คู่มือ
การจัดทำระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมทรัพยากรน้ำบาดาล

โดย

นายไพศาล ลักขณานุรักษ์
รักษาการผู้เชี่ยวชาญด้านนโยบายและแผน

กรมทรัพยากรน้ำบาดาล
กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
เมษายน ๒๕๕๕

คำนำ

ปัจจุบันระบบเครือข่ายคอมพิวเตอร์มีความสำคัญต่อการดำเนินงานของทุกองค์กรที่ต้องการทำให้การเข้าถึงข้อมูลมีความรวดเร็ว ถูกต้อง แม่นยำ สามารถติดต่อสื่อสารได้อย่างมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงาน ประกอบกับการพัฒนาอย่างรวดเร็วของระบบเครือข่ายอินเตอร์เน็ต ส่งผลให้การเชื่อมต่อระหว่างระบบเครือข่ายคอมพิวเตอร์ขององค์กรกับระบบเครือข่ายอินเตอร์เน็ตมีความจำเป็นและมีการใช้งานกันอย่างแพร่หลาย

ระบบเครือข่ายอินเตอร์เน็ตนั้นมีทั้งในแง่ดีซึ่งมากมายเกินกว่าจะกล่าวถึง แต่ในแง่ที่ไม่ดีก็มีมากมายเช่นกัน เหตุผลก็เนื่องจากระบบเครือข่ายอินเตอร์เน็ตนั้นเปรียบเสมือนห้องสมุด เป็นแหล่งการเรียนรู้ เป็นแหล่งสืบค้นที่ใหญ่ที่สุดในโลก เราต้องการทราบข้อมูลอะไรก็สามารถค้นหาได้จากเครือข่ายอินเตอร์เน็ต แต่ในแง่ของผู้ไม่ประสงค์ดีก็ใช้ช่องทางนี้เช่นกันในการสืบค้นข้อมูล เครื่องมือ หรือค้นหาวิธีการในการเจาะระบบเครือข่าย ทำให้ระบบเครือข่ายขององค์กรมีโอกาสถูกบุกรุกได้มากขึ้น ผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสารจึงควรตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กรอย่างจริงจัง

หวังเป็นอย่างยิ่งว่า คู่มือ “การจัดทำระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำบาดาล” ฉบับนี้ จะเป็นประโยชน์แก่ผู้บริหาร และบุคลากรที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมทรัพยากรน้ำบาดาล ในการจัดทำระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต่อไป

ไพศาล ลักขณานุรักษ์

เมษายน ๒๕๕๕

กิตติกรรมประกาศ

“คู่มือการจัดทำระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำบาดาล” ฉบับนี้ จะไม่สามารถสำเร็จลงได้หากไม่ได้รับความเห็นชอบจากบุคคลที่มีความรู้ความสามารถหลายท่านที่ทำให้เกิดเป็นคู่มือฉบับนี้ และสามารถนำไปใช้เป็นแนวทางในการจัดทำระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทรัพยากรน้ำบาดาลต่อไป ซึ่งประกอบไปด้วย อธิบดีกรมทรัพยากรน้ำบาดาล นายปราณีต ร้อยบาง และรองอธิบดีกรมทรัพยากรน้ำบาดาลอีกสองท่าน นายสัมฤทธิ์ ชุษณะทัศน์ และ นายสุพจน์ เจิมสวัสดิพงษ์ รวมถึงผู้เชี่ยวชาญ นายกมลศักดิ์ บัวอ่อน ที่ช่วยสนับสนุนให้เกิดคู่มือฉบับนี้ตั้งแต่ต้นจนเสร็จสิ้น ผู้จัดทำขอขอบพระคุณทุกท่านมา ณ ที่นี้

ขอขอบคุณ นางสาววรีวสยา สินธุเดชะ ที่ให้คำแนะนำ ตรวจทาน และแก้ไขข้อบกพร่องของข้อความต่าง ๆ ด้วยความเอาใจใส่ทุกขั้นตอน

ขอขอบคุณ นายมานพ สาทถาพร นายจตุพล สารีบทและทีมงาน ที่ให้ความช่วยเหลือในการตรวจสอบ และแก้ไขข้อบกพร่องของรูปแบบเอกสาร

สุดท้ายนี้ ต้องขอขอบคุณทุกท่านที่คอยให้กำลังใจ และถามไถ่ความเป็นไปของเอกสารผลงานอยู่เสมอโดยเฉพาะอย่างยิ่ง ท่านอธิบดีและท่านรองอธิบดีทั้งสองท่าน ทำให้ผู้จัดทำมีกำลังใจในการจัดทำผลงานจนสำเร็จได้

ไพศาล ลักขณานุรักษ์

เมษายน ๒๕๕๕

สารบัญ

สารบัญภาพ

บทที่ ๑

บทนำ

การบริหารงานขององค์กรทุกประเภท ทั้งภาครัฐและภาคเอกชน ต่างมีวัตถุประสงค์ของตนเองและมุ่งหวังที่จะทำงานไปให้ถึงเป้าหมายที่วางไว้อย่างดีที่สุด สูญเสียทรัพยากรให้น้อยที่สุด แต่การดำเนินการใด ๆ เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ มักจะต้องประสบกับความเสี่ยงที่จะเกิดความผิดพลาด ความเสียหาย ความสูญเปล่าหรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจเกิดขึ้นอย่างเฉียบพลันหรืออาจเริ่มต้นเพียงเล็กน้อยแล้วเพิ่มความรุนแรงต่อไปเรื่อย ๆ ซึ่งจะมีผลกระทบทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์ เป้าประสงค์ และเป้าหมายขององค์กร

ความก้าวหน้าของเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้น ส่งผลให้ความต้องการในการดูแลความมั่นคงปลอดภัยของระบบสารสนเทศเพิ่มสูงขึ้นด้วย องค์กรต่าง ๆ ทั้งภาครัฐและภาคเอกชนต่างก็ให้ความสำคัญอย่างมากต่อการพัฒนาระบบเพื่อการดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ มีการพัฒนามาตรฐานเกี่ยวกับการดูแลรักษาความมั่นคงปลอดภัยระบบสารสนเทศออกมาอย่างต่อเนื่อง เพื่อป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในรูปแบบต่าง ๆ ที่มีต่อระบบสารสนเทศขององค์กร ซึ่งนับวันจะทวีความรุนแรง และท้าทายต่อผู้ที่รับผิดชอบในการดูแลระบบ เป็นอย่างมาก

ทุกองค์กรที่มีการนำระบบคอมพิวเตอร์มาใช้ในการปฏิบัติงานจำเป็นอย่างยิ่งที่จะต้องกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ซึ่งจะต้องกำหนดให้ใครมีสิทธิและใครไม่มีสิทธิเข้าถึงระบบสารสนเทศ ทั้งทางด้านกายภาพและทางอิเล็กทรอนิกส์ และควรที่จะมีระเบียบแบบแผนการปฏิบัติที่ชัดเจนในการใช้ระบบสารสนเทศขององค์กร องค์กรต้องมีแผนปฏิบัติเมื่อเกิดเหตุฉุกเฉิน หรือเมื่อเกิดเหตุการณ์เกี่ยวกับความมั่นคงและความปลอดภัย นอกจากนี้องค์กรและผู้ใช้เองก็ต้องนำนโยบายด้านการรักษาความมั่นคงปลอดภัยมาใช้อย่างเคร่งครัดด้วย

๑. หลักการและเหตุผล

เนื่องจากคู่มือการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (พ.ศ. ๒๕๔๙ – ๒๕๕๑) ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้กำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทาง (roadmap) เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของประเทศ ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC 27001 และ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทาง

อิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ “คู่มือการจัดทำระบบรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกรมทรัพยากรน้ำบาดาล” ฉบับนี้จัดทำขึ้นเพื่อใช้เป็นแนวทางในการกำหนดนโยบาย แนวปฏิบัติ และวิธีปฏิบัติ เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ซึ่งเป็นเครื่องมือที่สำคัญในการปฏิบัติงานและการบริหารราชการขององค์กร

๒. วัตถุประสงค์

คู่มือฉบับนี้ จัดทำขึ้นเพื่อวัตถุประสงค์ดังนี้

๒.๑ เพื่อใช้เป็นแนวทางในการจัดทำระบบบริหารความมั่นคงปลอดภัยของสารสนเทศให้เป็นไปตามมาตรฐานสากล ส่งผลให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและมีประสิทธิภาพ

๒.๒ เพื่อให้ฝ่ายบริหาร และฝ่ายปฏิบัติการ เข้าใจหลักการและกระบวนการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๒.๓ เพื่อให้มีการปฏิบัติตามกระบวนการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นระบบและต่อเนื่อง

๒.๔ เพื่อเป็นเครื่องมือสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศกับกลยุทธ์ของกรมทรัพยากรน้ำบาดาล

๒.๕ เพื่อใช้เป็นเครื่องมือในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ในหน่วยงานทุกระดับของกรมทรัพยากรน้ำบาดาล ให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และให้เจ้าหน้าที่ทุกระดับในกรมทรัพยากรน้ำบาดาล และบุคคลที่เกี่ยวข้อง ถือปฏิบัติอย่างเคร่งครัด

๓. นิยามและคำจำกัดความที่สำคัญ

“กรมฯ” หมายถึง กรมทรัพยากรน้ำบาดาล

“ผู้บริหาร” หมายถึง อธิบดีหรือรองอธิบดี ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรมฯ

“ผู้บริหารสารสนเทศระดับสูง (Chief Information Officer: CIO)” หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของกรมฯ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน รวมถึงการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมฯ

“ศูนย์สารสนเทศ” หมายถึง ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล ซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสื่อสารภายในกรมฯ

“ผู้อำนวยการศูนย์สารสนเทศ” หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมฯ และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในกรมฯ

“หน่วยงาน” หมายถึง สำนัก กอง ศูนย์ หรือที่เรียกชื่อเป็นอย่างอื่นในสังกัดกรมฯ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายถึง กลุ่มของคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่ถูกนำมาเชื่อมต่อกันผ่านอุปกรณ์ด้านการสื่อสารหรือสื่ออื่นใด ทำให้ผู้ใช้ในระบบเครือข่ายสามารถติดต่อสื่อสารแลกเปลี่ยนและใช้อุปกรณ์ต่าง ๆ ของเครือข่ายร่วมกันได้

“ระบบสารสนเทศ” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศ ที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสารทั้งมีสายและไร้สาย ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ

“ผู้มีอำนาจ” หมายถึง หัวหน้าหน่วยงานที่มีระบบคอมพิวเตอร์ของกรมฯ อยู่ในความครอบครอง และให้หมายความรวมถึงผู้ซึ่งได้รับมอบหมายจากบุคคลดังกล่าวด้วย

“ผู้ใช้งาน” หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง เจ้าหน้าที่ ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ หรือผู้ที่หน่วยงาน อนุญาตให้ใช้ระบบคอมพิวเตอร์ได้

“ผู้ดูแลระบบ (system administrator)” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“บัญชีผู้ใช้งาน” หมายถึง บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมฯ

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับระบบสารสนเทศของกรมฯ

“ความมั่นคงปลอดภัยด้านสารสนเทศ (information security)” หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้ง การห้ามปฏิเสธความรับผิด (non-repudiation)

“ความเสี่ยง (risk)” หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเสีย ความสูญเปล่า หรือเหตุการณ์ซึ่งไม่พึงประสงค์ที่ทำให้งานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนด

“ปัจจัยเสี่ยง (risk factor)” หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

“การระบุความเสี่ยง (risk identification)” หมายถึง การค้นหา ระบุเหตุการณ์ใด ๆ ทั้งที่มีผลดีและผลเสียต่อการบรรลุวัตถุประสงค์ ทั้งในระดับองค์กรและกิจกรรมซึ่งค้นหาได้จากงาน โครงการ กิจกรรม จากข้อมูล สถิติที่เคยเกิดขึ้น หรือคาดว่าจะเกิดขึ้นโดยระบุด้วยว่าเหตุการณ์นั้น ๆ จะเกิดที่ไหน เมื่อใด อย่างไร และทำไม

“การวิเคราะห์ความเสี่ยง (risk analysis)” หมายถึง ขั้นตอนการวิเคราะห์ความเสี่ยงหรือผลกระทบของความเสี่ยงต่อองค์กร เทคนิคการวิเคราะห์ความเสี่ยงมีหลายวิธีเพราะการวัดความเสี่ยงเป็นตัวเลขว่ามีผลต่อองค์กรเท่าไรนั้นเป็นสิ่งที่ทำได้ยาก โดยทั่วไปจะวิเคราะห์ ความเสี่ยงโดยประเมินนัยสำคัญหรือผลกระทบของความเสี่ยง และความถี่ที่จะเกิดหรือ โอกาสที่จะเกิดความเสี่ยง

