คู่มือการรักษาความมั่นคงปลอดภัย

ด้านสารสนเทศของโรงพิมพ์ตำรวจ

คำนำ

ปัจจุบันระบบเครือข่ายคอมพิวเตอร์มีความสำคัญต่อการดำเนินงานของทุกองค์กรที่ต้องการทำให้การเข้าถึงข้อมูลมีความรวดเร็ว ถูกต้อง แม่นยำ สามารถติดต่อสื่อสารได้อย่างมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงาน ประกอบกับการพัฒนาอย่างรวดเร็วของระบบเครือข่ายอินเตอร์เน็ต ส่งผลให้การเชื่อมต่อระหว่างระบบเครือข่ายคอมพิวเตอร์ขององค์กรกับระบบเครือข่ายอินเตอร์เน็ตมีความจำเป็นและมีการใช้งานกันอย่างแพร่หลาย

ระบบเครือข่ายอินเตอร์เน็ตนั้นมีทั้งในแง่ดีซึ่งมากมายเกินกว่าจะกล่าวถึง แต่ในแง่ที่ไม่ดีก็มีมากมายเช่นกัน เหตุผลก็เนื่องจากระบบเครือข่ายอินเตอร์เน็ตนั้นเปรียบเสมือนห้องสมุด เป็นแหล่งการเรียนรู้ เป็นแหล่งสืบค้นที่ใหญ่ที่สุดในโลก เราต้องการทราบข้อมูลอะไรก็สามารถค้นหาได้จากเครือข่ายอินเตอร์เน็ต แต่ในแง่ของผู้ไม่ประสงค์ดีก็ใช้ช่องทางนี้เช่นกันในการสืบค้นข้อมูลเครื่องมือ หรือค้นหาวิธีการในการเจาะระบบเครือข่าย ทำให้ระบบเครือข่ายขององค์กรมีโอกาสถูกบุกรุกได้มากขึ้น ผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสารจึงควรตระหนักถึงการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศขององค์กรอย่างจริงจัง

หวังเป็นอย่างยิ่งว่า คู่มือ “การจัดทำระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพิมพ์ตำรวจ” ฉบับนี้ จะเป็นประโยชน์แก่ผู้บริหาร และบุคลากรที่เกี่ยวข้องกับระบบดิจิทัลของโรงพิมพ์ตำรวจ ในการจัดทำระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต่อไป

สารบัญ

บทนำ 1

ความมั่นคงปลอดภัยของระบบสารสนเทศ 4

การบริหารความเสี่ยงของระบบสารสนเทศ 12

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ 19

แนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity) 55

แนวทางในการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ ขององค์กร (ISMS Audit) 63

แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ IT Risk Management Implementation Guideline 65

กระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสำรสนเทศ (ISMS) ขององค์กร 99

กระบวนการบริหารจัดการบริหารความเสี่ยงความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร 101

สรุปและข้อเสนอแนะ 104

บทนำ

การบริหารงานขององค์กรทุกประเภท ทั้งภาครัฐและภาคเอกชน ต่างมีวัตถุประสงค์ของตนเอง และมุ่งหวังที่จะทำงานไปให้ถึงเป้าหมายที่วางไว้อย่างดีที่สุด สูญเสียทรัพยากรให้น้อยที่สุด แต่การดำเนินการใด ๆ เพื่อให้บรรลุวัตถุประสงค์ที่วางไว้ มักจะต้องประสบกับความเสี่ยงที่จะเกิดความผิดพลาด ความเสียหาย ความสูญเปล่าหรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจเกิดขึ้นอย่างเฉียบพลันหรืออาจเริ่มต้นเพียงเล็กน้อยแล้วเพิ่มความรุนแรงต่อไปเรื่อย ๆ ซึ่งจะมีผลกระทบทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์ เป้าประสงค์ และเป้าหมายขององค์กรความก้าวหน้าของเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้น ส่งผลให้ความต้องการในการดูแลความมั่นคงปลอดภัยของระบบสารสนเทศเพิ่มสูงขึ้นด้วย องค์กรต่าง ๆ ทั้งภาครัฐและภาคเอกชนต่าง ๆ ก็ให้ความสำคัญอย่างมากต่อการพัฒนาระบบเพื่อการดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ มีการพัฒนามาตรฐานเกี่ยวกับการดูแลรักษาความมั่นคงปลอดภัยระบบสารสนเทศออกมาอย่างต่อเนื่อง เพื่อป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในรูปแบบต่าง ๆ ที่มีต่อระบบสารสนเทศขององค์กร ซึ่งนับวันจะทวีความรุนแรง และท้าทายต่อผู้ที่รับผิดชอบในการดูแลระบบ เป็นอย่างมากทุกองค์กรที่มีการนำระบบคอมพิวเตอร์มาใช้ในการปฏิบัติงานจำเป็นอย่างยิ่งที่จะต้องกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ซึ่งจะต้องกำหนดให้ใครมีสิทธิและใครไม่มีสิทธิเข้าถึงระบบสารสนเทศทั้งทางด้านกายภาพและทางอิเล็กทรอนิกส์ และควรที่จะมีระเบียบแบบแผนการปฏิบัติที่ชัดเจนในการใช้ระบบสารสนเทศขององค์กร องค์กรต้องมีแผนปฏิบัติเมื่อเกิดเหตุฉุกเฉิน หรือเมื่อเกิดเหตุการณ์เกี่ยวกับความมั่นคงและความปลอดภัย นอกจากนี้องค์กรและผู้ใช้เองก็ต้องนำนโยบายด้านการรักษาความมั่นคงปลอดภัยมาใช้อย่างเคร่งครัดด้วย

1. หลักการและเหตุผล

การจัดทำคู่มือการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้กำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทาง (roadmap) เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ “คู่มือการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของโรงพิมพ์ตำรวจ” ฉบับนี้จัดทำขึ้นเพื่อใช้เป็นแนวทางในการกำหนดโยบายแนวปฏิบัติ และวิธีปฏิบัติ เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ซึ่งเป็นเครื่องมือที่สำคัญในการปฏิบัติงานและการบริหารขององค์กร

2. วัตถุประสงค์

คู่มือฉบับนี้ จัดทำขึ้นเพื่อวัตถุประสงค์ดังนี้

2.1 เพื่อใช้เป็นแนวทางในการจัดทำระบบบริหารความมั่นคงปลอดภัยของสารสนเทศให้เป็นไปตามมาตรฐานสากล ส่งผลให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและมีประสิทธิภาพ

2.2 เพื่อให้ฝ่ายบริหาร และฝ่ายปฏิบัติการ เข้าใจหลักการและกระบวนการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2.3 เพื่อให้มีการปฏิบัติตามกระบวนการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นระบบและต่อเนื่อง

2.4 เพื่อเป็นเครื่องมือสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศกับกลยุทธ์ของโรงพิมพ์ตำรวจ

2.5 เพื่อใช้เป็นเครื่องมือในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ในหน่วยงานทุกระดับของโรงพิมพ์ตำรวจ ให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และให้เจ้าหน้าที่ทุกระดับในโรงพิมพ์ตำรวจ และบุคคลที่เกี่ยวข้อง ถือปฏิบัติอย่างเคร่งครัด

3. นิยามและคำจำกัดความที่สำคัญ

“องค์กร” หมายถึง โรงพิมพ์ตำรวจ

“ผู้บริหาร” หมายถึง ผู้อำนวยการหรือรองผู้อำนวยการ

“ผู้บริหารสารสนเทศระดับสูง (Chief Information Officer: CIO)” หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน รวมถึงการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

“หน่วยงาน” หมายถึง ฝ่าย งาน หมวด

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายถึง กลุ่มของคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่ถูกนำมาเชื่อมต่อกันผ่านอุปกรณ์ด้านการสื่อสารหรือสื่ออื่นใด ทำให้ผู้ใช้ในระบบเครือข่ายสามารถติดต่อสื่อสารแลกเปลี่ยนและใช้อุปกรณ์ต่าง ๆ ของเครือข่ายร่วมกันได้

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

“ผู้มีอำนาจ” หมายถึง หัวหน้าหน่วยงานที่มีระบบคอมพิวเตอร์ขององค์กร อยู่ในความครอบครอง และให้หมายความรวมถึงผู้ซึ่งได้รับมอบหมายจากบุคคลดังกล่าวด้วย

“ผู้ใช้งาน” หมายถึง พนักงาน ลูกจ้าง เจ้าหน้าที่ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการหรือผู้ที่หน่วยงานอนุญาตให้ใช้ระบบคอมพิวเตอร์ได้

“ผู้ดูแลระบบ (system administrator)” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“บัญชีผู้ใช้งาน” หมายถึง บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร

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

“ความเสี่ยง (risk)” หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหลความสูญเสีย ความสูญเปล่า หรือเหตุการณ์ซึ่งไม่พึงประสงค์ที่ทำให้งานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนด

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

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

“การวิเคราะห์ความเสี่ยง (risk analysis)” หมายถึง ขั้นตอนการวิเคราะห์ความเสี่ยงหรือผลกระทบของความเสี่ยงต่อองค์กร เทคนิคการวิเคราะห์ความเสี่ยงมีหลายวิธี เพราะการวัดความเสี่ยงเป็นตัวเลขว่ามีผลต่อองค์กรเท่าไรนั้นเป็นสิ่งที่ทำได้ยาก โดยทั่วไปจะวิเคราะห์ความเสี่ยงโดยประเมินนัยสำคัญหรือผลกระทบของความเสี่ยง และความถี่ที่จะเกิด หรือโอกาสที่จะเกิดความเสี่ยง

