรกระจายเสียง และแพร่ภาพแห่งประเทศไทย โดยงานวิจัยมีวัตถุประสงค์เพื่อลดความเสี่ยงต่างๆ ที่เกิดขึ้นกับระบบสารสนเทศภายในองค์กรฯ โดยการใช้มาตรฐาน ISO/IEC27001 เป็นแนวทางปฏิบัติ ผลการศึกษาพบว่าจากการสำรวจการดำเนินงาน ตามมาตรฐาน ISO/IEC 27001 ทั้ง 11 หมวด พบว่าองค์กรฯ ได้ดำเนินการตามมาตรรฐาน ISO/IEC27001 แล้วเสร็จ คิดเป็นร้อยละ 33.84 และกำลังดำเนินการคิดเป็นร้อยละ 10.53 และอีกร้อยละ 55.63 ที่องค์กรฯ ยังไม่เริ่มดำเนินการ

ว่าที่ร้อยตรี ภูมินทร์ ภูดวงสี (2550) ได้ทำการศึกษาเรื่อง การศึกษาแนวทางการพัฒนานโยบายความมั่นคงปลอดภัยสารสนเทศภายในองค์กร กรณีศึกษา

บริษัท NEC Corporation (Thailand) Ltd. พบว่า จากการศึกษาข้อมูลนโยบายความมั่นคงปลอดภัยสาสนเทศขององค์กรและการประเมินความเสี่ยงขององค์กร โดยอ้างอิงมาตรฐาน ISO/IEC27001:2005 และจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กรทำให้ความเสี่ยงภัยคุกคามด้านต่างๆ ลดลง

2. งานวิจัยต่างประเทศ

Eijiroh Ohki, Yonosuke Harada, Shuji Kawaguchi, Tetsuo Shiozaki and Tetsuyuki Kagaua (2009) ได้ทำการศึกษาเรื่อง Information Security Governance Framework ผลจากการศึกษาทำให้ได้ Information Security Governance model ใหม่ ซึ่งเป็นโมเดลสำหรับการบริหารจัดการความมั่นคงปลอดภัยภายในองค์กร ประกอบไปด้วยกระบวนการ DIRECT, MONITOR, EVALUATE, OVERSEE และ REPORT โดยกระบวนการทั้ง 5 กระบวนการนี้ครอบคลุมฟังก์ชันที่ขาดหายไปของการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

Mehrdad Sepehri Sharbaf (2014) ได้ทำการศึกษาเรื่อง A New Perspective to Information Security: Total Quality Information Security Management งานวิจัยนี้ได้นำเสนอแนวคิดใหม่ในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยการออกแบบการพัฒนาและการสร้างแบบจำลอง TQISM เพื่อการรักษาความมั่นคงสารสนเทศ และสินทรัพย์ขององค์กร TQISM เป็นการรวมของการรักษาความมั่นคงปลอดภัยสารสนเทศและการบริหารจัดการโดยที่ผู้บริหารและพนักงานมีส่วนร่วมในการพัฒนาอย่างต่อเนื่อง