“การประเมินความเสี่ยง (risk assessment)” หมายถึง กระบวนการที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง

“การบริหารความเสี่ยง (risk management)” หมายถึง กระบวนการจัดการความเสี่ยง ประกอบด้วยกระบวนการในการระบุ วิเคราะห์ (risk analysis) ประเมิน (risk assessment) ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับ ภารกิจ หน้าที่และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด

“โปรแกรมประสงค์ร้าย (malware)” หมายถึง โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (computer virus) หรือสปายแวร์ (spyware) หรือหนอน (worm) หรือม้าโทรจัน (trojan horse) หรือฟิชชิง (phishing) หรือจดหมายลูกโซ่ (mass mailing) เป็นต้น

บทที่ ๒

ความมั่นคงปลอดภัยของระบบสารสนเทศ

ปัจจุบันปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศ และต่างประเทศ และมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐ และภาคธุรกิจมากขึ้น ทำให้ผู้ประกอบการ ตลอดจนองค์กร ภาครัฐ และภาคเอกชน ที่มีการดำเนินงานโดยการนำระบบสารสนเทศและการสื่อสาร มาประยุกต์ใช้ ต้องตระหนักถึงความมั่นคงปลอดภัยของระบบสารสนเทศ ซึ่งช่วยปกป้องเครื่องคอมพิวเตอร์ รวมไปถึงอุปกรณ์ต่าง ๆ ที่เกี่ยวข้อง และที่สำคัญยังสามารถช่วยปกป้องข้อมูลที่ได้จัดเก็บไว้ภายในระบบอีกด้วย

๑. จุดประสงค์ของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ

จุดประสงค์หลักของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศคือ ความลับ (confidentiality) ความสมบูรณ์ (integrity) ความพร้อมใช้ (availability) และการห้ามปฏิเสธความรับผิดชอบ (non-repudiation) ของข้อมูลต่าง ๆ ภายในองค์กร โดยมีรายละเอียดดังนี้

๑.๑. การรักษาความลับ (confidentiality) คือการรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ ทำให้มั่นใจว่ามีเฉพาะผู้มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้

๑.๒. การรักษาความสมบูรณ์ (integrity) คือการรับรองว่าข้อมูลที่ปกป้องนั้น ต้องมีความถูกต้องสมบูรณ์ จะไม่ถูกแก้ไข เปลี่ยนแปลง หรือทำลาย จากผู้ไม่มีสิทธิไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา

๑.๓. ความพร้อมใช้ (availability) คือการรับรองว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมใช้งานสามารถตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ

๑.๔. การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) คือวิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

๒. องค์ประกอบของระบบสารสนเทศ

ระบบสารสนเทศซึ่งเป็นระบบสนับสนุนการบริหารงาน การจัดการ และการปฏิบัติงานของบุคลากร ไม่ว่าจะเป็นระดับบุคคล ระดับกลุ่ม หรือ ระดับองค์กร ไม่ใช่มีเพียงเครื่องคอมพิวเตอร์เท่านั้น แต่ยังมีองค์ประกอบอื่น ๆ ที่เกี่ยวข้องกับความสำเร็จของระบบอีก รวม ๕ องค์ประกอบ ซึ่งจะขาดองค์ประกอบใดไม่ได้คือ

๒.๑ ฮาร์ดแวร์ เป็นองค์ประกอบสำคัญของระบบสารสนเทศ หมายถึง เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง รวมทั้งอุปกรณ์สื่อสารสำหรับเชื่อมโยงคอมพิวเตอร์เข้าเป็นเครือข่าย เช่น เครื่องพิมพ์ อุปกรณ์กระจายสัญญาณ

๒.๒ ซอฟต์แวร์ หรือโปรแกรมคอมพิวเตอร์เป็นองค์ประกอบที่สำคัญประการที่สอง ซึ่งก็คือลำดับขั้นตอนของคำสั่งที่จะสั่งงานให้ฮาร์ดแวร์ทำงาน เพื่อประมวลผลข้อมูลให้ได้ผลลัพธ์ตามความต้องการของการใช้งาน ในปัจจุบันมีซอฟต์แวร์ระบบปฏิบัติงาน ซอฟต์แวร์ควบคุมระบบงาน ซอฟต์แวร์สำเร็จ และซอฟต์แวร์ประยุกต์สำหรับงานต่าง ๆ ลักษณะการใช้งานของซอฟต์แวร์ก่อนหน้านี้ ผู้ใช้จะต้องติดต่อใช้งานโดยใช้ข้อความเป็นหลัก แต่ในปัจจุบันซอฟต์แวร์มีลักษณะการใช้งานที่ง่ายขึ้น โดยมีรูปแบบการติดต่อที่สื่อความหมายให้เข้าใจง่าย เช่น มีส่วนต่อประสานกราฟฟิกส์กับผู้ใช้ที่เรียกว่า จียูไอ (Graphical User Interface: GUI) ส่วนซอฟต์แวร์สำเร็จที่มีใช้ในท้องตลาดทำให้การใช้งานคอมพิวเตอร์ในระดับบุคคลเป็นไปอย่างกว้างขวาง และเริ่มมีลักษณะส่งเสริมการทำงานของกลุ่มมากขึ้น ส่วนงานในระดับองค์กรส่วนใหญ่มักจะมีการพัฒนาระบบตามความต้องการโดยการว่าจ้าง หรือโดยนักคอมพิวเตอร์ขององค์กร เป็นต้น ซอฟต์แวร์สามารถแบ่งได้ดังนี้

๒.๑.๑ ซอฟต์แวร์ระบบ หมายถึง โปรแกรมทุกโปรแกรมที่ทำหน้าที่ติดต่อกับส่วนประกอบต่าง ๆ ของฮาร์ดแวร์คอมพิวเตอร์ และอำนวยเครื่องมือสำหรับทำงานพื้นฐานต่าง ๆ ที่เกี่ยวข้องกับฮาร์ดแวร์

๒.๑.๒ ซอฟต์แวร์ประยุกต์ จะเป็นโปรแกรมที่ทำให้คอมพิวเตอร์สามารถทำงานต่าง ๆ ตามที่ผู้ใช้ต้องการ ไม่ว่างานด้านการจัดทำเอกสาร การทำบัญชี การจัดเก็บข้อมูลข่าวสาร ตลอดจนงานทุก ๆ ด้านตามแต่ผู้ใช้ต้องการ จนสามารถกล่าวได้ว่าซอฟต์แวร์ประยุกต์ก็คือซอฟต์แวร์ที่ทำให้เกิดการใช้งานคอมพิวเตอร์กันอย่างกว้างขวาง และทำให้คอมพิวเตอร์เป็นปัจจัยที่ไม่สามารถขาดได้ในยุคสารสนเทศนี้

ในองค์กรขนาดใหญ่หรืองานที่มีความต้องการเฉพาะด้าน การจัดหาซอฟต์แวร์มาใช้งานจะใช้วิธีพัฒนาซอฟต์แวร์ขึ้นมาเอง หรือว่าจ้างบริษัทซอฟต์แวร์เพื่อทำซอฟต์แวร์เฉพาะงานขึ้นมาใช้เอง ซอฟต์แวร์ประเภทนี้จะเรียกว่าซอฟต์แวร์เฉพาะงาน (tailor made software) มีข้อดีคือมีความเหมาะสมกับงานและสามารถแก้ไขตามความต้องการได้ ข้อเสียคือค่าใช้จ่ายสูงและใช้เวลาสำหรับการ

พัฒนา ปัจจุบันนี้จึงมีโปรแกรมคอมพิวเตอร์ที่เขียนขึ้นมาเพื่อใช้สำหรับงานทั่ว ๆ ไป วางจำหน่ายเป็นชุดสำเร็จรูปเรียกว่าซอฟต์แวร์สำเร็จรูป (software package)

๒.๓ ข้อมูล เป็นองค์ประกอบที่สำคัญอีกประการหนึ่งของระบบสารสนเทศ อาจจะเป็นตัวชี้ความสำเร็จหรือความล้มเหลวของระบบได้ เนื่องจากจะต้องมีการเก็บข้อมูลจากแหล่งกำเนิด ข้อมูลจะต้องมีความถูกต้อง มีการกลั่นกรองและตรวจสอบแล้วเท่านั้นจึงจะมีประโยชน์ ข้อมูลจำเป็นจะต้องมีมาตรฐาน โดยเฉพาะอย่างยิ่งเมื่อใช้งานในระดับกลุ่มหรือระดับองค์กร ข้อมูลต้องมีโครงสร้างในการจัดเก็บที่เป็นระบบระเบียบเพื่อการสืบค้นที่รวดเร็วมีประสิทธิภาพ

๒.๔ บุคลากร ในระดับผู้บริหาร ผู้ดูแลระบบ ผู้พัฒนาระบบ นักวิเคราะห์ระบบ นักเขียนโปรแกรม และผู้ใช้บริการ เป็นองค์ประกอบสำคัญในความสำเร็จของระบบสารสนเทศ บุคลากรมีความรู้ความสามารถทางคอมพิวเตอร์มากเท่าใด โอกาสที่จะใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ได้เต็มศักยภาพและคุ้มค่ายิ่งมากขึ้นเท่านั้น โดยเฉพาะระบบสารสนเทศในระดับบุคคลซึ่งเครื่องคอมพิวเตอร์มีขีดความสามารถมากขึ้น ทำให้ผู้ใช้มีโอกาสพัฒนาความสามารถของตนเองและพัฒนาระบบงานได้เองตามความต้องการ สำหรับระบบสารสนเทศในระดับกลุ่มและองค์กรที่มีความซับซ้อนมาก อาจจะต้องใช้บุคลากรในสาขาคอมพิวเตอร์ โดยตรงมาพัฒนาและดูแลระบบงาน

๒.๕ ขั้นตอนการปฏิบัติงาน ขั้นตอนการปฏิบัติงานที่ชัดเจนของผู้ใช้หรือของบุคลากรที่เกี่ยงข้องก็เป็นเรื่องสำคัญอีกประการหนึ่ง เมื่อได้พัฒนาระบบงานแล้วจำเป็นต้องปฏิบัติงานตามลำดับขั้นตอนในขณะที่ใช้งานก็จำเป็นต้องคำนึงถึงลำดับขั้นตอน การปฏิบัติของคนและความสัมพันธ์กับเครื่อง ทั้งในกรณีปกติและกรณีฉุกเฉิน เช่น ขั้นตอนการบันทึกข้อมูล ขั้นตอนการประมวลผล ขั้นตอนการปฏิบัติเมื่อเครื่องมือชำรุดหรือข้อมูลสูญหาย และขั้นตอนการทำสำเนาข้อมูลสำรองเพื่อความปลอดภัย เป็นต้น สิ่งเล่านี้ต้องมีการซักซ้อม มีการเตรียมการ และการทำเอกสารคู่มือการใช้งานให้ชัดเจน