“การประเมินความเสี่ยง (risk assessment)” หมายถึง กระบวนการที่ใช้ในการระบุ และวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง

“การบริหารความเสี่ยง (risk management)” หมายถึง กระบวนการจัดการความเสี่ยง ประกอบด้วยกระบวนการในการระบุ วิเคราะห์ (risk analysis) ประเมิน (risk assessment) ดูแลตรวจสอบและควบคุมความเสี่ยงที่สัมพันธ์กับ ภารกิจ หน้าที่ และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด

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

ความมั่นคงปลอดภัยของระบบสารสนเทศ

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

1. จุดประสงค์ของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ

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

1.1 การรักษาความลับ (confidentiality) คือการรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ ทำให้มั่นใจว่ามีเฉพาะผู้มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้

1.2 การรักษาความสมบูรณ์ (integrity) คือการรับรองว่าข้อมูลที่ปกป้องนั้น ต้องมีความถูกต้องสมบูรณ์ จะไม่ถูกแก้ไข เปลี่ยนแปลง หรือทำลาย จากผู้ไม่มีสิทธิไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา

1.3 ความพร้อมใช้ (availability) คือการรับรองว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมใช้งานสามารถตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ

1.4 การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) คือวิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

2. องค์ประกอบของระบบสารสนเทศ

ระบบสารสนเทศซึ่งเป็นระบบสนับสนุนการบริหารงาน การจัดการ และการปฏิบัติงานของบุคลากร ไม่ว่าจะเป็นระดับบุคคล ระดับกลุ่ม หรือ ระดับองค์กร ไม่ใช่มีเพียงเครื่องคอมพิวเตอร์เท่านั้น แต่ยังมีองค์ประกอบอื่น ๆ ที่เกี่ยวข้องกับความสำเร็จของระบบอีก รวม 5 องค์ประกอบ ซึ่งจะขาดองค์ประกอบใดไม่ได้คือ

2.1 ฮาร์ดแวร์ เป็นองค์ประกอบสำคัญของระบบสารสนเทศ หมายถึง เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง รวมทั้งอุปกรณ์สื่อสารสำหรับเชื่อมโยงคอมพิวเตอร์เข้าเป็นเครือข่ายเช่น เครื่องพิมพ์ อุปกรณ์กระจายสัญญาณ

2.2 ซอฟต์แวร์ หรือโปรแกรมคอมพิวเตอร์เป็นองค์ประกอบที่สำคัญประการที่สอง ซึ่งก็คือลำดับขั้นตอนของคำสั่งที่จะสั่งงานให้ฮาร์ดแวร์ทำงาน เพื่อประมวลผลข้อมูลให้ได้ผลลัพธ์ตามความต้องการของการใช้งาน ในปัจจุบันมีซอฟต์แวร์ระบบปฏิบัติงาน ซอฟต์แวร์ควบคุมระบบงานซอฟต์แวร์สำเร็จ และซอฟต์แวร์ประยุกต์สำหรับงานต่าง ๆ ลักษณะการใช้งานของซอฟต์แวร์ก่อนหน้านี้ ผู้ใช้จะต้องติดต่อใช้งานโดยใช้ข้อความเป็นหลัก แต่ในปัจจุบันซอฟต์แวร์มีลักษณะการใช้งานที่ง่ายขึ้น ส่วนซอฟต์แวร์สำเร็จที่มีใช้ในท้องตลาดทำให้การใช้งานคอมพิวเตอร์ในระดับบุคคลเป็นไปอย่างกว้างขวาง และเริ่มมีลักษณะส่งเสริมการทำงานของกลุ่มมากขึ้น ส่วนงานในระดับองค์กรส่วนใหญ่มักจะมีการพัฒนาระบบตามความต้องการโดยการว่าจ้าง หรือโดยนักคอมพิวเตอร์ขององค์กร เป็นต้น ซอฟต์แวร์สามารถแบ่งได้ดังนี้

2.2.1 ซอฟต์แวร์ระบบ หมายถึง โปรแกรมทุกโปรแกรมที่ทำหน้าที่ติดต่อกับส่วนประกอบต่าง ๆ ของฮาร์ดแวร์คอมพิวเตอร์ และอำนวยเครื่องมือสำหรับทำงานพื้นฐานต่าง ๆ ที่เกี่ยวข้องกับฮาร์ดแวร์

2.2.2 ซอฟต์แวร์ประยุกต์ จะเป็นโปรแกรมที่ทำให้คอมพิวเตอร์สามารถทำงานต่าง ๆ ตามที่ผู้ใช้ต้องการ ไม่ว่างานด้านการจัดทำเอกสาร การทำบัญชี การจัดเก็บข้อมูลข่าวสารตลอดจนงานทุก ๆ ด้านตามแต่ผู้ใช้ต้องการ จนสามารถกล่าวได้ว่าซอฟต์แวร์ประยุกต์ก็คือซอฟต์แวร์ที่ทำให้เกิดการใช้งานคอมพิวเตอร์กันอย่างกว้างขวาง และทำให้คอมพิวเตอร์เป็นปัจจัยที่ไม่สามารถขาดได้ในยุคสารสนเทศนี้ ในองค์กรขนาดใหญ่หรืองานที่มีความต้องการเฉพาะด้าน การจัดหาซอฟต์แวร์มาใช้งานจะใช้วิธีพัฒนาซอฟต์แวร์ขึ้นมาเอง หรือว่าจ้างบริษัทซอฟต์แวร์เพื่อทำซอฟต์แวร์เฉพาะงานขึ้นมาใช้เอง ซอฟต์แวร์ประเภทนี้จะเรียกว่าซอฟต์แวร์เฉพาะงาน มีข้อดีคือมีความเหมาะสมกับงานและสามารถแก้ไขตามความต้องการได้ ข้อเสียคือค่าใช้จ่ายสูงและใช้เวลาสำหรับการพัฒนา ปัจจุบันนี้จึงมีโปรแกรมคอมพิวเตอร์ที่เขียนขึ้นมาเพื่อใช้สำหรับงานทั่ว ๆ ไป วางจำหน่ายเป็นชุดสำเร็จรูปเรียกว่าซอฟต์แวร์สำเร็จรูป

2.3 ข้อมูล เป็นองค์ประกอบที่สำคัญอีกประการหนึ่งของระบบสารสนเทศ อาจจะเป็นตัวชี้ความสำเร็จหรือความล้มเหลวของระบบได้ เนื่องจากจะต้องมีการเก็บข้อมูลจากแหล่งกำเนิดข้อมูลจะต้องมีความถูกต้อง มีการกลั่นกรองและตรวจสอบแล้วเท่านั้นจึงจะมีประโยชน์ ข้อมูลจำเป็นจะต้องมีมาตรฐานโดยเฉพาะอย่างยิ่งเมื่อใช้งานในระดับกลุ่มหรือระดับองค์กร ข้อมูลต้องมีโครงสร้างในการจัดเก็บที่เป็นระบบระเบียบเพื่อการสืบค้นที่รวดเร็วมีประสิทธิภาพ

2.4 บุคลากร ในระดับผู้บริหาร ผู้ดูแลระบบ ผู้พัฒนาระบบ และผู้ใช้บริการ เป็นองค์ประกอบสำคัญในความสำเร็จของระบบสารสนเทศบุคลากรมีความรู้ความสามารถทางคอมพิวเตอร์มากเท่าใด โอกาสที่จะใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ได้เต็มศักยภาพและคุ้มค่ายิ่งมากขึ้นเท่านั้น โดยเฉพาะระบบสารสนเทศในระดับบุคคลซึ่งเครื่องคอมพิวเตอร์มีขีดความสามารถมากขึ้น ทำให้ผู้ใช้มีโอกาสพัฒนาความสามารถของตนเองและพัฒนาระบบงานได้เองตามความต้องการ สำหรับระบบสารสนเทศในระดับกลุ่ม

และองค์กรที่มีความซับซ้อนมาก อาจจะต้องใช้บุคลากรในสาขาคอมพิวเตอร์ โดยตรงมาพัฒนาและดูแลระบบงาน

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

3. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

การนำมาตรฐานการรักษาความมั่นคงปลอดภัยมาประยุกต์ใช้กับระบบสารสนเทศในองค์กรเริ่มเป็นที่แพร่หลายมากขึ้น มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานหนึ่งที่กำลังได้รับความนิยมอย่างแพร่หลายในปัจจุบัน ได้รับการยอมรับจากหลายประเทศในการนำไปใช้บริหารจัดการระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

การบริหารจัดการเรื่องความมั่นคงปลอดภัยของระบบสารสนเทศมีประสิทธิผลเต็มที่ ทำให้องค์กรรอดพ้นจากภัยคุกคามต่าง ๆ และทำให้องค์กรมั่นใจที่จะใช้ระบบสารสนเทศมาเป็นเครื่องมือในการปฏิบัติงานตามภารกิจขององค์กร ซึ่งสาระสำคัญของมาตรฐานดังกล่าว แบ่งเป็น 2 ส่วนหลักคือ

3.1 กระบวนการการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

3.1.1 รายละเอียดของระบบบริหารจัดการความปลอดภัยสำหรับสารสนเทศ

1) ข้อกำหนดทั่วไป

องค์กรจะต้องกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวนบำรุง รักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ได้กำหนดไว้เป็นลายลักษณ์อักษร ภายในกรอบกิจกรรมการดำเนินการตามภารกิจต่าง ๆ รวมทั้งความเสี่ยงที่เกี่ยวข้อง แนวทางที่ใช้ในมาตรฐานนี้จะนำกระบวนการดำเนินงานที่มีคุณภาพตามวงจร Plan-Do-Check-Act มาประยุกต์ใช้ รวมถึงระบบการปฏิบัติงานต่าง ๆ ที่เกิดขึ้นทำให้ระบบการรักษาความมั่นคงปลอดภัยข้อมูลตรงตามความต้องการและความคาดหมายได้ ซึ่งแต่ละขั้นตอนประกอบด้วยรายละเอียดโดยย่อ ดังนี้

1) Plan คือการวางแผน การกำหนดนโยบายความมั่นคง

2) Do คือการลงมือปฏิบัติหรือดำเนินการตามระบบ

3) Check คือการตรวจสอบและทบทวนผลการดำเนินการตามระบบ

4) Act คือ การแก้ไข บำรุงรักษา และปรับปรุงคุณภาพของระบบ ๆ

เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบและมีการพัฒนาขึ้นอย่างต่อเนื่อง

1.1) กำหนดระบบบริหารจัดการความมั่นคงปลอดภัย โดยองค์กรควรกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยและกำหนดนโยบายความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะขององค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี นอกจากนี้ยังต้องกำหนดวิธีการ

ประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร ระบบความเสี่ยง วิเคราะห์และประเมินความเสี่ยง ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงการดำเนินการที่เป็นไปได้เลือกวัตถุประสงค์และมาตรการทางด้านความปลอดภัยเพื่อจัดการกับความเสี่ยง

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

1.3) เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย (Check) โดยองค์กรควรลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่น ๆ สำหรับการเฝ้าระวังและทบทวน ดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ วัดความสัมฤทธิ์ผลของมาตรการทางด้านความมั่นคงปลอดภัย ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้กับระดับความเสี่ยงที่เหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ ดำเนินการตรวจสอบและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย ปรับปรุงแผนทางด้านความปลอดภัยโดยนำผลของการเฝ้าระวัง และทบทวนกิจกรรมต่าง ๆ มาพิจารณาร่วมด้วย และบันทึกการดำเนินการซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

1.4) บำรุงรักษาและปรับปรุงระบบบริหารจัดการด้านความมั่นคงปลอดภัย (Act) โดยองค์กรควรปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้ รวมถึงการใช้มาตรการเชิงแก้ไขป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและองค์กรอื่น แจ้งการปรับปรุงและดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้อง และตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

2) ข้อกำหนดทางด้านการจัดทำเอกสาร

2.1) ความต้องการทั่วไป เอกสารที่จำเป็นต้องจัดทำจะรวมถึงบันทึกแสดงการตัดสินใจของผู้บริหาร ได้แก่ นโยบายความมั่นคงปลอดภัย ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย วิธีการประเมินความเสี่ยง เป็นต้น

2.2) การบริหารจัดการเอกสาร ซึ่งเอกสารตามข้อกำหนดของระบบบริหารจัดการความมั่นคงปลอดภัยจะต้องได้รับการป้องกันและควบคุม ขั้นตอนการปฏิบัติที่เกี่ยวข้องกับการจัดการเอกสาร ได้แก่ อนุมัติการใช้งานเอกสารก่อนที่จะเผยแพร่ ทบทวน ปรับปรุงและอนุมัติเอกสารตามความจำเป็น ระบุการเปลี่ยนแปลงและสถานภาพของเอกสารปัจจุบัน เป็นต้น

2.3) การบริหารจัดการบันทึกข้อมูลหรือฟอร์มต่าง ๆ องค์กรจะต้องมีการกำหนดจัดทำและบำรุงรักษาบันทึกข้อมูลหรือฟอร์มต่าง ๆ เพื่อใช้เป็นหลักฐานแสดงความสอดคล้องกับข้อกำหนดและการดำเนินการที่มีประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

3.1.2 หน้าที่ความรับผิดชอบของผู้บริหาร

1) การให้ความสำคัญในการบริหารจัดการ โดยผู้บริหารจะต้องแสดงถึงการให้ความสำคัญต่อการกำหนดการลงมือปฏิบัติการ ดำเนินการ เฝ้าระวัง การทบทวน การบำรุงรักษาและการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย

2) การบริหารจัดการทรัพยากรที่จำเป็นและการอบรม การสร้างความตระหนักและการเพิ่มขีดความสามารถเพื่อให้บุคลากรทั้งหมดที่ได้รับมอบหมายหน้าที่สามารถปฏิบัติงานได้ตามที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย

3.1.3 องค์กรควรดำเนินการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนดไว้เพื่อตรวจสอบว่า วัตถุประสงค์ มาตรการ กระบวนการ และขั้นตอนปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัยมีความสอดคล้องกับข้อกำหนดในมาตรฐานฉบับนี้และกฎหมายระเบียบ ข้อบังคับต่าง ๆ รวมถึงสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย และได้รับการลงมือปฏิบัติและบำรุงรักษาอย่างสัมฤทธิ์ผลและเป็นไปตามที่คาดหมายไว้ นอกจากนี้ องค์กรจะต้องวางแผนตรวจสอบภายในโดยพิจารณาถึงสถานภาพและความสำคัญของกระบวนการและส่วนต่าง ๆ ที่จะได้รับการตรวจสอบและผลการตรวจสอบในครั้งที่ผ่านมา รวมถึงองค์กรจะต้องระบุหน้าที่ความรับผิดชอบและข้อกำหนดต่าง ๆ ในการวางแผนและดำเนินการตรวจสอบ จัดทำรายงานผลการตรวจสอบและบันทึกข้อมูลของการตรวจสอบนั้น

3.1.4 ผู้บริหารจะต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนดไว้ (เช่นปีละ 1 ครั้ง) เพื่อให้มีการดำเนินการที่เหมาะสม พอเพียงและสัมฤทธิ์ผลการทบทวนจะต้องรวมถึงการปรับปรุงหรือเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งหมายรวมถึงนโยบายความมั่นคงปลอดภัยและวัตถุประสงค์ทางด้านความปลอดภัย ผลของการทบทวนจะต้องได้รับการบันทึกไว้อย่างเป็นลายลักษณ์อักษรและบันทึกข้อมูลที่เกี่ยวข้องกับการทบทวนจะต้องได้รับการบำรุงรักษาไว้

3.2 มาตรการการจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

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

3.2.2 โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (internal organization) โดยได้กล่าวถึงบทบาทของผู้บริหารองค์กรและหัวหน้างานสารสนเทศ ในด้านต่าง ๆ ดังต่อไปนี้

1) โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

2) โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับหน่วยงานภายนอก เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับหน่วยงานภายนอก

3.2.3 การบริหารจัดการทรัพย์สินขององค์กร (asset management) โดยได้กล่าวถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานพัสดุในด้านต่าง ๆ ดังต่อไปนี้

1) หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจขึ้นได้

2) การจัดหมวดหมู่สารสนเทศ เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

3.2.4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (human resources security) โดยได้กล่าวถึงบทบาทของผู้บริหารสารสนเทศ หัวหน้าหมวดสารสนเทศ หัวหน้าหมวดบริหารงานบุคคล และหัวหน้างาน หัวหน้าหมวดที่เกี่ยวข้อง ดังต่อไปนี้

1) การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

2) การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคาม และปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบ และทำความเข้าใจกับนโยบาย เพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

3) การสิ้นสุดและการเปลี่ยนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

3.2.5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (physical and environmental security) โดยได้กล่าวถึงบทบาทของหัวหน้าหมวดสารสนเทศ ดังต่อไปนี้

1) บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

2) ความมั่นคงปลอดภัยของอุปกรณ์ เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และทำให้กิจกรรมการดำเนินงานต่าง ๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

3.2.6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (communications and operations management) โดยได้กล่าวถึงบทบาทของผู้บริหารองค์กร ผู้บริหารสารสนเทศ หัวหน้าหมวดสารสนเทศ ผู้ที่เป็นเจ้าของกระบวนการทำงาน และเจ้าหน้าที่สารสนเทศในด้านต่าง ๆ ดังต่อไปนี้

1) การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

2) การบริหารจัดการการให้บริการของหน่วยงานภายนอก เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

3) การวางแผนและการตรวจรับทรัพยากรสารสนเทศ เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

4) การป้องกันโปรแกรมที่ไม่ประสงค์ดี เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

5) การสำรองข้อมูล เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

6) การบริหารจัดการทางด้านความปลอดภัยสำหรับเครือข่ายขององค์กรเพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

7) การจัดการสื่อที่ใช้ในการบันทึกข้อมูล เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ

8) การแลกเปลี่ยนสารสนเทศ เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

9) การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และการใช้งาน

10) การเฝ้าระวังทางด้านความมั่นคงปลอดภัย เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

3.2.7 การควบคุมการเข้าถึง (access control) โดยได้กล่าวถึงบทบาทของผู้บริหารสารสนเทศ หัวหน้าหมวดสารสนเทศ ผู้ดูแลระบบและเจ้าหน้าที่ในด้านต่าง ๆ ดังต่อไปนี้

1) ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ เพื่อควบคุมการเข้าถึงสารสนเทศ

2) การบริหารจัดการการเข้าถึงของผู้ใช้ เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

3) การควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต

4) การควบคุมการเข้าถึงระบบปฏิบัติการที่ไม่ได้รับอนุญาต

5) การควบคุมการเข้าถึง application และสารสนเทศที่ไม่ได้รับอนุญาต

6) การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกเพื่อสร้างความมั่นคงปลอดภัยให้กับอุปกรณ์และการปฏิบัติงานที่เกี่ยวข้อง