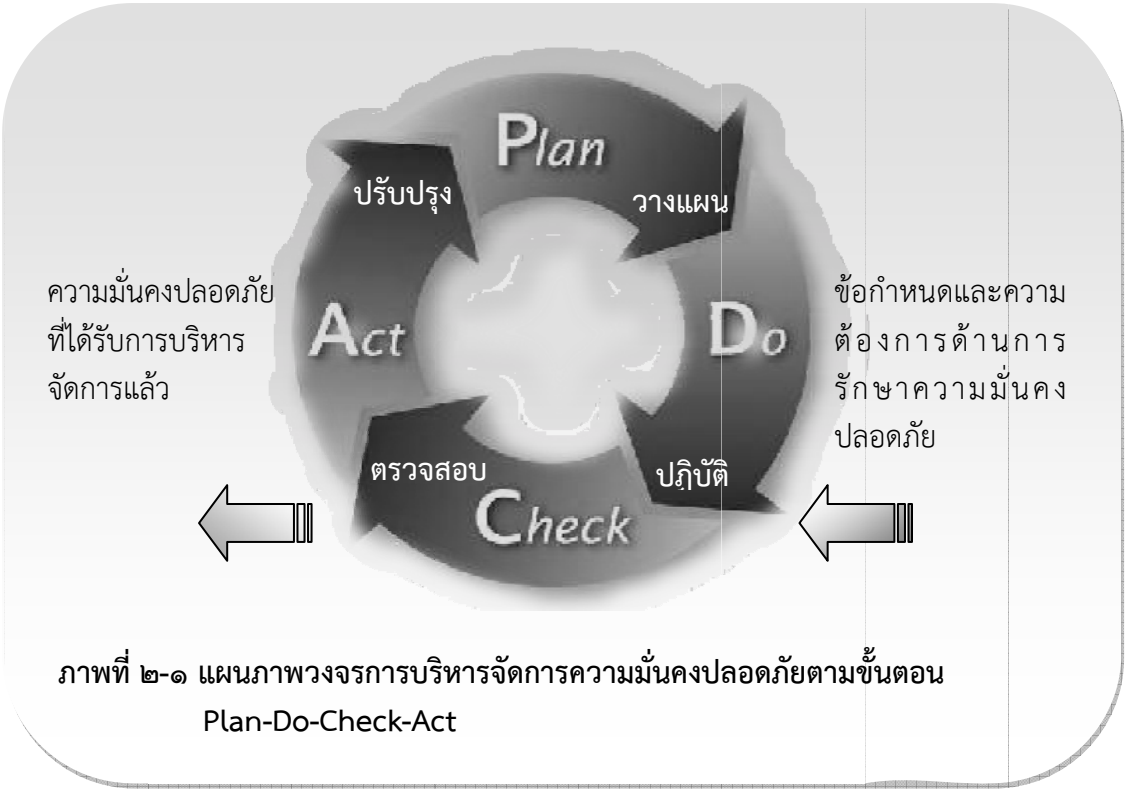
๓. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

การนำมาตรฐานการรักษาความมั่นคงปลอดภัยมาประยุกต์ใช้กับระบบสารสนเทศในองค์กรเริ่มเป็นที่แพร่หลายมากขึ้น มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานหนึ่งที่กำลังได้รับความนิยมอย่างแพร่หลายในปัจจุบัน ได้รับการยอมรับจากหลายประเทศในการนำไปใช้บริหารจัดการระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานที่พัฒนามาจากมาตรฐานในตระกูล ISO/IEC 27000 ซึ่งเกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security Management System: ISMS) ได้ผ่านการ

ปรับปรุงและนำออกเผยแพร่เมื่อเดือนตุลาคม ๒๕๔๘ โดย International Organization for Standardization (ISO) และ International Electrotechnical Commission (IEC)

จุดประสงค์ของมาตรฐานนี้เพื่อจะทำให้องค์กรสามารถบริหารจัดการทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างมีระบบ และเพียงพอเหมาะสมต่อการดำเนินภารกิจขององค์กร โดยเริ่มแรกองค์กรต้องทำการวิเคราะห์ความเสี่ยงของระบบ จากภัยคุกคาม และจุดอ่อนต่างๆ โดยการประเมินความเสี่ยง และการจัดการกับความเสี่ยง เช่น ลด โอนย้าย หรือยอมรับ ความเสี่ยง (Risk Assessment and Treatment) เพื่อรักษาระบบสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม และพอเพียง ขณะเดียวกันมาตรฐานนี้ยังกำหนดให้องค์กรต้องควบคุมดูแลระบบการรักษาความมั่นคงปลอดภัย และกลไกในการพัฒนาอย่างต่อเนื่องอีกด้วย

นอกจากนี้ มาตรฐาน ISO/IEC 27001 ยังประกอบด้วยไปด้วยวงจรบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act (Plan: การวางแผน - Do: การปฏิบัติ – Check: การตรวจสอบ – Act: การปรับปรุง) ดังแสดงในภาพที่ ๒-๑



ภาพที่ ๒-๑ แผนภาพวงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act

ซึ่งจะทำให้การบริหารจัดการเรื่องความมั่นคงปลอดภัยของระบบสารสนเทศ มีประสิทธิผลเต็มที่ ทำให้องค์กรรอดพ้นจากภัยคุกคามต่าง ๆ และทำให้องค์กรมั่นใจที่จะใช้ระบบ

สารสนเทศมาเป็นเครื่องมือในการปฏิบัติงานตามภารกิจขององค์กร ซึ่งสาระสำคัญของมาตรฐานดังกล่าว แบ่งเป็น ๒ ส่วนหลักคือ

๓.๑ กระบวนการการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (อ้างอิงข้อกำหนดตามมาตรฐาน ISO/IEC 27001)

๓.๑.๑ รายละเอียดของระบบบริหารจัดการความปลอดภัยสำหรับสารสนเทศ

๑) ข้อกำหนดทั่วไป

องค์กรจะต้องกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุง รักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ได้กำหนดไว้เป็นลายลักษณ์อักษร ภายในกรอบกิจกรรมการดำเนินการตามภารกิจต่าง ๆ รวมทั้งความเสี่ยงที่เกี่ยวข้อง แนวทางที่ใช้ในมาตรฐานนี้จะนำกระบวนการดำเนินงานที่มีคุณภาพตามวงจร Plan-Do-Check-Act มาประยุกต์ใช้ จากภาพที่ ๒-๑ แสดงให้เห็นถึงแบบจำลองขั้นตอนการทำงานของระบบ ISMS ที่ตรงตามความต้องการของกลุ่มองค์กร รวมถึงระบบการปฏิบัติงานต่าง ๆ ที่เกิดขึ้นทำให้ระบบการรักษาความมั่นคงปลอดภัยข้อมูลตรงตามความต้องการและความคาดหมายได้ ซึ่งแต่ละขั้นตอนประกอบด้วยรายละเอียดโดยย่อดังนี้ ๑) Plan คือการวางแผน การกำหนดนโยบายความมั่นคงและจัดทำระบบ ISMS ๒) Do คือการลงมือปฏิบัติหรือดำเนินการตามระบบ ISMS ๓) Check คือการตรวจสอบและทบทวนผลการดำเนินการตามระบบ ISMS ๔) Act คือ การแก้ไข บำรุงรักษา และปรับปรุงคุณภาพของระบบ ISMS เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบและมีการพัฒนาขึ้นอย่างต่อเนื่อง (continuous improvement)

๑.๑) กำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan) โดยองค์กรควรกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยและกำหนดนโยบายความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะขององค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี นอกจากนี้ยังต้องกำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร ระบบความเสี่ยง วิเคราะห์และประเมินความเสี่ยง ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงการดำเนินการที่เป็นไปได้ เลือกวัตถุประสงค์และมาตรการทางด้านความปลอดภัยเพื่อจัดการกับความเสี่ยง

๑.๒) ลงมือปฏิบัติและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัย (Do) โดยองค์กรควรจัดทำแผนการจัดการความเสี่ยง ลงมือปฏิบัติตามแผนการจัดการความเสี่ยงและตามมาตรฐานที่เลือกไว้ กำหนดวิธีการในการวัดความสัมฤทธิ์ผลของมาตรการที่เลือกมาใช้งาน จัดทำและลงมือปฏิบัติตามแผนการอบรมและสร้างความตระหนัก บริหารจัดการดำเนินงานและบริหารทรัพยากรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย รวมถึงจัดทำและลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่น ๆ ซึ่งช่วยในการตรวจจับและรับมือกับเหตุการณ์ทางด้านความมั่นคงปลอดภัย

๑.๓) เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย (Check) โดยองค์กรควรลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่น ๆ สำหรับการเฝ้าระวังและทบทวน ดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ วัดความสัมฤทธิ์ผลของมาตรการทางด้านความมั่นคงปลอดภัย ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้กับระดับความเสี่ยงที่เหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ ดำเนินการตรวจสอบและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย ปรับปรุงแผนทางด้านความปลอดภัยโดยนำผลของการเฝ้าระวังและทบทวนกิจกรรมต่าง ๆ มาพิจารณาร่วมด้วย และบันทึกการดำเนินการซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

๑.๔) บำรุงรักษาและปรับปรุงระบบบริหารจัดการด้านความมั่นคงปลอดภัย (Act) โดยองค์กรควรปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้ รวมถึงการใช้มาตรการเชิงแก้ไข ป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและองค์กรอื่น แจ้งการปรับปรุงและดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้อง และตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

๒) ข้อกำหนดทางด้านการจัดทำเอกสาร

๒.๑) ความต้องการทั่วไป เอกสารที่จำเป็นต้องจัดทำจะรวมถึงบันทึกแสดงการตัดสินใจของผู้บริหาร ได้แก่ นโยบายความมั่นคงปลอดภัย ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย วิธีการประเมินความเสี่ยง เป็นต้น

๒.๒) การบริหารจัดการเอกสาร ซึ่งเอกสารตามข้อกำหนดของระบบบริหารจัดการความมั่นคงปลอดภัยจะต้องได้รับการป้องกันและควบคุม ขั้นตอนการปฏิบัติที่เกี่ยวข้องกับการจัดการเอกสาร ได้แก่ อนุมัติการใช้งานเอกสารก่อนที่จะเผยแพร่ ทบทวน ปรับปรุงและอนุมัติเอกสารตามความจำเป็น ระบุการเปลี่ยนแปลงและสถานภาพของเอกสารปัจจุบัน เป็นต้น

๒.๓) การบริหารจัดการบันทึกข้อมูลหรือฟอร์มต่าง ๆ องค์กรจะต้องมีการกำหนด จัดทำและบำรุงรักษาบันทึกข้อมูลหรือฟอร์มต่าง ๆ เพื่อใช้เป็นหลักฐานแสดงความสอดคล้องกับข้อกำหนดและการดำเนินการที่มีประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

๓.๑.๒ หน้าที่ความรับผิดชอบของผู้บริหาร

๑) การให้ความสำคัญในการบริหารจัดการ โดยผู้บริหารจะต้องแสดงถึงการให้ความสำคัญต่อการกำหนดการลงมือปฏิบัติการ ดำเนินการ เฝ้าระวัง การทบทวน การบำรุงรักษาและการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย

๒) การบริหารจัดการทรัพยากรที่จำเป็นและการอบรม การสร้างความตระหนักและการเพิ่มขีดความสามารถเพื่อให้บุคลากรทั้งหมดที่ได้รับมอบหมายหน้าที่สามารถปฏิบัติงานได้ตามที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย

๓.๑.๓ องค์กรควรดำเนินการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัย ตามรอบระยะเวลาที่กำหนดไว้เพื่อตรวจสอบว่า วัตถุประสงค์ มาตรการ กระบวนการ และขั้นตอนปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัยมีความสอดคล้องกับข้อกำหนดในมาตรฐานฉบับนี้และกฎหมาย ระเบียบ ข้อบังคับต่าง ๆ รวมถึงสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย และได้รับการลงมือปฏิบัติและบำรุงรักษาอย่างสัมฤทธิ์ผลและเป็นไปตามที่คาดหมายไว้ นอกจากนี้ องค์กรจะต้องวางแผนตรวจสอบภายในโดยพิจารณาถึงสถานภาพและความสำคัญของกระบวนการและส่วนต่าง ๆ ที่จะได้รับการตรวจสอบและผลการตรวจสอบในครั้งที่ผ่านมา รวมถึงองค์กรจะต้องระบุหน้าที่ความรับผิดชอบและข้อกำหนดต่าง ๆ ในการวางแผนและดำเนินการตรวจสอบ จัดทำรายงานผลการตรวจสอบและบันทึกข้อมูลของการตรวจสอบนั้น

๓.๑.๔ ผู้บริหารจะต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนดไว้ (เช่นปีละ ๑ ครั้ง) เพื่อให้มีการดำเนินการที่เหมาะสม พอเพียงและสัมฤทธิ์ผล การทบทวนจะต้องรวมถึงการปรับปรุงหรือเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งหมายรวมถึงนโยบายความมั่นคงปลอดภัยและวัตถุประสงค์ทางด้านความปลอดภัย ผลของการทบทวนจะต้องได้รับการบันทึกไว้อย่างเป็นลายลักษณ์อักษรและบันทึกข้อมูลที่เกี่ยวข้องกับการทบทวนจะต้องได้รับการบำรุงรักษาไว้

๓.๒ มาตรการการจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

๓.๒.๑ นโยบายความมั่นคงปลอดภัย (security policy) ประกอบด้วยนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ ซึ่งมีวัตถุประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง โดยผู้บริหารองค์กรจะต้องมีการจัดทำนโยบายที่เป็นลายลักษณ์อักษร รวมถึงการทบทวนนโยบายตามระยะเวลาที่กำหนดหรือมีเปลี่ยนแปลงที่สำคัญขององค์กร

๓.๒.๒ โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (internal organization) โดยได้กล่าวถึงบทบาทของผู้บริหารองค์กรและหัวหน้างานสารสนเทศ ในด้านต่าง ๆ ดังต่อไปนี้