3.2.8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (information systems acquisition, development and maintenance) โดยได้กล่าวถึงบทบาทของหัวหน้าหมวดสารสนเทศ ผู้พัฒนาระบบ และผู้เป็นเจ้าของระบบในด้านต่าง ๆ ดังต่อไปนี้

1) ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ เพื่อให้การจัดหาและพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

2) การประมวลผลสารสนเทศใน application เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาตหรือการใช้งานสารสนเทศผิดวัตถุประสงค์

3) มาตรการการเข้ารหัสข้อมูล เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการทางการเข้ารหัสข้อมูล

4) การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

5) การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

6) การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

3.2.9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (information security incident management) โดยได้กล่าวถึงบทบาทของหัวหน้าหมวดสารสนเทศนิติกร ผู้ดูแลระบบ และเจ้าหน้าที่ในด้านต่าง ๆ ดังต่อไปนี้

1) การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

1) การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

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

3.2.11 การปฏิบัติตามข้อกำหนด (compliance) โดยได้กล่าวถึงบทบาทของหัวหน้าหมวดสารสนเทศ และนิติกร ในด้านต่าง ๆ ดังต่อไปนี้

1) การปฏิบัติตามข้อกำหนดทางกฎหมาย เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ

2) การปฏิบัติตามนโยบาย มาตรฐานความปลอดภัยและข้อกำหนดทางเทคนิค เพื่อให้ระบบเป็นตามนโยบายและมาตรฐานความมั่นคงปลอดภัยตามที่องค์กรกำหนดไว้

3) การตรวจประเมินระบบสารสนเทศ เพื่อตรวจประเมินระบบสารสนเทศให้ได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทำงานน้อยที่สุด

การบริหารความเสี่ยงของระบบสารสนเทศ

คำว่าความเสี่ยง (risk) นั้นมีความหมายที่หลากหลาย มีการตีความแตกต่างกันไปหลายอย่าง ตามแต่ความคิด 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

1. ความเสี่ยงด้านระบบสารสนเทศ

จากการศึกษา และการตรวจสอบหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการบริหารจัดการและการควบคุมความเสี่ยงด้านระบบสารสนเทศ พอสรุปได้ว่าความเสี่ยงด้านระบบสารสนเทศสามารถแบ่งออกเป็น 4 ประเภทหลัก ดังนี้

1.1 ความเสี่ยงด้านการเข้าถึงระบบสารสนเทศ (access risk) เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานที่รับผิดชอบไม่ได้มีวิธีการจัดการ และควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปใช้ก่อให้เกิดความเสียหายได้ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูล และระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ

ได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การไม่ได้มีการกำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การไม่ได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

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

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

1.4 ความเสี่ยงด้านโครงสร้างหน่วยงานและการบริหารจัดการ (infrastructure risk) เป็นความเสี่ยงเกี่ยวกับการที่หน่วยงานเทคโนโลยีสารสนเทศมิได้มีการจัดโครงสร้างและการบริหารจัดการที่ดีเพียงพอ ไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดีรวมทั้งไม่ได้จัดให้มีระบบคอมพิวเตอร์และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการปฏิบัติงาน โดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการที่ไม่ได้จัดให้มีนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่าง ๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการที่ไม่ได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการ

ดำเนินงานและการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

2. กระบวนการบริหารความเสี่ยง (risk management process)

เนื่องจากความสี่ยงเป็นองค์ประกอบสำคัญที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ดังนั้นการบริหารความเสี่ยงจึงเป็นเรื่องที่มีความสำคัญ และจำเป็นอย่างยิ่งเพราะจะช่วยให้การดำเนินการตามภารกิจเป็นไปได้อย่างน่าเชื่อถือ สามารถหลีกเลี่ยงโอกาสที่จะเกิดความเสียหาย หรือความสูญเสียที่จะเกิดขึ้น 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

2.1 การกำหนดวัตถุประสงค์ (objective setting) การกำหนดวัตถุประสงค์ เป็นขั้นตอนแรกที่มีความสำคัญโดยต้องมีการออกเป็นนโยบายว่าองค์กรจะทำการบริหารความเสี่ยงเพื่ออะไร ใครรับผิดชอบ มีข้อดีข้อเสียอย่างไรในการทำหรือวัตถุประสงค์ในการทำของเราว่าเราทำเพื่ออะไร หลัก ๆ ก็คือการมีการร่างนโยบาย (policy statement) ออกมาก่อน ซึ่งก็คือ ระดับผู้บริหารที่เป็นคนวางนโยบายว่าเราคิดจะบริหารความเสี่ยงของระบบสารสนเทศ และมีเรื่องสำคัญอะไรบ้างที่ต้องกำหนดไว้ในนโยบาย 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 ความสมเหตุสมผลและต้องมีกรอบเวลาที่แน่นอน

2.2 การระบุความเสี่ยง (risk identification) เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติร่วมกันค้นหาว่ามีความเสี่ยง และปัจจัยเสี่ยงใดบ้างที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร โดยปกติการระบุความ

เสี่ยงจะดูจากเหตุการณ์หรือสิ่งที่เคยเกิดขึ้นมาแล้วในอดีตกับองค์กร หรือองค์กรอื่นใด หรืออาจเป็นสิ่งที่มีความเป็นไปได้ว่าจะเกิดขึ้นแม้ไม่เคยเกิดขึ้นมาก่อนก็ได้ กระบวนการระบุความเสี่ยงอาจใช้วิธีการต่าง ๆ เช่น การระดมสมอง การออกแบบสอบถาม การประชุมเชิงปฏิบัติการด้านการประเมินความเสี่ยง หรือการวิเคราะห์สถานการณ์ เป็นต้น ในการวิเคราะห์เพื่อระบุความเสี่ยงต่าง ๆ ควรดูทั้งปัจจัยภายใน และปัจจัยภายนอกเป็นส่วนประกอบ ซึ่งอาจพิจารณาจากปัจจัยเสี่ยงในหลายด้าน เช่น

2.2.1 ความเสี่ยงที่เกี่ยวข้องในระดับด้านกลยุทธ์ (strategic risk) คือความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนดำเนินงานและการนำไปปฏิบัติ ที่ไม่เหมาะสมหรือไม่สอดคล้องกับปัจจัยภายในและสภาพแวดล้อมภายนอก อันส่งผลกระทบต่อการทำงานขององค์กรดังนั้น ผู้บริหารระดับสูงต้องวางแผนกลยุทธ์และแผนดำเนินงานด้านระบบสารสนเทศอย่าง รอบคอบส่งเสริมการบริหารตามหลักธรรมาภิบาล พร้อมทั้งจัดให้มีโครงสร้างพื้นฐานภายในที่เหมาะสมสำหรับการนำไปปฏิบัติ เช่น การจัดองค์กร บุคลากร งบประมาณ ระบบการติดตาม และควบคุมการปฏิบัติงาน เป็นต้น

2.2.2 ความเสี่ยงที่เกี่ยวข้องในระดับปฏิบัติการ (operational risk) คือ ความเสี่ยงที่จะเกิดความเสียหายอันเนื่องมาจากการขาดการกำกับดูแลกิจการที่ดีหรือขาดธรรมาภิบาลในองค์กร และการขาดการควบคุมที่ดี โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน บุคคลระบบงาน หรือเหตุการณ์ภายนอก และส่งผลกระทบต่อองค์กร เช่น กระบวนการ เทคโนโลยี และบุคลากรในองค์กร เป็นต้น

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

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

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

2.3 การประเมินความเสี่ยง (risk assessment) หลังจากระบุความเสี่ยงได้แล้วขั้นต่อไปคือขั้นตอนการประเมินความเสี่ยง ซึ่งต้องทำให้ครบทุกปัจจัยเสี่ยงที่ได้ระบุไว้ ขั้นตอนนี้ มีอยู่ 4 ส่วน ได้แก่การอธิบายความเสี่ยง การประเมินระดับความเสี่ยง การวิเคราะห์ความเสี่ยง และการจัดลำดับความเสี่ยง กล่าวคือ

2.3.1 การอธิบายความเสี่ยง (risk description) หลังจากทราบว่าความเสี่ยงคืออะไรแล้ว ก็จะเป็นขั้นตอนการอธิบายว่าทุก ๆ ความเสี่ยงและปัจจัยเสี่ยงที่พบนั้นมีรายละเอียดและลักษณะอย่างไร ตัวอย่าง เช่น ชื่อความเสี่ยง ปัจจัยของความเสี่ยง ผู้รับผิดชอบ ผู้ที่ได้รับผลกระทบการบำบัด และการควบคุม เป็นต้น

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

1) พิจารณาโอกาส หรือความถี่ในการเกิดเหตุการณ์ต่าง ๆ (likelihood) เป็นการประเมินระดับโอกาสที่จะเกิดความเสี่ยง โดยสามารถพิจารณาได้ในรูปแบบของความถี่ (frequency) หรือโอกาสที่จะเกิดความเสี่ยง ตัวอย่างเกณฑ์การประเมินระดับโอกาสที่จะเกิดความเสี่ยงเชิงปริมาณ และเชิงคุณภาพ

2) พิจารณาความรุนแรงหรือความเสียหาย จากผลกระทบของความเสี่ยง (impact) เป็นการประเมินผลกระทบของความเสี่ยง ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงินที่อาจเกิดขึ้น เช่น ผลกระทบด้านการเงินซึ่งเป็นผลกระทบหรือความเสียหายที่เกิดจากความเสี่ยง และสามารถประเมินค่าเป็นตัวเงินได้ ผลกระทบด้านชื่อเสียงขององค์กรไม่ว่าจะเป็นผลจากการดำเนินงานทั้งทางตรงและทางอ้อม ที่ส่งผลต่อภาพพจน์และความเชื่อถือขององค์กร เป็นต้น

2.3.3 การวิเคราะห์ความเสี่ยง เมื่อทุกหน่วยงานที่รับผิดชอบ พิจารณาโอกาสและผลกระทบ ของแต่ละปัจจัยเสี่ยงแล้ว ต้องนำผลที่ได้มาพิจารณาความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยง เพื่อใช้ในการจัดทำแผนผังประเมินความเสี่ยง (risk assessment matrix) เพื่อหาระดับความเสี่ยง (degree of risk) สำหรับค่าความเสี่ยง (level of risk) สามารถคำนวณได้ตามสูตรต่อไปนี้

ค่าความเสี่ยง = ระดับโอกาสที่จะเกิดความเสี่ยง x ระดับผลกระทบจากความเสี่ยง

จำนวนของระดับความเสี่ยงไม่มีข้อกำหนดแน่นอน อาจจะแบ่งออกเป็น 4 ระดับหรือ 3 ระดับก็ได้ ขึ้นอยู่กับการจัดกลุ่มความเสี่ยงตามที่องค์กรเห็นสมควร

การจัดลำดับความเสี่ยง เมื่อได้ค่าความเสี่ยงแล้ว จะนำมาจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร และหน่วยงาน เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่มีนัยสำคัญให้เหมาะสม โดยพิจารณาจากระดับของความเสี่ยงเรียงตามลำดับจากระดับ สูงมาก สูง ปานกลาง ต่ำ โดยเลือกความเสี่ยงที่มีระดับสูงมาก และหรือสูง มาจัดทำแผนการบริหารจัดการความเสี่ยงในขั้นตอนต่อไป

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

1) ค่าใช้จ่าย ประโยชน์และความคุ้มทุนที่จะได้รับจากการแก้ไขบำบัดความเสี่ยง

2) ข้อกำ หนดด้านกฎหมายและกฎระเบียบขององค์กร

3) ปัจจัยด้านสิ่งแวดล้อม

4) ประเด็นสาระสำคัญในมุมมองของผู้มีส่วนได้เสีย ฯลฯ

2.3.4 การกำหนดเกณฑ์ในการยอมรับความเสี่ยง จากแผนผังประเมินความเสี่ยงขั้นตอนต่อไปคือ นำรายการความเสี่ยงของแต่ละระดับความเสี่ยงที่ได้จัดเรียงลำดับไว้ (risk ranking) มาวิเคราะห์เปรียบเทียบกับเกณฑ์ในการยอมรับความเสี่ยง

2.4 การจัดการความเสี่ยง (risk treatment) เป็นการหากลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยงว่าสามารถช่วยควบคุมความเสี่ยง หรือปัจจัยเสี่ยงได้เพียงพอหรือไม่ หรือเกิดประสิทธิผลตามวัตถุประสงค์ของการควบคุมมากน้อยเพียงใดเพื่อให้สามารถมั่นใจได้ว่าจะสามารถควบคุมความเสี่ยงที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กรได้อย่างมีประสิทธิภาพ ซึ่งวิธีการจัดการความเสี่ยงสามารถพิจารณาได้จาก 4 ทางเลือกหลักคือ

2.4.1 การยอมรับความเสี่ยง (risk acceptance) หมายถึง การรับความเสี่ยงไว้เองโดยไม่กระทำใด ๆ เพิ่มเติม กรณีนี้ใช้กับความเสี่ยงที่มีน้อยความน่าจะเกิดน้อย หรือเห็นว่ามีต้นทุนในการบริหารความเสี่ยงสูง โดยขออนุมัติหลักการในการรับความเสี่ยงไว้เอง

2.4.2 การลด (risk reduction) หรือควบคุมความเสี่ยง (risk control) หมายถึงการลดโอกาสความน่าจะเกิด หรือลดความเสียหาย โดยการจัดระบบการควบคุม เพื่อป้องกัน การปรับปรุงแก้ไขกระบวนการ รวมทั้ง การกำหนดแผนสำรองในเหตุฉุกเฉิน

2.4.3 การหลีกเลี่ยงความเสี่ยง (risk avoidance) หมายถึง การหยุด หรือการเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น งดทำขั้นตอนที่ไม่จำเป็นและอาจจะนำมาซึ่งความเสี่ยงปรับเปลี่ยนรูปแบบการทำงาน หรือลดขอบเขตการดำเนินการ เป็นต้น

2.4.4 การกระจายความเสี่ยง (risk sharing) หรือการโอนความเสี่ยง (risk spreading) หมายถึงการลดโอกาสความน่าจะเกิด หรือลดความเสียหายโดยการแบ่งโอน การหาผู้รับผิดชอบในความเสี่ยงโดยการจ้างบุคคลภายนอกเป็นผู้ดำเนินการแทน หรือการจัดทำประกันภัยเป็นต้น

ทั้งนี้ควรคำนึงถึงต้นทุนและผลประโยชน์ที่จะได้รับภายใต้ทางเลือกต่าง ๆ และเมื่อได้ทางเลือกที่เหมาะสมในการบริหารความเสี่ยงแล้ว ทีมงานบริหารความเสี่ยงต้องกำหนดแผนกลยุทธ์การบริหารความเสี่ยงที่แต่ละหน่วยงานต้องร่วมกันปฏิบัติ ซึ่งการนำแผนกลยุทธ์ไปสู่การปฏิบัตินั้นจะต้องอาศัยความเข้าใจและความร่วมมือจากทุกฝ่ายที่เกี่ยวข้อง

2.5 กิจกรรมการบริหารความเสี่ยง (control activities) การนำกลยุทธ์ มาตรการหรือ แผนงานมาใช้ปฏิบัติงาน เพื่อลดโอกาสที่จะเกิดความเสี่ยง หรือลดความเสียหายจากผลกระทบในการดำเนินงานต่าง ๆ ที่ไม่มีกิจกรรมควบคุม หรือมีไม่เพียงพอ การควบคุม หมายถึง นโยบายแนวทาง หรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยงให้บรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท ดังนี้

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

2.5.2 การควบคุมเพื่อให้ตรวจพบ (detective control) การควบคุมเพื่อให้ตรวจพบเป็นการควบคุมที่กำหนดไว้เพื่อให้สามารถค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว เช่นการสอบทาน การวิเคราะห์ การยืนยันยอด การตรวจนับ การรายงานข้อบกพร่อง ฯลฯ

2.5.3 การควบคุมโดยการชี้แนะ (directive control) การควบคุมโดยการชี้แนะที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การให้รางวัลแก่ผู้มีผลงานดีเป็นต้น

2.5.4 การควบคุมเพื่อการแก้ไข (corrective control) การควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง

2.6 ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (information and communication) การจัดทำรายงานผลการติดตามการดำเนินการตามแผนการบริหารความเสี่ยงที่ได้ดำเนินการตามลำดับให้ฝ่ายบริหารรับทราบ และสามารถดำเนินการแก้ไขปัญหาที่มีได้ทันท่วงที

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

ทั้งนี้ การบริหารความเสี่ยงเป็นงานที่ต้องทำอย่างต่อเนื่อง ความเสี่ยงแต่ละประเภทเปลี่ยนไปตามความเปลี่ยนแปลงของโลก การบริหารความเสี่ยงจึงต้องได้รับความประเมินผล และปรับปรุงให้สอดคล้องกับสถานการณ์ปัจจุบัน การประเมินผลจึงไม่ใช่ขั้นตอนสุดท้ายของการบริหารความเสี่ยง แต่เป็นขั้นตอนที่นำไปสู่ระบบการบริหารความเสี่ยง ที่มีความต่อเนื่องและทันต่อเหตุการณ์

แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

1.1. หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ในมาตรา 5 *"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"* และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กร ซึ่งจะได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัย เช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีสำคัญอย่างยิ่งต่อองค์กร ที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมาย และมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้อนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

1.2. วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพิมพ์ตำรวจ ฉบับนี้มีวัตถุประสงค์เพื่อ

1) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของโรงพิมพ์ตำรวจ ที่สอดคล้องกับบริบทองค์กร และกฎหมายที่เกี่ยวข้อง

2) จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศ เทคโนโลยีและการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

3) เพื่อให้มั่นใจได้ว่าข้อมูลและระบบสารสนเทศของโรงพิมพ์ตำรวจ มีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจจะเกิดขึ้นในระบบสารสนเทศโรงพิมพ์ตำรวจ และใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ

1.3 องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพิมพ์ตำรวจ โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ มาตรฐานสากล ISO/IEC 27001 และสำนักงานตำรวจแห่งชาติ โดยแนวทางปฏิบัตินี้ ประกอบด้วย วัตถุประสงค์ ผู้เกี่ยวข้อง และรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ

1.4 บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของโรงพิมพ์ตำรวจ บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุนและติดตามการประยุกต์ใช้ โดยผู้อำนวยการโรงพิมพ์ตำรวจ

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูง (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

1.5. การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพิมพ์ตำรวจ ฉบับนี้ จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ 1 ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายในโรงพิมพ์ตำรวจ เผยแพร่ผ่านเว็บไซต์ของโรงพิมพ์ตำรวจ เพื่อให้บุคลากรโรงพิมพ์ตำรวจ และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