๑) โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

๒) โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับหน่วยงานภายนอก เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับหน่วยงานภายนอก

๓.๒.๓ การบริหารจัดการทรัพย์สินขององค์กร (asset management) โดยได้กล่าวถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานพัสดุในด้านต่าง ๆ ดังต่อไปนี้

๑) หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจขึ้นได้

๒) การจัดหมวดหมู่สารสนเทศ เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

๓.๒.๔ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (human resources security) โดยได้กล่าวถึงบทบาทของผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ หัวหน้างานบุคคล และหัวหน้างานที่เกี่ยวข้องในต่าง ๆ ดังต่อไปนี้

๑) การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

๒) การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบและทำความเข้าใจกับนโยบาย เพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

๓) การสิ้นสุดและการเปลี่ยนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

๓.๒.๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (physical and environmental security) โดยได้กล่าวถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานอาคารในด้านต่าง ๆ ดังต่อไปนี้

๑) บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

๒) ความมั่นคงปลอดภัยของอุปกรณ์ เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และทำให้กิจกรรมการดำเนินงานต่าง ๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

๓.๒.๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (communications and operations management) โดยได้กล่าวถึงบทบาทของผู้บริหารองค์กร ผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ ผู้ที่เป็นเจ้าของกระบวนการทำงานและเจ้าหน้าที่สารสนเทศในด้านต่าง ๆ ดังต่อไปนี้

๑) การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

๒) การบริหารจัดการการให้บริการของหน่วยงานภายนอก เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

๓) การวางแผนและการตรวจรับทรัพยากรสารสนเทศ เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

๔) การป้องกันโปรแกรมที่ไม่ประสงค์ดี เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

๕) การสำรองข้อมูล เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

๖) การบริหารจัดการทางด้านความปลอดภัยสำหรับเครือข่ายขององค์กร เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

๗) การจัดการสื่อที่ใช้ในการบันทึกข้อมูล เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ

๘) การแลกเปลี่ยนสารสนเทศ เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

๙) การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และการใช้งาน

๑๐) การเฝ้าระวังทางด้านความมั่นคงปลอดภัย เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

๓.๒.๗ การควบคุมการเข้าถึง (access control) โดยได้กล่าวถึงบทบาทของผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ ผู้ดูแลระบบและเจ้าหน้าที่ในด้านต่าง ๆ ดังต่อไปนี้

๑) ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ เพื่อควบคุมการเข้าถึงสารสนเทศ

๒) การบริหารจัดการการเข้าถึงของผู้ใช้ เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๓) การควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต

๔) การควบคุมการเข้าถึงระบบปฏิบัติการที่ไม่ได้รับอนุญาต

๕) การควบคุมการเข้าถึง application และสารสนเทศที่ไม่ได้รับอนุญาต

๖) การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกเพื่อสร้างความมั่นคงปลอดภัยให้กับอุปกรณ์และการปฏิบัติงานที่เกี่ยวข้อง

๓.๒.๘ การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (information systems acquisition, development and maintenance) โดยได้กล่าวถึงบทบาทของหัวหน้างานสารสนเทศ ผู้พัฒนาระบบ และผู้เป็นเจ้าของระบบในด้านต่าง ๆ ดังต่อไปนี้

๑) ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ เพื่อให้การจัดหาและพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

๒) การประมวลผลสารสนเทศใน application เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์

๓) มาตรการการเข้ารหัสข้อมูล เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการทางการเข้ารหัสข้อมูล

๔) การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

๕) การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

๖) การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

๓.๒.๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (information security incident management) โดยได้กล่าวถึงบทบาทของหัวหน้างานสารสนเทศ หัวหน้างานนิติกร ผู้ดูแลระบบและเจ้าหน้าที่ในด้านต่าง ๆ ดังต่อไปนี้

๑) การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

๒) การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

๓.๒.๑๐ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (business continuity management) โดยได้กล่าวถึงบทบาทของผู้บริหารสารสนเทศ และหัวหน้างานสารสนเทศ ที่เกี่ยวกับหัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ เพื่อป้องกันกระบวนการทำงานที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๓.๒.๑๑ การปฏิบัติตามข้อกำหนด (compliance) โดยได้กล่าวถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานนิติกร ในด้านต่าง ๆ ดังต่อไปนี้

๑) การปฏิบัติตามข้อกำหนดทางกฎหมาย เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ

๒) การปฏิบัติตามนโยบาย มาตรฐานความปลอดภัยและข้อกำหนดทางเทคนิค เพื่อให้ระบบเป็นตามนโยบายและมาตรฐานความมั่นคงปลอดภัยตามที่องค์กรกำหนดไว้

๓) การตรวจประเมินระบบสารสนเทศ เพื่อตรวจประเมินระบบสารสนเทศให้ได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทำงานน้อยที่สุด

บทที่ ๓

การบริหารความเสี่ยงของระบบสารสนเทศ

คำว่าความเสี่ยง (risk) นั้นมีความหมายที่หลากหลาย มีการตีความแตกต่างกันไปหลายอย่างตามแต่ความคิด ความเชี่ยวชาญ และอาชีพของผู้ให้คำจำกัดความ เช่น ความเสี่ยงคือ การลองเผชิญดู ความเสี่ยงคือความไม่แน่นอนที่อาจนำไปสู่ความสำเร็จ หรือความสูญเสีย ความเสี่ยงคือโอกาสที่จะสูญเสียหรือบาดเจ็บ ความเสี่ยงคือความเป็นไปได้ที่จะได้รับความเสียหายจากภัยต่าง ๆ ความเสี่ยงคือ โอกาสที่สิ่งไม่ดีจะเกิดขึ้น ความเสี่ยงคือความไม่แน่นอนที่อาจนำไปสู่ความสูญเสีย ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ฯลฯ ความเสี่ยงมีทั้งประเภทที่เป็นความเสี่ยงที่แท้จริงที่เกิดขึ้นโดยธรรมชาติ และความเสี่ยงที่เกิดจากการกระทำของมนุษย์ โดยสรุปความเสี่ยง คือ เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบ หรือสร้างความเสียหาย หรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จตามเป้าหมายและวัตถุประสงค์ ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคล

ในขณะที่เทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกลอันทรงพลังในการขับเคลื่อน ทุกภาคส่วนให้ดำเนินไปอย่างไม่หยุดยั้ง ทุกกิจกรรมที่เกิดขึ้นล้วนแต่มีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวัน ข้อมูลจำนวนมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศ เพื่ออำนวยความสะดวกให้กับการดำเนินชีวิตประจำวัน และโดยเฉพาะอย่างยิ่งการดำเนินงานของทุกองค์กร แต่ระบบสารสนเทศซึ่งถือเป็นทรัพย์สินอันทรงคุณค่า ต่างตกอยู่ในภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กร โดยเจตนา หรือไม่เจตนา ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัยของระบบสารสนเทศ โดยเริ่มจากการบริหารความเสี่ยงของระบบสารสนเทศในองค์กร เป็นอันดับแรก

๑. ความเสี่ยงด้านระบบสารสนเทศ

จากการศึกษา และการตรวจสอบหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการบริหารจัดการและการควบคุมความเสี่ยงด้านระบบสารสนเทศ พอสรุปได้ว่าความเสี่ยงด้านระบบสารสนเทศสามารถแบ่งออกเป็น ๔ ประเภทหลัก ดังนี้

๑.๑ ความเสี่ยงด้านการเข้าถึงระบบสารสนเทศ (access risk) เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยง

ในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานที่รับผิดชอบไม่ได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปใช้ก่อให้เกิดความเสียหายได้ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การไม่ได้มีการกำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การไม่ได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

๑.๒ ความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของระบบสารสนเทศ (integrity risk) เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานที่รับผิดชอบไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไขหรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

๑.๓ ความเสี่ยงด้านการใช้ระบบสารสนเทศได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ (availability risk) เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูล หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหรือการให้บริการด้านต่าง ๆ อาจหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากการที่ไม่ได้มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการที่ไม่ได้ทำการสำรองข้อมูลและระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ ถ้าหากไม่ได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

๑.๔ ความเสี่ยงด้านโครงสร้างหน่วยงานและการบริหารจัดการ (infrastructure risk) เป็นความเสี่ยงเกี่ยวกับการที่หน่วยงานเทคโนโลยีสารสนเทศมิได้มีการจัดโครงสร้างและการบริหารจัดการที่ดีเพียงพอ ไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดีรวมทั้งไม่ได้จัดให้มีระบบคอมพิวเตอร์และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการปฏิบัติงาน โดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการที่ไม่ได้จัดให้มีนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่าง ๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการที่ไม่ได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินงานและการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

๒. **กระบวนการบริหารความเสี่ยง (risk management process)**

เนื่องจากความสี่ยงเป็นองค์ประกอบสำคัญที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ดังนั้นการบริหารความเสี่ยงจึงเป็นเรื่องที่มีความสำคัญ และจำเป็นอย่างยิ่งเพราะจะช่วยให้การดำเนินการตามภารกิจเป็นไปได้อย่างน่าเชื่อถือ สามารถหลีกเลี่ยงโอกาสที่จะเกิดความเสียหาย หรือ ความสูญเสียที่จะเกิดขึ้น ในกระบวนการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ความเสี่ยงเป็นภาวะคุกคามที่จะก่อปัญหา เกิดอุปสรรค หรือก่อผลเสียหายแก่องค์กร ทั้งในด้านยุทธศาสตร์ การดำเนินงาน การเงิน ทรัพยากรต่าง ๆ หรือ แม้แต่ชื่อเสียง และภาพลักษณ์

การบริหารความเสี่ยง คือ การบริหารปัจจัย และควบคุมกิจกรรม รวมทั้งกระบวนการการดำเนินงานต่าง ๆ โดยลดมูลเหตุและโอกาสที่องค์กรจะเกิดความเสียหาย เพื่อให้ระดับและขนาดของความเสียหายที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมและตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายขององค์กรเป็นสำคัญ ซึ่งขั้นตอนการดำเนินการ มีดังต่อไปนี้

๒.๑ การกำหนดวัตถุประสงค์ (objective setting) การกำหนดวัตถุประสงค์ เป็นขั้นตอนแรกที่มีความสำคัญโดยต้องมีการออกเป็นนโยบายว่าองค์กรจะทำการบริหารความเสี่ยงเพื่ออะไร ใครรับผิดชอบ มีข้อดีข้อเสียอย่างไรในการทำหรือวัตถุประสงค์ในการทำของเราว่าเราทำเพื่ออะไร หลัก ๆ ก็คือการมีการร่างนโยบาย (policy statement) ออกมาก่อน ซึ่งก็คือ ระดับผู้บริหารที่เป็นคนวางนโยบายว่าเราคิดจะบริหารความเสี่ยงของระบบสารสนเทศ และมีเรื่องสำคัญอะไรบ้างที่

ต้องกำหนดไว้ในนโยบาย เป็นขั้นตอนที่สำคัญก่อนการวางแผนการบริหารความเสี่ยงด้านสารสนเทศขององค์กร เพราะเป็นขั้นตอนในการสร้างความรู้สึกมีส่วนร่วม ที่ทำให้ทุกคนในองค์กร ตระหนักว่าเขาเป็นส่วนหนึ่งขององค์กร การที่เขาจะทำอะไรไม่ดีจะส่งผลกระทบต่อความเสี่ยงด้านระบบสารสนเทศขององค์กร ให้ทุกคนเห็นความสำคัญและประโยชน์ของการบริหารความเสี่ยง เพื่อให้ทุกคนให้ความร่วมมือ และพร้อมที่จะปฏิบัติตามมาตรการในการบริหารความเสี่ยงในขั้นตอนต่าง ๆ โดยการให้ความรู้ และให้เจ้าหน้าที่ทุกระดับมีส่วนร่วมในการออกความเห็นเกี่ยวกับประเด็นความเสี่ยงของระบบสารสนเทศที่องค์กรเผชิญ จากนั้น ควรมอบหมาย ผู้รับผิดชอบงานบริหารความเสี่ยงด้านระบบสารสนเทศขององค์กร โดยเป็นผู้ที่มีความรู้ความเข้าใจเกี่ยวกับระบบสารสนเทศขององค์กรเป็นอย่างดี และสามารถปฏิบัติงานร่วมกับผู้บริหารในส่วนงานอื่นขององค์กรได้ โดยจะมีหน้าที่ในการกำหนดขอบเขตและเป้าหมายงานบริหารความเสี่ยงร่วมกับทีมงานด้านอื่นขององค์กร โดยควรจะประกอบด้วยผู้เชี่ยวชาญในด้านต่าง ๆ ที่จำเป็นในการวิเคราะห์และบริหารความเสี่ยง วางกรอบแนวทางวิเคราะห์ความเสี่ยง สร้างทีมงานบริหารความเสี่ยงด้านระบบสารสนเทศขององค์กรในการกำหนดวัตถุประสงค์จะต้องคำนึงถึง ความชัดเจน สามารถวัดได้ สามารถปฏิบัติได้ ความสมเหตุสมผล และต้องมีกรอบเวลาที่แน่นอน