คำนิยาม

1. คำเรียกแทนหน่วยงานในเอกสารฉบับนี้ เช่น สำนักงาน,ฝ่าย หมายถึง โรงพิมพ์ตำรวจ

2. ผู้บริหารระดับสูง หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารราชการของโรงพิมพ์ตำรวจ

3. การรักษาความมั่นคงปลอดภัย หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับด้านสารสนเทศขอโรงพิมพ์ตำรวจ

4. **ผู้ใช้งาน** หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร

ผู้รับผิดชอบ ผู้ใช้งานทั่วไป อันได้แก่

4.1. ผู้บริหารสูงสุด หมายความว่า ผู้อำนวยนการโรงพิมพ์ตำรวจโรงพิมพ์ตำรวจ

4.2. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Office : CIO) หมายความว่า ผู้บริหารโรงพิมพ์ตำรวจ ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสาร

4.3 ผู้ดูแลระบบ หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์

4.4 ผู้พัฒนาระบบ หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนาระบบแอพพลิเคชั่น

4.5 เจ้าหน้าที่ หมายความว่า พนักงาน ลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการขององค์กร

4.6 บุคคลภายนอก หมายความว่า บุคคลที่โรงพิมพ์ตำรวจอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจได้ชั่วคราว เพื่อประโยชน์ในการดำเนินงานของโรงพิมพ์ตำรวจ เช่น พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับโรงพิมพ์ตำรวจ หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง หรือนิสิตนักศึกษาฝึกงาน

5. สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

6. สินทรัพย์ (Asset) หรือ ทรัพย์สินสารสนเทศ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่

6.1.ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

6.2. ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

6.3. ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

7. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

8. ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ (Information Security) หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) ห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

9. เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันนำไปสู่ปัญหาด้านความมั่นคงปลอดภัย

10. สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

หมวดที่ 1 นโยบายการเข้าถึง และการควบคุมการใช้งานสารสนเทศ

วัตถุประสงค์

1) เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของโรงพิมพ์ตำรวจ

2) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับโรงพิมพ์ตำรวจ ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

1) หมวดนโยบายแผนและสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3) ผู้ใช้งาน

แนวปฏิบัติ

ส่วนที่ 1 การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

เพื่อให้การเข้าถึงและการควบคุมการใช้งานสารสนเทศมีความมั่นคงปลอดภัย กำหนดให้ผู้ดูแลระบบมีแนวปฏิบัติดังนี้

1. การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลข้อมูล

1.1 ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น

1.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

1.2.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

1.2.1.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

1.2.1.2 กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

1.2.1.3 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

1.2.1.4 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้ดูแลระบบ

2. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

โรงพิมพ์ตำรวจ ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

2.1 จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

- ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ (ระบุข้อมูลที่เป็นการให้บริการของหน่วยงาน เช่น บริการรับชำระภาษี บริการขึ้นทะเบียนผู้ประกอบการ เป็นต้น)

2.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ ดังนี้

ระดับที่ 1 ข้อมูลที่มีระดับความสำคัญมากที่สุด

ระดับที่ 2 ข้อมูลที่มีระดับความสำคัญปานกลาง

ระดับที่ 3 ข้อมูลที่มีระดับความสำคัญน้อย

2.3 จัดแบ่งลำดับชั้นความลับของข้อมูลดังนี้

“ข้อมูลลับที่สุด”	หมายถึง	ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
“ข้อมูลลับมาก”	หมายถึง	ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
“ข้อมูลลับ”	หมายถึง	ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
“ข้อมูลทั่วไป”	หมายถึง	ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

2.4 การจัดแบ่งระดับชั้นการเข้าถึง

ระดับที่ 1 ระดับชั้นสำหรับผู้บริหาร

ระดับที่ 2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

ระดับที่ 3 ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

2.5 การกำหนดเวลาในการเข้าถึงข้อมูล

การเข้าถึงข้อมูลของโรงพิมพ์ตำรวจ กำหนดไว้เป็นช่วงเวลาเข้าถึงได้ดังนี้

ลำดับ	เวลาที่เข้าถึงได้	ข้อมูล / ช่องทางการเข้าถึงข้อมูล
1	ในเวลาราชการ วันจันทร์ ถึง วันศุกร์ เวลา 08.30 – 16.30 น.	ระบบใบลา ● ใส่ระบบสารสนเทศองค์กรที่ให้บริการในช่วงเวลาดังกล่าว
2	นอกเวลาราชการ วันจันทร์ ถึง วันศุกร์ เวลา 16.30-20.30 น.	ใส่ระบบสารสนเทศองค์กรที่ให้บริการในช่วงเวลาดังกล่าว
3	วันหยุดราชการ/วันหยุดนักขัตฤกษ์ วันหยุดราชการ/วันหยุดนักขัตฤกษ์ เวลา 08.30 – 16.30 น.	ระบบใบลา ใส่ระบบสารสนเทศองค์กรที่ให้บริการในช่วงเวลาดังกล่าว
4	ทุกวัน 24 ชั่วโมง	เว็บไซต์ ใส่ระบบสารสนเทศองค์กรที่ให้บริการในช่วงเวลาดังกล่าว

ส่วนที่ 2 การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ

(Business Requirement for access control)

เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศขององค์กร และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย การใช้งานตามภารกิจเอควบคุมการเข้าถึงสารสนเทศมีแนวปฏิบัติ ดังนี้

2.1 การควบคุมการเข้าถึงสารสนเทศ

2.1.1ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

2.1.2 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

2.2 จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ และภารกิจ ดังนี้

2.2.1 Executive คือ กลุ่มผู้บริหาร ผู้อำนวยการ, รองผู้อำนวยการ. หัวหน้าฝ่าย

2.2.2 Administrator คือ กลุ่มของผู้ดูแลระบบ

2.2.3 Officer คือ กลุ่มผู้ใช้งานทั่วไปเป็นบุคลากรของโรงพิมพ์ตำรวจ

2.2.4 Consultant คือ กลุ่มที่ปรึกษาหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับโรงพิมพ์ตำรวจ

2.2.5 Guest คือ ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว

ส่วนที่ 3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อบริหารจัดการการเข้าถึงระบบสารสนเทศขององค์กร และมั่นใจได้ว่าเฉพาะผู้ที่ได้รับสิทธิการเข้าถึงระบบสารสนเทศตามที่กำหนดเท่านั้นสามารถเข้าใช้งานระบบสารสนเทศได้ โดยมีแนวปฏิบัติในการบริหารการเข้าถึงระบบสารสนเทศของผู้ใช้งาน ดังนี้

3.1 สร้างความรู้ ความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้งาน

3.1.1 โรงพิมพ์ตำรวจ จัดให้มีการอบรมเพื่อสร้างความรู้ และความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ และรู้เท่าทันต่อภัยคุกคาม และผลกระทบที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศอย่างไม่ระมัดระวัง โดยจัดให้มีการอบรมผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง

3.1.2 กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิเพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเมื่อได้รับสิทธิการเข้าใช้งานระบบสารสนเทศของหน่วยงาน

3.2 การลงทะเบียนผู้ใช้งาน (User Registration)

3.2.1 ผู้ดูแลระบบ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

3.2.2 ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

3.2.2 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามรายละเอียดสิทธิในแต่ละภารกิจในส่วนที่ 2

3.2.3 ผู้ดูแลระบบต้องชี้แจง และแจ้งผู้ใช้งาน เป็นลายลักษณ์อักษร เพื่อให้ผู้ใช้งานทราบถึงสิทธิ หน้าที่รับผิดชอบ และมาตรการรด้านความมั่นคงปลอดภัย ในการเข้าถึงระบบสารสนเทศ

3.2.4 กำหนดให้มีการยกเลิก เพิกถอนการอนุญาตเข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนผู้ใช้งาน เมื่อได้รับแจ้งจากต้นสังกัด หรือเมื่อมีการลาออก เปลี่ยนแปลงตำแหน่ง โยกย้าย หรือสิ้นสุดการจ้างเป็นต้น

3.3 การบริหารจัดการสิทธิผู้ใช้งาน (User Management)

3.3.1 กำหนดระดับสิทธิการเข้าถึงระบบสารสนเทศตามหน้าที่รับผิดชอบ ความจำเป็นในการใช้งาน และทบทวนสิทธิสม่ำเสมอ

3.3.2 ผู้ดูแลระบบต้องปรับปรุงสิทธิการเข้าถึงข้อมูล และระบบสารสนเทศตามหน้าที่รับผิดชอบ และจัดเก็บข้อมูลการมอบสิทธิให้แก่ผู้ใช้งานไว้เป็นฐานข้อมูล

3.3.3 ในกรณีที่ต้องให้สิทธิพิเศษนอกเหนือจากภาระงานที่กำหนด จะต้องได้รับการอนุมัติเห็นชอบจากผู้บริหาร จัดทำคำร้องเป็นลายลักษณ์อักษร โดยการให้สิทธิพิเศษดังกล่าวจะต้องกำหนดช่วงเวลาที่ชัดเจน และเมื่อพ้นกำหนดการให้สิทธิพิเศษ จะต้องระงับการช้งานทันที

3.4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

3.4.1 ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราวในครั้งแรกให้แก่ผู้ใช้งาน ส่งมอบให้ผู้ใช้งานเป็นเอกสารปิดผนึกที่เป็นความลับ เมื่อผู้ใช้งานได้รับจะต้องเปลี่ยนรหัสผ่านใหม่ทันที ภายใน 7 วัน (อาจใช้วิธีส่งให้ทางจดหมายอิเล็กทรอนิกส์ หรือวิธีอื่น ๆ ตามแนวทางของแต่ละองค์กร)