๒.๒ การระบุความเสี่ยง (risk identification) เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติร่วมกันค้นหาว่ามีความเสี่ยง และปัจจัยเสี่ยงใดบ้างที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร โดยปกติการระบุความเสี่ยงจะดูจากเหตุการณ์หรือสิ่งที่เคยเกิดขึ้นมาแล้วในอดีตกับองค์กร หรือองค์กรอื่นใด หรืออาจเป็นสิ่งที่มีความเป็นไปได้ว่าจะเกิดขึ้นแม้ไม่เคยเกิดขึ้นมาก่อนก็ได้ กระบวนการระบุความเสี่ยงอาจใช้วิธีการต่าง ๆ เช่น การระดมสมอง การออกแบบสอบถาม การประชุมเชิงปฏิบัติการด้านการประเมินความเสี่ยง หรือการวิเคราะห์สถานการณ์ เป็นต้น ในการวิเคราะห์เพื่อระบุความเสี่ยงต่าง ๆ ควรดูทั้งปัจจัยภายใน และปัจจัยภายนอกเป็นส่วนประกอบ ซึ่งอาจพิจารณาจากปัจจัยเสี่ยงในหลายด้าน เช่น

๒.๒.๑ ความเสี่ยงที่เกี่ยวข้องในระดับด้านกลยุทธ์ (strategic risk) คือความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนดำเนินงานและการนำไปปฏิบัติ ที่ไม่เหมาะสมหรือไม่สอดคล้องกับปัจจัยภายในและสภาพแวดล้อมภายนอก อันส่งผลกระทบต่อการทำงานขององค์กร ดังนั้น ผู้บริหารระดับสูงต้องวางแผนกลยุทธ์และแผนดำเนินงานด้านระบบสารสนเทศอย่าง รอบคอบ ส่งเสริมการบริหารตามหลักธรรมาภิบาล พร้อมทั้งจัดให้มีโครงสร้างพื้นฐานภายในที่เหมาะสมสำหรับการนำไปปฏิบัติ เช่น การจัดองค์กร บุคลากร งบประมาณ ระบบการติดตามและควบคุมการปฏิบัติงาน เป็นต้น

๒.๒.๒ ความเสี่ยงที่เกี่ยวข้องในระดับปฏิบัติการ (operational risk) คือ ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดีหรือขาดธรรมาภิบาลใน

องค์กร และการขาดการควบคุมที่ดี โดยอาจเกี่ยวข้องกับ กระบวนการปฏิบัติงานภายใน บุคคล ระบบงาน หรือเหตุการณ์ภายนอก และส่งผลกระทบต่อองค์กร เช่น กระบวนการ เทคโนโลยี และบุคลากรในองค์กร เป็นต้น

๒.๒.๓ ความเสี่ยงที่เกี่ยวข้องกับด้านการเงิน (financial risk) เป็นความเสี่ยงเกี่ยวกับการบริหารงบประมาณ และการเงิน เช่น ข้อมูลเอกสารหลักฐานทางการเงิน และการรายงานทางการเงินบัญชีผิดพลาด การบริหารการเงินไม่ถูกต้อง ไม่เหมาะสม ทำให้ขาดประสิทธิภาพ และไม่ทันต่อสถานการณ์ หรือเป็นความเสี่ยงที่เกี่ยวข้องกับการเงินขององค์กร เช่น การประมาณการงบประมาณไม่เพียงพอ และไม่สอดคล้องกับขั้นตอนการดำเนินการ เป็นต้น

๒.๒.๔ ความเสี่ยงด้านการปฏิบัติตามกฎหมายและกฎระเบียบ (compliance risk) เกี่ยวข้องกับการปฏิบัติตามกฎ ระเบียบต่าง ๆ โดยความเสี่ยงที่อาจเกิดขึ้นเป็นความเสี่ยงเนื่องจากความไม่ชัดเจน ความไม่ทันสมัย หรือความไม่ครอบคลุมของกฎหมาย กฎระเบียบ ข้อบังคับต่าง ๆ รวมทั้ง การทำนิติกรรมสัญญาการร่างสัญญาที่ไม่ครอบคลุมการดำเนินงาน

๒.๒.๕ ความเสี่ยงในด้านสิ่งแวดล้อมการทำงาน (hazard risk) เช่น อันตรายจากไฟฟ้า วัตถุที่แหลมคม ภัยธรรมชาติ และการก่อการร้าย เป็นต้น

๒.๓ การประเมินความเสี่ยง (risk assessment) หลังจากระบุความเสี่ยงได้แล้วขั้นต่อไปคือขั้นตอนการประเมินความเสี่ยง ซึ่งต้องทำให้ครบทุกปัจจัยเสี่ยงที่ได้ระบุไว้ ขั้นตอนนี้ มีอยู่ ๔ ส่วน ได้แก่การอธิบายความเสี่ยง การประเมินระดับความเสี่ยง การวิเคราะห์ความเสี่ยง และการจัดลำดับความเสี่ยง กล่าวคือ

๒.๓.๑ การอธิบายความเสี่ยง (risk description) หลังจากทราบว่าความเสี่ยงคืออะไรแล้ว ก็จะเป็นขั้นตอนการอธิบายว่าทุก ๆ ความเสี่ยงและปัจจัยเสี่ยงที่พบนั้นมีรายละเอียดและลักษณะอย่างไร ตัวอย่าง เช่น ชื่อความเสี่ยง ปัจจัยของความเสี่ยง ผู้รับผิดชอบ ผู้ที่ได้รับผลกระทบ การบำบัดและการควบคุม เป็นต้น

๒.๓.๒ การประเมินระดับความเสี่ยง (risk evaluation) เป็นการนำทุก ๆ ความเสี่ยงและปัจจัยเสี่ยงที่ระบุได้ มาประเมินโอกาส (likelihood) ที่จะเกิดเหตุการณ์ความเสี่ยงต่าง ๆ และประเมินระดับผลกระทบ ซึ่งเป็นความรุนแรงหรือมูลค่าความเสียหาย (impact) จากความเสี่ยง เพื่อให้เห็นถึงระดับของความเสี่ยงที่แตกต่างกัน ทำให้สามารถกำหนดการควบคุมความเสี่ยงได้อย่างเหมาะสม ซึ่งจะช่วยให้หน่วยงานสามารถวางแผนและจัดสรรทรัพยากรได้อย่างถูกต้อง ภายใต้งบประมาณ กำลังคน และเวลาที่มีจำกัด โดยอาศัยเกณฑ์มาตรฐานที่กำหนดไว้ ทั้งนี้อาจใช้ขั้นตอนดำเนินการ ดังนี้

๑) พิจารณาโอกาส หรือความถี่ในการเกิดเหตุการณ์ต่าง ๆ (likelihood) เป็นการประเมินระดับโอกาสที่จะเกิดความเสี่ยง โดยสามารถพิจารณาได้ในรูปแบบของ

ความถี่ (frequency) หรือโอกาสที่จะเกิดความเสี่ยง ตัวอย่างเกณฑ์การประเมินระดับโอกาสที่จะเกิดความเสี่ยงเชิงปริมาณ และเชิงคุณภาพ ดังแสดงในภาพที่ ๓-๑

ระดับ	โอกาสที่จะเกิด	คำอธิบาย	
		เชิงปริมาณ	เชิงคุณภาพ (โอกาส)
๑	น้อยมาก	๕ ปีต่อครั้ง	มีโอกาสเกิดในกรณียกเว้น
๒	น้อย	๓ ปีต่อครั้ง	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
๓	ปานกลาง	๑ ปีต่อครั้ง	มีโอกาสเกิดบางครั้ง
๔	สูง	๖ เดือนต่อครั้ง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
๕	สูงมาก	๑ เดือนต่อครั้ง	มีโอกาสในการเกิดเกือบทุกครั้ง

ภาพที่ ๓-๑ แสดงตัวอย่างเกณฑ์การประเมินระดับโอกาสที่จะเกิดความเสี่ยง

๒) พิจารณาความรุนแรงหรือความเสียหาย จากผลกระทบของความเสี่ยง (impact) เป็นการประเมินผลกระทบของความเสี่ยง ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงินที่อาจ

ระดับ	ผลกระทบ	คำอธิบาย	
		เชิงปริมาณ	เชิงคุณภาพ
๕	สูงมาก รุนแรงสูง	> ๑๐ ล้านบาท	มีการสูญเสียทรัพย์สินอย่างมหันต์ มีการบาดเจ็บถึงชีวิต
๔	สูง ค่อนข้างรุนแรง	> ๕ – ๑๐ ล้านบาท	มีการสูญเสียทรัพย์สินมาก มีการบาดเจ็บสาหัสถึงขั้นพักงาน
๓	ปานกลาง	> ๑ – ๕ ล้านบาท	มีการสูญเสียทรัพย์ปานกลาง มีการบาดเจ็บสาหัสถึงขั้นหยุดงาน
๒	น้อย	> ๐.๕ – ๑ ล้านบาท	การสูญเสียทรัพย์สินพอสมควร มีการบาดเจ็บรุนแรง
๑	น้อยมาก	ไม่เกิน ๐.๕ ล้านบาท	มีการสูญเสียทรัพย์สินเล็กน้อย ไม่มีการบาดเจ็บรุนแรง

ภาพที่ ๓-๒ แสดงตัวอย่างเกณฑ์การประเมินระดับความรุนแรงของผลกระทบ

เกิดขึ้น เช่น ผลกระทบด้านการเงินซึ่งเป็นผลกระทบหรือความเสียหายที่เกิดจากความเสี่ยง และสามารถประเมินค่าเป็นตัวเงินได้ ผลกระทบด้านชื่อเสียงขององค์กรไม่ว่าจะเป็นผลจากการดำเนินงานทั้งทางตรงและทางอ้อม ที่ส่งผลต่อภาพพจน์และความเชื่อถือขององค์กร เป็นต้น ดังตัวอย่างที่แสดงในภาพที่ ๓-๒

๒.๓.๓ การวิเคราะห์ความเสี่ยง เมื่อทุกหน่วยงานที่รับผิดชอบ พิจารณาโอกาส (ตามภาพที่ ๓-๑) และผลกระทบ (ตามภาพที่ ๓-๒) ของแต่ละปัจจัยเสี่ยงแล้ว ต้องนำผลที่ได้มาพิจารณาความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยง เพื่อใช้ในการจัดทำแผนผังประเมินความเสี่ยง (risk assessment matrix) เพื่อหาระดับความเสี่ยง (degree of risk) สำหรับค่าความเสี่ยง (level of risk) สามารถคำนวณได้ตามสูตรต่อไปนี้

ค่าความเสี่ยง = ระดับโอกาสที่จะเกิดความเสี่ยง x ระดับผลกระทบจากความเสี่ยง

ภาพที่ ๓-๓ แสดงแผนผังประเมินความเสี่ยง (risk assessment matrix) ซึ่งมีค่าความเสี่ยงระหว่าง ๑ - ๒๕ คะแนน

ภาพที่ ๓-๓ แสดงแผนผังประเมินความเสี่ยง

จำนวนของระดับความเสี่ยงไม่มีข้อกำหนดแน่นอน อาจจะแบ่งออกเป็น ๔ ระดับหรือ ๓ ระดับก็ได้ ขึ้นอยู่กับการจัดกลุ่มความเสี่ยงตามที่องค์กรเห็นสมควร

การจัดลำดับความเสี่ยง เมื่อได้ค่าความเสี่ยงแล้ว จะนำมาจัดลำดับความรุนแรงของความเสี่ยง ที่มีผลต่อองค์กร และหน่วยงาน เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่มีนัยสำคัญให้เหมาะสม โดยพิจารณาจากระดับของความเสี่ยงเรียง

ตามลำดับจากระดับ สูงมาก สูง ปานกลาง ต่ำ โดยเลือกความเสี่ยงที่มีระดับสูงมาก และหรือสูง มาจัดทำแผนการบริหารจัดการความเสี่ยงในขั้นตอนต่อไป

หลักเกณฑ์ในการยอมรับความเสี่ยง (risk acceptance criteria) ว่าจะยอมรับได้มากน้อยเพียงใด เพื่อประกอบการตัดสินใจว่าจะบำบัดความเสี่ยงนั้น ๆ ต่อไปอย่างไร พึงพิจารณาในแง่ต่าง ๆ ดังต่อไปนี้ เช่น

๑) ค่าใช้จ่าย ประโยชน์และความคุ้มทุนที่จะได้รับจากการแก้ไขบำบัดความเสี่ยง (costs and benefits)

๒) ข้อกำหนดด้านกฎหมายและกฎระเบียบขององค์กร (legal requirements)

๓) ปัจจัยด้านสิ่งแวดล้อม (environmental factors)

๔) ประเด็นสาระสำคัญในมุมมองของผู้มีส่วนได้เสีย (concerns of stakeholders)

ฯลฯ

๒.๓.๔ การกำหนดเกณฑ์ในการยอมรับความเสี่ยง จากแผนผังประเมินความเสี่ยง (ภาพที่ ๓-๓) ขั้นตอนต่อไปคือ นำรายการความเสี่ยงของแต่ละระดับความเสี่ยงที่ได้จัดเรียงลำดับไว้ (risk ranking) มาวิเคราะห์เปรียบเทียบกับเกณฑ์ในการยอมรับความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	ความหมาย
ต่ำ	๑ – ๓	ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยงไม่ต้องมีการจัดการเพิ่มเติม
ปานกลาง	๔ – ๙	ระดับที่พอยอมรับได้แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
สูง	๑๐ – ๑๖	ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
สูงมาก	๑๗ – ๒๕	ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการให้อยู่ในระดับที่ยอมรับได้ทันที

ภาพที่ ๓-๔ แสดงเกณฑ์ในการยอมรับความเสี่ยง

๒.๔ การจัดการความเสี่ยง (risk treatment) เป็นการหากลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยงว่าสามารถช่วยควบคุมความเสี่ยง หรือปัจจัยเสี่ยงได้เพียงพอหรือไม่ หรือเกิด

ประสิทธิผลตามวัตถุประสงค์ของการควบคุมมากน้อยเพียงใดเพื่อให้สามารถมั่นใจได้ว่าจะสามารถควบคุมความเสี่ยงที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กรได้อย่างมีประสิทธิภาพ ซึ่งวิธีการจัดการความเสี่ยงสามารถพิจารณาได้จาก ๔ ทางเลือกหลักคือ

๒.๔.๑ การยอมรับความเสี่ยง (risk acceptance) หมายถึง การรับความเสี่ยงไว้เองโดย ไม่กระทำใด ๆ เพิ่มเติม กรณีนี้ใช้กับความเสี่ยงที่มีน้อยความน่าจะเกิดน้อย หรือเห็นว่ามีต้นทุนในการบริหารความเสี่ยงสูง โดยขออนุมัติหลักการในการรับความเสี่ยงไว้เอง

๒.๔.๒ การลด (risk reduction) หรือควบคุมความเสี่ยง (risk control) หมายถึง การลดโอกาสความน่าจะเกิด หรือลดความเสียหาย โดยการจัดระบบการควบคุม เพื่อป้องกัน การปรับปรุงแก้ไขกระบวนการ รวมทั้ง การกำหนดแผนสำรองในเหตุฉุกเฉิน

๒.๔.๓ การหลีกเลี่ยงความเสี่ยง (risk avoidance) หมายถึง การหยุด หรือการเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น งดทำขั้นตอนที่ไม่จำเป็นและอาจจะนำมาซึ่งความเสี่ยง ปรับเปลี่ยนรูปแบบการทำงาน หรือลดขอบเขตการดำเนินการ เป็นต้น

๒.๔.๔ การกระจายความเสี่ยง (risk sharing) หรือการโอนความเสี่ยง (risk spreading) หมายถึงการลดโอกาสความน่าจะเกิด หรือลดความเสียหายโดยการแบ่งโอน การหาผู้รับผิดชอบในความเสี่ยง โดยการจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน หรือการจัดทำประกันภัย เป็นต้น

ทั้งนี้ควรคำนึงถึงต้นทุนและผลประโยชน์ที่จะได้รับภายใต้ทางเลือกต่าง ๆ และเมื่อได้ทางเลือกที่เหมาะสมในการบริหารความเสี่ยงแล้ว ทีมงานบริหารความเสี่ยงต้องกำหนดแผนกลยุทธ์การบริหารความเสี่ยงที่แต่ละหน่วยงานต้องร่วมกันปฏิบัติ ซึ่งการนำแผนกลยุทธ์ไปสู่การปฏิบัตินั้นจะต้องอาศัยความเข้าใจและความร่วมมือจากทุกฝ่ายที่เกี่ยวข้อง

๒.๕ กิจกรรมการบริหารความเสี่ยง (control activities) การนำกลยุทธ์ มาตรการ หรือ แผนงาน มาใช้ปฏิบัติงาน เพื่อลดโอกาสที่จะเกิดความเสี่ยง หรือลดความเสียหายจากผลกระทบในการดำเนินงานต่าง ๆ ที่ไม่มีกิจกรรมควบคุม หรือมีไม่เพียงพอ การควบคุม หมายถึง นโยบาย แนวทาง หรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยงให้บรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท ดังนี้

๒.๕.๑ การควบคุมเพื่อการป้องกัน (preventive control) การควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การแบ่งแยกหน้าที่ การควบคุมการเข้าถึงเอกสาร ข้อมูล ทรัพย์สิน ฯลฯ

๒.๕.๒ การควบคุมเพื่อให้ตรวจพบ (detective control) การควบคุมเพื่อให้ตรวจพบ เป็นการควบคุมที่กำหนดไว้เพื่อให้สามารถค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว เช่นการสอบทาน การวิเคราะห์ การยืนยันยอด การตรวจนับ การรายงานข้อบกพร่อง ฯลฯ

๒.๕.๓ การควบคุมโดยการชี้แนะ (directive control) การควบคุมโดยการชี้แนะที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การให้รางวัลแก่ผู้มีผลงานดี เป็นต้น

๒.๕.๔ การควบคุมเพื่อการแก้ไข (corrective control) การควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง

๒.๖ ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (information and communication) การจัดทำรายงานผลการติดตามการดำเนินการตามแผนการบริหารความเสี่ยงที่ได้ดำเนินการตามลำดับ ให้ฝ่ายบริหารรับทราบ และสามารถดำเนินการแก้ไขปัญหาที่มีได้ทันท่วงที

๒.๗ การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (monitoring) เป็นการดำเนินการอย่างต่อเนื่องในการตรวจสอบและรายงานผลอย่างเป็นระบบ เพื่อให้ทราบว่าแผนบริหารความเสี่ยงที่ดำเนินการอยู่นั้น มีความเหมาะสมกับสถานการณ์ที่มีการเปลี่ยนแปลงไปหรือไม่ รวมถึงทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงในทุกขั้นตอน และพัฒนาระบบให้ดียิ่งขึ้นรวมทั้งทำให้มีการปรับปรุงการทำงานต่าง ๆ

ทั้งนี้ การบริหารความเสี่ยงเป็นงานที่ต้องทำอย่างต่อเนื่อง ความเสี่ยงแต่ละประเภทเปลี่ยนไปตามความเปลี่ยนแปลงของโลก การบริหารความเสี่ยงจึงต้องได้รับความประเมินผล และปรับปรุงให้สอดคล้องกับสถานการณ์ปัจจุบัน การประเมินผลจึงไม่ใช่ขั้นตอนสุดท้ายของการบริหารความเสี่ยง แต่เป็นขั้นตอนที่นำไปสู่ระบบการบริหารความเสี่ยง ที่มีความต่อเนื่องและทันต่อเหตุการณ์

บทที่ ๔

แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

ในบทนี้จะกล่าวถึงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ เพื่อให้กรมทรัพยากรน้ำบาดาลใช้เป็นแนวทางในการจัดทำนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ โดยแบ่งออกเป็น ๒ ส่วนคือ ส่วนของแนวนโยบาย และส่วนของแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๑. แนวนโยบายรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ

๑.๑ วัตถุประสงค์

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยเกี่ยวกับระบบสารสนเทศของกรมฯ เพื่อให้เป็นไปตามหรือสอดคล้องกับพันธกิจ และระเบียบปฏิบัติที่เกี่ยวข้อง การจัดให้มีนโยบายรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ รวมถึงแนวปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

๑.๒ แนวทางปฏิบัติ

๑.๒.๑ การจัดทำนโยบาย

๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานต้องมีส่วนร่วมในการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศของกรมฯ

๒) ต้องจัดทำนโยบายที่เป็นลายลักษณ์อักษร และต้องได้รับการอนุมัติจากผู้บริหารก่อนนำไปเผยแพร่ด้วยการปิดประกาศและผ่านระบบอิเล็กทรอนิกส์ของกรมฯ เพื่อให้ผู้ใช้งาน บุคคลที่เกี่ยวข้อง รวมถึงหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบและใช้เป็นแนวทางปฏิบัติ

๓) ต้องกำหนดผู้รับผิดชอบตามนโยบายในด้านต่าง ๆ ให้ชัดเจน

๔) ผู้บริหารต้องดำเนินการทบทวน นโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร โดยต้องทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมอ

๑.๒.๒ รายละเอียดของนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศต้องระบุวัตถุประสงค์และขอบเขตอย่างชัดเจน และมีเนื้อหาครอบคลุมอย่างน้อยในเรื่องต่อไปนี้

๑) มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๒) มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึงโดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้ง มีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๓) มีนโยบายในมีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

๔) มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทาคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศให้แก่ผู้ใช้งานทั้งภายในและภายนอก

๑.๒.๓ การปฏิบัติตามนโยบาย

๑) ต้องประกาศใช้นโยบายและมีการประชาสัมพันธ์ให้แก่บุคคลที่เกี่ยวข้องอย่างทั่วถึง เพื่อให้สามารถปฏิบัติตามได้ เช่น จัดการฝึกอบรม เป็นต้น

๒) ต้องมีระบบติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามนโยบายอย่างเคร่งครัด

๓) ต้องมีการตรวจสอบ รวมทั้งประเมินความเพียงพอของนโยบายและระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยหน่วยงานที่เป็นอิสระอย่างน้อยปีละครั้ง ซึ่งอาจเป็นหน่วยงานตรวจสอบภายในของกรมฯ หรือผู้ตรวจสอบภายนอก

๔) ต้องแจ้งผู้บริหารหรือผู้มีอำนาจโดยเร็ว เมื่อมีกรณีที่ส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

๕) ต้องมีขั้นตอนหรือวิธีปฏิบัติเพื่อรองรับให้มีการปฏิบัติตามนโยบายที่ได้กำหนดไว้

๖) ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องอย่างชัดเจน เช่น หน้าที่ของผู้ใช้งานในกรณีที่พบว่าเครื่องคอมพิวเตอร์มีการติดไวรัส หน้าที่

และความรับผิดชอบของเจ้าหน้าที่รักษาความมั่นคงปลอดภัยระบบเครือข่าย หน้าที่และความรับผิดชอบของลูกจ้างชั่วคราว เป็นต้น

๒. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ

เพื่อเป็นการกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยมีเนื้อหาครอบคลุมอย่างน้อยดังต่อไปนี้

๒.๑ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑.๑ วัตถุประสงค์

เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ และเพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และระบบป้องกันความเสียหายต่าง ๆ

๒.๑.๒ แนวทางปฏิบัติ

ให้ศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล ปฏิบัติดังนี้

๑) กำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (network zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (server zone) ส่วนปฏิบัติงาน เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากยิ่งขึ้น

๒) กำหนดสิทธิในการเข้าถึง และมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานในแต่ละส่วนให้ชัดเจน

๓) จัดให้มีระบบบันทึกรายละเอียดการผ่านเข้า-ออกพื้นที่ใช้งานโดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

๔) ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารต้องมีระบบป้องกันความเสียหายต่าง ๆ ดังนี้

๔.๑) ระบบป้องกันไฟไหม้

- ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

- ในส่วนระบบเครือข่าย และส่วนเครื่องคอมพิวเตอร์แม่ข่าย ต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับส่วนปฏิบัติงานอย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

๔.๒) ระบบป้องกันไฟฟ้าขัดข้อง

- ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ

- ต้องมีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์สำคัญ เพื่อให้การดำเนินงานมีความต่อเนื่อง