3.4.2 การตั้งรหัสผ่านใหม่จะต้องตั้งรหัสให้มีความยากในการคาดเดา โดยรหัสผ่านต้องประกอบด้วย ตัวอักษรเล็ก ตัวอักษรใหญ่ สัญลักษณ์พิเศษ 7 หลัก (digits)

3.4.3 กำหนดให้การเข้ารหัสผิดได้ไม่เกิน 3 ครั้ง กรณีบัญชีผู้ใช้งานไม่สามารถเข้าใช้งานได้เนื่องจากเข้ารหัสผิดเกินจำนวนครั้งที่กำหนดให้ติดต่อผู้ดูแลระบบ และแจ้งความจำนงค์ขอตั้งรหัสผ่านใหม่

3.4.4 กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ทุก ๆ 180 วัน

3.5 การทบทวนสิทธิการเขาถึงของผู้ใช้งาน (Review of user access right)

ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตจากผู้ที่ไม่สิทธิการเข้าถึง โดยมีแนวปฏิบัติ ดังนี้

3.5.1 พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน พร้อมรายละเอียดสิทธิที่ได้รับของแต่ละบุคคล

3.5.2 จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

3.5.3 ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับผู้ดูแลระบบ

3.5.4 ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกต้องดำเนินการภายใน 3 วัน หรือ เมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน 7 วัน

ส่วนที่ 4 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

4.1 การใช้งานรหัสผ่าน (Password Use)

4.1.1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน(Password)

4.1.2 การกำหนดรหัสผ่าน (Password) ที่เดาสุ่มได้ยาก ซึ่งประกอบด้วย

- กำหนดให้ความยาวไม่น้อยกว่า 8 ตัวอักษร
- ใช้อักขระพิเศษประกอบ เช่น :;<> เป็นต้น
- ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef”, “aaaaa” เป็นต้น
- การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับของเดิมครั้งสุดท้าย
- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องผู้ใช้งาน เช่น ชื่อ, นามสกุล หรือวันเกิด เป็นต้น
- ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม
- ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

4.1.3 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

4.1.4 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

4.1.5 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน 180 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

4.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

การป้องกันอุปกรณ์เมื่อไม่มีผู้ใช้งาน มีแนวปฏิบัติเพื่อป้องกันผู้ไม่มีสิทธิเข้าถึงอุปกรณ์ขณะที่ไม่มีผู้ดูแลได้ดังนี้

4.2.1 มีการกำหนดมาตรการป้องกันทรัพย์สินขององค์กรและควบคุมไม่ให้มีการทิ้ง หรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัยให้ ครอบคลุมเรื่องต่าง ๆ คือ การจัดการบริเวณล้อมรอบ, การควบคุมการเข้าออก, การจัดบริเวณการเข้าถึงกรณีมีการส่งผลิตภัณฑ์โดยบุคคลภายนอก, การจัดวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการท างานในสถานที่ที่มีความ ปลอดภัย

4.2.2 การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ เจ้าของข้อมูลต้องปฏิบัติตาม แนวทางการทำลาย ดังนี้

ลำดับ	ประเภทสื่อบันทึกข้อมูล	แนวทางการทำลาย
1	แฟลชไดรฟ์ (Flash Drive) ฮาร์ดิสก์ (Hard disk) เอ็กเทอนอลฮาร์ดดิสก์ (External Hard disk)	1. ทำลายข้อมูลตามแนวทางของ DOD 5220.22-M ของกระทรวงกลาโมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลาย ๆ รอบ 2. ทุบทำลาย หรือบดให้อุปกรณ์เสียหายไม่สามารถนำไปใช้งานได้
2	แผ่นซีดี / ดีวีดี (CD/DVD)	ใช้วิธีการตัด เผา ทำให้สิ้นสภาพการใช้งาน
3	เทป	ใช้วิธีทุบ ทำลายให้เสียหายสิ้นสภาพการใช้งาน
4	กระดาษ	ตัดด้วยเครื่องทำลายเอกสาร

4.2.3 ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบ การรักษาความลับทางราชการ พ.ศ. 2544 โดยการรับ-ส่งข้อมูลสำคัญ หรือ ข้อมูลซึ่งเป็นความลับให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล SSL หรือ VPN

4.3 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

องค์กรได้กำหนดแนวปฏิบัติเพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ รวมถึงกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน โดยมีแนวปฏิบัติดังนี้

4.3.1 ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

4.3.2 ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าขณะที่ไม่ได้ใช้งาน เช่นภายใน 15 นาที ให้เครื่องล๊อคหน้าจอ และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิด หน้าจอได้

4.3.3 ผู้ใช้งานต้องล็อกใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

4.3.4 กรณีข้อมูลสำคัญที่บันทึกไว้ใน กระดาษ สื่อบันทึกข้อมูล แฟลชไดร์ฟ หรือ ฮาร์ดดิสก์ เมื่อไม่ใช้งานต้องจัดเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

4.3.5 ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

4.4 การใช้งานระบบสารสนเทศอย่างปลอดภัย

เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัย และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศขององค์กร กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งานดังนี้

4.4.1 การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

4.4.2 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงานและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อคก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

4.4.3 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นขององค์กร หรือเป็นบุคคลภายนอก

4.4.4 ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

4.4.5 ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่องค์กรต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับองค์กร ซึ่งองค์กรอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

4.4.6 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์(BitTorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

4.4.7 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น

4.4.8 ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจขององค์กร

4.4.9 ห้ามใช้ระบบสารสนเทศขององค์กรเพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจขององค์กร

4.4.10 ห้ามใช้ระบบสารสนเทศขององค์กรเพื่อประโยชน์ทางการค้า

4.4.11 ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายขององค์กรโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตามห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ส่วนที่ 5 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการเครือข่ายโดยไม่ได้รับอนุญาต จึงได้กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบดังนี้

5.1 การใช้งานบริการเครือข่าย

5.1.1 กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

5.1.2 กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

5.1.3 กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย(Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ 1 ครั้ง

5.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร

5.2.1 เมื่อผู้ใช้งานที่อยู่ภายนอกองค์กร เมื่อต้องเข้าใช้งานระบบสารสนเทศต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

5.2.2 มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงด้วยการใช้รหัสผ่าน (Password)

5.2.3 การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ตต้องได้รับอนุญาตจาก ผู้บริหารด้านเทคโนโลยีสารสนเทศ และต้องมีการเข้ารหัสที่เป็นมาตรฐานสากลเพื่อความมั่นคงปลอดภัยด้วย VPN

5.3 การระบุอุปกรณ์บนเครือข่าย

5.3.1 กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย IP Address และ MAC Address

5.3.2 จัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่ใช้เชื่อมกับระบบเครือข่ายขององค์กร โดยมีรายละเอียดของอุปกรณ์ประกอบด้วย เครื่องคอมพิวเตอร์, IP Address, MAC Address, สถานที่ติดตั้ง, ผู้ใช้งาน เป็นต้น

5.3.3 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับอนุญาตเท่านั้น

5.3.4 ต้องใช้ไฟร์วอลล์ (Firewall) ที่สามารถกำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายของหน่วยงานได้

5.3.5 จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

5.3.6 แผนผังเครือข่าย เป็นเอกสารในระดับลับมากจะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่ และทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ 1 ครั้ง

5.4 การป้องกันพอร์ตที่ใช้สำหรับการตรจสอบและปรับแต่งระบบ

5.4.1 การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่ายต้องมีการตั้งรหัสผ่านและให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

5.4.2 มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย และเปิดใช้เฉพาะอุปกรณ์และเวลาที่จ าเป็นเท่านั้น

5.4.3 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น

5.4.4 ติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

5.5 การแบ่งแยกเครือข่าย

กำหนดให้มีการแบ่งแยกเครือข่ายตามประเภทการใช้งานเพื่อความปลอดภัย ดังนี้

Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

5.5.2 Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

5.6 การควบคุมการเชื่อมต่อทางเครือข่าย

เพื่อควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้มีความมั่นคงปลอดภัย ได้กำหนดแนวปฏิบัติ ดังนี้

5.6.1 จำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

5.6.2 ระบบเครือข่ายต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall, IDS/IPS)

5.6.3 การเข้าสู่ระบบเครือข่ายของหน่วยงานต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยที่กำหนดไว้เท่านั้น

5.6.4 ต้องระบุอุปกรณ์และเครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

5.6.5 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

5.6.6 ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนี้

1) จำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

2) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

3) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

4) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

5) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

6) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ 1 ครั้ง หากมีการแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

7) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

8) IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

9) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

5.7 การควบคุมการจัดเส้นทางบนเครือข่าย

การจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือ สารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ซึ่งมีแนวปฏิบัติ ในการจัดเส้นทางบนเครือข่าย ดังนี้

5.7.1 ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

5.7.2 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

5.7.3 กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก

5.7.4 ต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง(Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

ส่วนที่ 6 การควบคุมการเข้าถึงระบบปฏิบัติการ

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการขององค์กรโดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบ ดังนี้

6.1 ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

6.1.1 กำหนดให้ระบบไม่ให้แสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

6.1.2 กำหนดให้ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

6.1.3 จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน โดยผู้ใช้งานจะต้องป้อนรหัสผ่านภายในเวลา 30 นาทีเพื่อเข้าใช้งานระบบ