๔.๓) ระบบควบคุมอุณหภูมิและความชื้นเพื่อควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (specification) ของอุปกรณ์คอมพิวเตอร์ เนื่องจากอุปกรณ์คอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

๒.๒ การรักษาความปลอดภัยด้านการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

๒.๒.๑ วัตถุประสงค์

เป็นการควบคุมการใช้ระบบคอมพิวเตอร์และระบบเครือข่ายเพื่อให้มีการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยให้ผู้ใช้บริการได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒.๒.๒ แนวทางปฏิบัติ

๑) ผู้ใช้บริการจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ เพื่อนำเข้า เผยแพร่ หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะดังต่อไปนี้

๑.๑) ข้อมูลคอมพิวเตอร์ใด ๆ ที่อาจกระทบกระเทือนต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

๑.๒) ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ซึ่งประชาชนทั่วไปอาจเข้าถึงข้อมูลนั้นได้

๑.๓) ข้อมูลคอมพิวเตอร์อันเป็นเท็จ หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน อันน่าจะเกิดความเสียหายแก่ผู้อื่น

๒) ผู้ใช้บริการจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตาม ๒.๒.๒ ๑) ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๓) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

๓.๑) ต้องมีขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติงานเกี่ยวกับระบบคอมพิวเตอร์ (computer operator) เช่น ขั้นตอนในการเปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

๓.๒) ควรกำหนดให้เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ปฏิบัติงานโดยผ่านเมนู และควรจำกัดการปฏิบัติงานโดยใช้ command line เท่าที่จำเป็น

๓.๓) ควรกำหนดให้มีการบันทึก (log book) รายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่างๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้

- ผู้ปฏิบัติงาน
- เวลาปฏิบัติงาน
- รายละเอียดการปฏิบัติงาน
- ปัญหาที่เกิดขึ้นและการแก้ไข
- สถานะของระบบ
- ผู้ตรวจทานการปฏิบัติงาน

๔) การติดตามการทำงานของระบบคอมพิวเตอร์ (monitoring)

๔.๑) ต้องติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เช่น การรับส่งข้อมูล การเชื่อมต่อระหว่างระบบคอมพิวเตอร์ส่วนกลางและระบบคอมพิวเตอร์ส่วนภูมิภาค การใช้งานฮาร์ดดิสก์ การใช้งานหน่วยประมวลผล (CPU) เป็นต้น เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพของระบบ

๔.๒) ควรบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่างๆ ให้อยู่ในสภาพที่ดีและพร้อมใช้งานอยู่เสมอ

๕) การจัดการปัญหาต่าง ๆ

๕.๑) ต้องกำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน เช่น กำหนดผู้รับผิดชอบในการแก้ไขปัญหาเกี่ยวกับ ฮาร์ดแวร์ ซอฟท์แวร์ และระบบเครือข่าย เป็นต้น ทั้งนี้ต้องระบุช่องทางในการติดต่อในกรณีที่มีปัญหา

๕.๒) ควรมีระบบจัดเก็บบันทึกปัญหาและเหตุการณ์ผิดปกติที่เกิดขึ้นและรายงานให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหาและตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาต่อไป

๒.๓ การรักษาความปลอดภัยด้านข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย

๒.๓.๑ วัตถุประสงค์

การรักษาความปลอดภัยด้านข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่ายมีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (integrity risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่ ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง malware ต่างๆ มิให้เข้าถึง หรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

๒.๓.๒ แนวทางปฏิบัติ

๑) การบริหารจัดการข้อมูล

๑.๑) ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๑.๒) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ เช่น การใช้ SSL VPN เป็นต้น ข้อมูลต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๑.๓) ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ นำเข้าประมวลผล และแสดงผล นอกจากนี้ ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน

๑.๔) ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ เช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒) การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User privilege)

๒.๑) ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๒) ในกรณีมีความจำเป็นต้องใช้ user ที่มีสิทธิพิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม โดยใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณา

- ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่ และควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

- ควรควบคุมการใช้งาน user ที่มีสิทธิพิเศษอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งาน user ดังกล่าวในลักษณะ dual control โดยให้เจ้าหน้าที่ ๒ รายถือรหัสผ่านคนละครึ่ง หรือเก็บ password ไว้ในตู้เซฟ เป็นต้น และจำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๒.๓) ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (log out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

๒.๔) ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ share files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐาน

๓) การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (user account)

๓.๑) ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (identification and authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี user account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น สำนักงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

๓.๒) ต้องมีระบบการเข้ารหัส (encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง

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

๔) การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (server)

๔.๑) ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

๔.๒) ต้องเปิดใช้บริการ (service) เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

๔.๓) ต้องดำเนินการติดตั้ง patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (system software) เช่น ระบบปฏิบัติการ DBMS และ web server เป็นต้น อย่างสม่ำเสมอ

๔.๔) ควรทดสอบ system software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

๔.๕) ควรมีแนวทางปฏิบัติในการใช้งาน software utility เช่น personal firewall password cracker เป็นต้น และตรวจสอบการใช้งาน software utility อย่างสม่ำเสมอ

๔.๖) ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของโปรแกรมระบบอย่างชัดเจน

๕) การบริหารจัดการและการตรวจสอบระบบเครือข่าย (network)

๕.๑) ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งานกลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (internal zone) โซนภายนอก (external zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๕.๒) ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๓) ผู้ดูแลระบบควรมีมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๕.๔) ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆได้ กำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต่างๆของระบบ

๕.๕) การป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง

นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่าparameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๕.๖) ระบบเครือข่ายทั้งหมดของกรมฯ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกกรมฯ ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (malware) ด้วย

๕.๗) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกรมฯ ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๖) การบริหารการเปลี่ยนแปลงระบบคอมพิวเตอร์ (configuration management)

๗) การวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (capacity planning)

๘) การป้องกันไวรัส และ malicious code

๙) บันทึกเพื่อการตรวจสอบ (audit logs)

๒.๔ การรักษาความปลอดภัยด้านการพัฒนาหรือปรับปรุงระบบงานคอมพิวเตอร์

๒.๔.๑ วัตถุประสงค์

การควบคุมการพัฒนา หรือปรับปรุงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

๒.๔.๒ แนวทางปฏิบัติ

๑) การกำหนดขั้นตอนการปฏิบัติงาน

๑.๑) ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน

๑.๒) ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (emergency change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

๑.๓) ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

๒) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

๒.๑) การร้องขอ

- การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร (อาจเป็น electronic transaction เช่น email เป็นต้น) และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หัวหน้าฝ่ายคอมพิวเตอร์ เป็นต้น

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

- ควรสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางการ

๒.๒) การพัฒนาระบบงาน

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

- ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ

- ควรตระหนักถึงระบบรักษาความปลอดภัย (security) และเสถียรภาพการทำงาน (availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

๒.๓) การทดสอบ

- ผู้ที่ร้องขอและฝ่ายคอมพิวเตอร์ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือ

แก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

- ในระบบงานสำคัญควรมีหน่วยงานหรือทีมงานอิสระ เข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนาและการทดสอบระบบ ก่อนที่จะโอนย้ายไปใช้งานจริง

๒.๔) การโอนย้ายระบบงานเพื่อใช้งานจริง ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

๒.๕) การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ version ของระบบงานที่ได้รับการพัฒนา

- ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา

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

- ต้องจัดเก็บโปรแกรม version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

๒.๖) การทดสอบหลังการใช้งาน (post- implementation test) ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

๒.๗) การสื่อสารการเปลี่ยนแปลง ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

๒.๕ การรักษาความปลอดภัยด้านการสำรองข้อมูลและระบบคอมพิวเตอร์

๒.๕.๑ วัตถุประสงค์

การสำรองข้อมูลและระบบคอมพิวเตอร์ มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และพร้อมใช้งานในเวลาที่ต้องการ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา

๒.๕.๒ แนวทางปฏิบัติ

๑) การสำรอง

๑.๑) ต้องสำรองข้อมูลสำคัญที่ใช้ในการปฏิบัติงาน รวมถึงโปรแกรมระบบปฏิบัติการ โปรแกรมระบบงานคอมพิวเตอร์ และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

๑.๒) ควรมีขั้นตอนและวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยอย่างน้อยควรมีรายละเอียด ดังนี้

- ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
- ประเภทสื่อบันทึก (media)
- จำนวนที่ต้องสำรอง (copy)
- ขั้นตอนและวิธีการสำรองโดยละเอียด
- สถานที่และวิธีการเก็บรักษาสื่อบันทึก

๑.๓) ควรมีการบันทึกการปฏิบัติงาน เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

๒) การทดสอบ

๒.๑) ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

๒.๒) ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

๓) การเก็บรักษา

๓.๑) ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในข้อ Physical Security ด้วย

๓.๒) ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

๓.๓) ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

๓.๔) การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา

๓.๕) ควรมีขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์ที่ยังค้างอยู่ใน recycle bin

๒.๖ การรักษาความปลอดภัยด้านการเตรียมพร้อมกรณีฉุกเฉิน

๒.๖.๑ วัตถุประสงค์

การเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีการจัดทำและการทดสอบแผนฉุกเฉิน เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และพร้อมใช้งานในกรณีเกิดเหตุการณ์ฉุกเฉิน

๒.๖.๒ แนวทางปฏิบัติ

๑) ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินต้องมีรายละเอียด ดังนี้

๑.๑) ต้องจัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงาน

๑.๒) ต้องกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

๑.๓) ต้องมีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

๑.๔) ต้องกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ

๑.๕) รวมทั้งต้องมีรายชื่อและหมายเลขโทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

๑.๖) ต้องมีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ขั้นต่ำ และอุปกรณ์เครือข่าย เป็นต้น

๑.๗) ในกรณีที่บริษัทมีศูนย์คอมพิวเตอร์สำรองก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น หมายเลขโทรศัพท์ สถานที่ตั้ง แผนที่ เป็นต้น

๑.๘) ต้องปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่

๒) ต้องทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย

๓) ควรสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น

๔) ในกรณีเกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

๒.๗ การรักษาความปลอดภัยด้านการใช้บริการจากผู้ให้บริการรายอื่น

๒.๗.๑ วัตถุประสงค์

การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงต่อกรมฯ ในรูปแบบต่าง ๆ เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลและการประมวลผลของระบบงาน ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น เพื่อให้กรมฯ ใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ จึงจำเป็นต้องกำหนดแนวปฏิบัติโดยมีเนื้อหาครอบคลุมเกี่ยวกับการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

๒.๗.๒ แนวทางปฏิบัติ

๑) การคัดเลือกผู้ให้บริการ

๑.๑) ควรมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ

๑.๒) ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) ขอบเขตงานและเงื่อนไขในการให้บริการอย่างชัดเจน

๒) การควบคุมผู้ให้บริการ

๒.๑) ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่ผู้รับผิดชอบ ควบคุมดูแลการทำงานของผู้ให้บริการอย่างละเอียดและใกล้ชิด ทั้งในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ในพื้นที่ของกรมฯ (onsite service) และในกรณีที่เป็นการให้บริการโดยเข้าถึงคอมพิวเตอร์หรือเครือข่ายจากระยะทางไกล (remote access) และต้องปิดการสื่อสาร (modem) ทันทีที่การให้บริการเสร็จสิ้น เป็นต้น

๒.๒) ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

๒.๓) ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข

๒.๔) ควรมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ ให้เป็นไปตามกฎระเบียบและวิธีปฏิบัติของทางราชการอย่างเคร่งครัด

๒.๘ การรักษาความปลอดภัยด้านการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

๒.๘.๑ วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานระบบจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรมฯ ซึ่งผู้ใช้ จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด ซึ่งจะส่งผลให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและ มีประสิทธิภาพ

๒.๘.๒ แนวทางปฏิบัติ

๑) สำหรับผู้ใช้งาน

๑.๑) ผู้ใช้งานที่ต้องการใช้ระบบจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรมฯ ต้องทำการกรอกข้อมูลคำขอเข้าใช้งานและยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิชื่อผู้ใช้งาน (user name) และรหัสผ่าน (password) และเมื่อได้รับรหัสผ่านแล้วจะต้องเปลี่ยนรหัสผ่าน โดยทันที หลังจากการเข้าสู่ระบบเป็นครั้งแรก

๑.๒) ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของกรมฯ เพื่อการทำงานของกรมฯ เท่านั้น

๑.๓) ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๑.๔) หลังจากการใช้งาน ควรลงชื่อออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบ

๑.๕) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๑.๖) ควรตรวจสอบและลบจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน เพื่อลดปริมาณการใช้พื้นที่ของระบบให้เหลือจำนวนน้อยที่สุด

๑.๗) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้งาน และรหัสผ่าน เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๑.๘) ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์

๒) สำหรับผู้ดูแลระบบ

๒.๑) ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมฯ ให้เหมาะสมกับการ เข้าใช้บริการของผู้ใช้ และหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้ง มีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การโอนย้าย เป็นต้น

๒.๒) ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมฯ

๒.๓) ต้องกำหนดการใส่รหัสผ่านจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น ‘*’ ในการพิมพ์แต่ละตัวอักษร

๒.๔) ควรกำหนดจานวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

๒.๕) ควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการตัดการใช้งานของผู้ใช้เมื่อผู้ใช้ ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

๒.๙ การรักษาความปลอดภัยด้านการใช้งานระบบอินเทอร์เน็ต (internet)

๒.๙.๑ วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และ เป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบ คอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของกรมฯ ถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒.๙.๒ แนวทางปฏิบัติ

๑) สำหรับผู้ใช้งาน

๑.๑) ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของกรมฯ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทาการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๑.๒) ต้องถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพ ของเครือข่ายและความปลอดภัยทางข้อมูลของกรมฯ

๑.๓) ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับกรมฯ

๑.๔) ห้ามผู้ใช้ เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๑.๕) ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูล คอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๑.๖) ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรมฯ รวมถึง การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

๑.๗) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดโปรแกรมเว็บบราวเซอร์ (web browser) เพื่อป้องกันการเข้าใช้งาน โดยบุคคลอื่น

๒) สำหรับผู้ดูแลระบบ

๒.๑) ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น firewall เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น dial-up modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและได้รับการอนุมัติจากผู้ดูแลระบบที่ได้รับมอบหมายแล้วเท่านั้น

๒.๒) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาจะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์

๒.๑๐ การรักษาความปลอดภัยด้านการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (traffic log)

๒.๑๐.๑ วัตถุประสงค์

เพื่อให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งเป็นข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ที่แสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๒.๑๐.๒ แนวทางปฏิบัติ

๑) ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

๒) ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน หรือบุคคลที่หน่วยงานมอบหมาย

๓) กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

บทที่ ๕

สรุปและข้อเสนอแนะ

๑. สรุป

ระบบบริหารจัดการความมั่นคงปลอดภัยด้านระบบสารสนเทศ (Information Security Management System: ISMS) เป็นส่วนหนึ่งของระบบบริหารจัดการความเสี่ยงขององค์กร ซึ่งมีกระบวนการตั้งแต่การ สร้าง นำมาใช้ ดำเนินการ ตรวจสอบติดตาม สอบทาน บำรุงรักษา และการพัฒนาความมั่นคงปลอดภัยด้านระบบสารสนเทศ โดยคำนึงถึงโครงสร้าง นโยบาย การวางแผน ความรับผิดชอบ การปฏิบัติ ขั้นตอน กระบวนการ และทรัพยากรขององค์กร

วัตถุประสงค์หลักของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ คือการกำหนดมาตรการที่ใช้สำหรับป้องกันผู้ที่ไม่ได้รับอนุญาตในการเข้าถึง ลบ แก้ไข หรือขัดขวางไม่ให้ผู้ที่ได้รับอนุญาตใช้งาน ได้รับความรู้ แนวคิด และข้อเท็จจริง ซึ่งการที่จะทำให้ระบบสารสนเทศมีความมั่นคงปลอดภัยนั้น.จำเป็นต้องคำนึงถึงสิ่งต่างๆ ดังต่อไปนี้

๑.๑ ความลับของข้อมูล (confidentiality)

๑.๒ ความถูกต้องสมบูรณ์ของข้อมูล (integrity)

๑.๓ การมีอยู่ของข้อมูล (availability)

๑.๔ ผู้ใช้ไม่สามารถปฏิเสธการกระทำ (non-repudiation)

๑.๕ การมีตัวตนจริงของผู้ใช้ระบบ (authentication)

๑.๖ การกำหนดสิทธิของผู้ใช้ระบบ (authorization)

เพื่อสร้างความตระหนักถึงความสำคัญและกระตุ้นให้บุคลากรทุกระดับของกรมฯ เล็งเห็นถึงความจำเป็นในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ ที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศซึ่งเป็นเครื่องมือที่สำคัญที่สุดในการให้บริการประชาชนและการตัดสินใจของผู้บริหาร ตลอดจนรัฐบาลผู้บริหารประเทศ

ระบบรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ จะทำให้เจ้าหน้าที่ที่เกี่ยวข้องทราบถึงแนวทางในการปฏิบัติ เพื่อหลีกเลี่ยงความเสี่ยงต่าง ๆ หรือลดความรุนแรงของผลเสียหายที่อาจเกิดขึ้นต่อระบบปฏิบัติราชการของกรมฯ จากการวิเคราะห์และประสบการณ์พบว่าปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นได้นั้น ส่วนใหญ่เกิดจากสามสาเหตุหลักคือ ๑) ด้านเทคโนโลยี ๒) ด้านกระบวนการทำงาน และ ๓) ด้านบุคลากร

ซึ่งปัญหาทั้ง ๓ ด้านข้างต้นหากกรมฯ ไม่ดำเนินการป้องกันและแก้ไข อาจทำให้กรมฯ มีภาวะเสี่ยงต่อการเกิดภาวะคุกคาม อาจก่อให้เกิดปัญหา อุปสรรค หรือการสูญเสียโอกาส ซึ่งจะมีผลทำให้กรมฯ ไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อหน่วยงาน โดยเฉพาะอย่างยิ่งผลเสียต่อระบบสารสนเทศที่องค์กรต้องใช้ในการบริหารงาน และปฏิบัติงาน โดยเฉพาะอย่างยิ่งด้านการให้บริการแก่ประชาชน

๒. ข้อเสนอแนะ

กรมฯ ควรเร่งจัดทำระบบบริหารความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้สามารถรองรับเหตุการณ์ด้านความมั่นคงปลอดภัยภายในองค์กร รวมทั้งเพื่อให้บุคลากรในหน่วยงานทราบถึงรูปแบบการดำเนินการที่เป็นรูปธรรม รวมถึงระเบียบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีขั้นตอนการดำเนินการดังต่อไปนี้

มอบหมายผู้รับผิดชอบในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๑ แต่งตั้งคณะกรรมการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ กำหนดนโยบายหรือแนวทางการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓ แต่งตั้งคณะทำงานบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อดำเนินการดังต่อไปนี้

๒.๓.๑ กำหนดโครงสร้างการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓.๒ ดำเนินการตามกระบวนการบริหารความเสี่ยงด้านระบบสารสนเทศ

๑) ระบุความเสี่ยง

๒) วิเคราะห์และประเมินความเสี่ยง

๓) จัดลำดับความสำคัญของปัจจัยเสี่ยง

๔) กำหนดกิจกรรมบริหารความเสี่ยง

๕) จัดทำแผนบริหารความเสี่ยงของแต่ละปัจจัยเสี่ยงที่อยู่ในระดับที่มีนัยสำคัญ

๖) สื่อสารทำความเข้าใจเกี่ยวกับแผนบริหารความเสี่ยงให้บุคลากรขององค์กร เพื่อให้สามารถนำไปปฏิบัติได้จริง

๗) รายงานสรุปผล ข้อดี ข้อเสีย ปัญหา อุปสรรค และข้อเสนอแนะของการดำเนินการตามแผนบริหารความเสี่ยงต่อประธานคณะกรรมการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

รายการอ้างอิง

กิตติพงษ์ เกียรตินิยมรุ่ง. ระบบมาตรฐานด้านความปลอดภัยของข้อมูล ISO/IEC 27001 (Information Security Management System: ISMS). เอกสารเผยแพร่บนเว็บไซต์ http://www.tuv.com/th/_iso_27001.html.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (๒๕๕๐). คู่มือการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (พ.ศ. ๒๕๔๙-๒๕๕๑). เอกสารเผยแพร่บนเว็บไซต์ http://security.mict.go.th. กรุงเทพมหานคร.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (๒๕๕๒). แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับที่ ๒ ของประเทศไทย (พ.ศ.๒๕๕๒-๒๕๕๖). เอกสารเผยแพร่บนเว็บไซต์ http://www.mict.go.th. กรุงเทพมหานคร.

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พุทธศักราช ๒๕๕๓. (๒๕๕๓, ๓๑ พฤษภาคม). ราชกิจจานุเบกษา เล่ม ๑๒๗ ตอนพิเศษ ๗๘ ง. หน้า ๑๓๑-๑๓๘.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช ๒๕๕๐. (๒๕๕๐, ๑๐ มิถุนายน). ราชกิจจานุเบกษา เล่ม ๑๒๔ ตอนที่ ๒๗ ก. หน้า ๔-๑๓.

บรรณานุกรม

กรมอนามัย. (๒๕๕๑). วิธีปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร. กรุงเทพมหานคร.

กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช. (๒๕๕๔). แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ. กรุงเทพมหานคร.

สำนักงานตำรวจแห่งชาติ. (๒๕๕๑). นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ. เอกสารเผยแพร่บนเว็บไซต์ http://www.edupol.org/edu_P/note/note3/doc/download-201.pdf. กรุงเทพมหานคร.

กรมฯ . (๒๕๕๓). คู่มือการปฏิบัติงานการพัฒนาข้อมูลและเทคโนโลยีสารสนเทศ. กรุงเทพมหานคร : ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร.

ภาคผนวก

– ร่าง –

คำสั่งกรมทรัพยากรน้ำบาดาล
ที่ __ / ๒๕๕๕
เรื่อง แต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัย
ระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมทรัพยากรน้ำบาดาลสามารถรองรับเหตุการณ์ด้านความมั่นคงปลอดภัยภายในองค์กร จึงมีคำสั่ง ดังนี้

๑.	ผู้บริหารสารสนเทศระดับสูง (CIO)	ประธาน
๒.	ผู้อำนวยการสำนักสำรวจและประเมินศักยภาพน้ำบาดาล	กรรมการ
๓.	ผู้อำนวยการสำนักอนุรักษ์และฟื้นฟูทรัพยากรน้ำบาดาล	กรรมการ
๔.	ผู้อำนวยการสำนักพัฒนาทรัพยากรน้ำบาดาล	กรรมการ
๕.	ผู้อำนวยการสำนักบริหารกลาง	กรรมการ
๖.	ผู้อำนวยการสำนักควบคุมการประกอบกิจการน้ำบาดาล	กรรมการ
๗.	ผู้อำนวยการสำนักพัฒนาทรัพยากรน้ำบาดาลเขต ๑ – ๑๒	กรรมการ
๘.	ผู้อำนวยการกองแผนงาน	กรรมการ
๙.	ผู้อำนวยการกองวิเคราะห์น้ำบาดาล	กรรมการ
๑๐.	ผู้อำนวยการกลุ่มนิติการ	กรรมการ
๑๑.	ผู้อำนวยการกลุ่มตรวจสอบภายใน	กรรมการ
๑๒.	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทรัพยากรน้ำบาดาล	กรรมการและเลขานุการ

ให้คณะกรรมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร มีอำนาจหน้าที่ดังนี้

๑. แต่งตั้งคณะทำงานที่มีความเหมาะสม (มีความรู้ความสามารถและประสบการณ์ด้านระบบสารสนเทศ ในระดับที่สามารถรับและถ่ายทอดความรู้ด้านการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร) รับผิดชอบดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒. รายงานเหตุการณ์ด้านการรักษาความปลอดภัยระบบสารสนเทศ ของหน่วยงาน ให้ผู้บริหารทราบเป็นประจำทุกเดือน และรายงานทันทีที่พบว่าระบบฯ ถูกบุกรุก เพื่อให้ผู้เกี่ยวข้องตรวจสอบจุดอ่อน รวมทั้งความเสียหายและหาทางแก้ไขได้อย่างถูกต้อง

๓. เสนอนโยบายด้านการรักษาความปลอดภัยระบบฯ เช่น การอนุญาตเข้าถึงข้อมูลหรือระบบสารสนเทศที่มีความสำคัญ ระเบียบปฏิบัติในการใช้งานระบบอย่างปลอดภัย

๔. ควบคุม กำกับ ดูแลให้มีการปฏิบัติตามระเบียบการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่...../...../ ๒๕๕๕

ลงชื่อ.....

(นายปราณีต ร้อยบาง)

อธิบดีกรมทรัพยากรน้ำบาดาล