6.1.4 จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

6.2 การระบุและยืนยันตัวตนของผู้ใช้งาน

6.2.1 ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

6.2.2 หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นทางด้านเทคนิค หรือสอดคล้องกับการปฏิบัติงาน โดยจะต้องขออนุญาตใช้จาก ผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย และกำหนดกรอบเวลาการใช้งานที่ชัดเจน และยุติการใช้งานทันทีเมื่อพบความผิดปกติหรือหมดช่วงเวลาที่ขออนุญาตไว้

6.3 การบริหารจัดการรหัสผ่าน

กำหนดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

6.3.1 มีระบบการตรวจสอบการกำหนดรหัสผ่าน ซึ่งประกอบด้วยตัวอักขระ ตัวเลข และตัวอักขระพิเศษ หรือเทคนิคอื่นใดในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) และมีคุณภาพ

6.3.2 เมื่อดำเนินการติดตั้งระบบแล้วให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของรายชื่อผู้ใช้งานทั้งหมดที่ถูกกำหนดไว้เริ่มต้นซึ่งมาพร้อมกับการติดตั้งระบบโดยทันที

6.4 การใช้งานโปรแกรมอรรถประโยชน์

กำหนดให้มีการจำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่กำหนด โดยมีแนวปฏิบัติ ดังนี้

6.4.1 การใช้งานโปรแกรมอรรถประโยชน์ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

6.4.2 โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

6.4.3 จัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน และเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

6.4.4 จำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์เท่านั้น

6.4.5 กำหนดให้ผู้ดูแลระบบมีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

6.5 การกำหนดระยะเวลายุติการใช้งานระบบสารสนเทศ

6.5.1 กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 30 นาที

6.5.2 ระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นระยะเวลา 30 นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

6.6 การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ

เพื่อป้องกันการเข้าถึงระบบสารสนเทศ และโปรแกรมที่มีความเสี่ยงสูง หรือมีความสำคัญสูง กำหนดแนวปฏิบัติในการจำกัดระยะเวลาในการเชื่อมต่อเพื่อความมั่นคงปลอดภัย ดังนี้

6.6.1 กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ให้ใช้งานได้ภายใน 3 ชั่วโมงต่อการเชื่อมต่อ 1 ครั้ง และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาราชาการ วันจันทร์ ถึงวันศุกร์ เวลา 8.30 – 16.30 น. เท่านั้น

6.6.2 กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อไม่เกิน 3 ชั่วโมงต่อครั้ง

ส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศโดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบต้องดำเนินการ ดังนี้

7.1 จำกัดการเข้าถึงสารสนเทศ

ควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน โดยการเข้าใช้งาน การเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ได้กำหนดหลักเกณฑ์การจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศ ดังนี้

7.1.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงานตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศและข้อมูล

7.1.2 จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด โดยยกเลิกการเชื่อมต่อระบบเมื่อครบกำหนดเวลา

7.1.3 ผู้ให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน และต้องลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของหน่วยงาน

7.1.4 ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของ ผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

7.1.5 ผู้ดูแลระบบต้องควบคุม การเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource)

7.2 ระบบซึ่งไวต่อการรบกวน

มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ กำหนดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์ และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking) โดยกำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัยไว้

ดังนี้

7.2.1 แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น และแสดงให้เห็น ถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

7.2.2 ควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ดังนี้

1) ระบบซึ่งไวต่อการรบกวน จะต้องควบคุมการเข้าถึงอุปกรณ์ และระบบ โดยติดตั้งไว้ในในพื้นที่ปลอดภัย

2) ติดตามเฝ้าระวังการใช้งานระบบซึ่งไวต่อการรบกวน และระงับการใช้งานทันทีเมื่อพบเหตุการณ์ผิดปกติ

7.2.3 ควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับ ระบบดังกล่าวโดย

1) อุปกรณ์ที่ใช้ในการสื่อสาร หรือปฏิบัติงานจากภายนอกหน่วยงาน ต้องนำมาขึ้นทะเบียนกับผู้ดูแลระบบ

2) การเข้าถึงระบบโดยการปฏิบัติงานจากภายนอกต้องขออนุมัติการใช้งานจากผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย เพื่อเปิดสิทธิให้ปฏิบัติงานจากภายนอกได้

3) ผู้ปฏิบัติงานจากภายนอก ต้องปฏิบัติงานในที่ปลอดภัย และงดการใช้เครือข่ายสาธารณะเพื่อเข้าถึงระบบสารสนเทศขององค์กร

7.2.4 ควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนด

7.2.5 วางแผนการสำรองและทดสอบการกู้คืนระบบ ตามนโยบายการสำรองระบบสารสนเทศ

7.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

กำหนดแนวปฏิบัติและมาตรการเพื่อปกป้องระบบสารสนเทศ ซึ่งจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ โดยผู้ใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องปฏิบัติ ดังนี้

7.3.1 การป้องกันอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ครอบคลุมการใช้งาน อุปกรณ์สื่อสารประเภทพกพา ได้แก่ Smart Phone, Notebook, Laptop, Tablet หรืออุปกรณ์อื่นใดในลักษณะเดียวกันนี้ โดยกำาหนดให้มีการป้องกัน การเชื่อมต่อของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เข้ากับเครือข่ายของ หน่วยงานโดยไม่ได้รับอนุญาต

7.3.2 กำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ซึ่งจะต้องแสดงตัวตนเมื่อเข้าใช้งาน

7.3.3 ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ของตนเอง

7.4 การปฏิบัติงานจากภายนอกหน่วยงาน

เพื่อปกป้องระบบสารสนเทศจากการปฏิบัติงานจากภายนอกหน่วยงาน กำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัย ดังนี้

7.4.1 การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่างๆ ภายในหน่วยงาน

7.4.2 การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของ ส่วนตัว ต้องได้รับอนุญาตจาก ผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

7.4.3 การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกหน่วยงานได้ ต้องมีหนังสือเป็นลายลักษณ์อักษร และมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย โดยระบุรายละเอียดการขอเปิดใช้งานระบบสารสนเทศจากภายนอกโดยมีรายละเอียดดังนี้

1) เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกหน่วยงาน

2) รายละเอียดและลักษณะของระบบงาน

3) ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก

4) รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน

5) ช่วงเวลาและระยะเวลาในการปฏิบัติงานจากภายนอกหน่วยงาน

7.4.4 ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับในระดับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

7.4.5 การเข้าสู่ระบบระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

7.4.6 ผู้ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงานโดยไม่ให้สมาชิกภายในครอบครัว หรือบุคคลอื่นใดสามารถเข้าถึงระบบได้

7.4.7 ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

7.4.8 ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกหน่วยงาน แก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

7.4.9 ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกหน่วยงานอย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

เพื่อให้การเข้าถึงระบบเครือข่ายไร้สายในหน่วยงาน มีความมั่นคงปลอดภัยกำหนดแนวทางปฏิบัติเพื่อควบคุมการเข้าถึงระบบเครือข่ายไร้สายไว้ดังนี้

8.1 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานจะต้องลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยี สารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย

8.2 ผู้ดูแลระบบต้องดำเนินการลงทะเบียนผู้ใช้งาน ดังนี้

8.2.1 ลงทะเบียน และกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายเหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

8.2.2 ต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

8.2.3 ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่ง

สัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

8.2.4 ดำเนินการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งานและกำหนดให้ซ่อน SSID (Service Set Identifier) เพื่อความปลอดภัย

8.2.5 เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถคาดเดาหรือเจาะรหัสได้โดยง่าย

8.2.6 กำหนดค่าใช้ WEP(Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจาย (Access Point) เพื่อให้ยากต่อการดักจับ เพื่อความปลอดภัย

8.2.7 เลือกใช้วิธีการควบคุ ม MAC Address (Media Access Control Address) ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Addressชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้สามารถเข้าใช้ระบบเครือข่ายไร้สายได้

8.2.8 ควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

8.2.9 กำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

8.2.10 ใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทันที

ส่วนที่ 9 การควบคุมการใช้อินเทอร์เน็ต

กำหนดแนวปฏิบัติเพื่อควบคุมการใช้งานอินเทอร์เน็ตอย่างปลอดภัยดังนี้

9.1 ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร

9.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

9.3 การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

9.4 ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็น การส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

9.5 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

9.6 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

9.7 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์จะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

9.8 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

9.9 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์ (Web Browser) และออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

9.10 ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

ส่วนที่ 10 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)

เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลให้มีความปลอดภัย กำหนดแนวปฏิบัติดังนี้

10.1 เครื่องคอมพิวเตอร์ส่วนบุคคลที่หน่วยงานอนุญาตให้ผู้ใช้ระบบสารสนเทศใช้งาน เป็นทรัพย์สินของหน่วยงาน ที่ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

10.2 โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคลหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

10.3 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น การนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกนอกหน่วยงานเพื่อการใดก็ตาม ต้องขออนุมัติผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น

10.4 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล

10.5 ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดย

10.5.1 กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เพื่อเปิดใช้เครื่อง และเก็บรักษารหัสผ่านอย่างปลอดภัย

10.5.2 เมื่อไม่ได้ใช้งานเกิน 30 นาที เครื่องควรตั้งโปรแกรม Screen Saver และต้องใช้รหัสผ่านเพื่อเข้าใช้งานอีกครั้ง และเมื่อเลิกใช้งานควรล็อกเอาท์ (Log Out) ออกจากเครื่อง

10.5.3 ต้องอัปเดต (Update) ระบบปฏิบัติการ เว็บบราวเซอร์และ โปรแกรมใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

10.5.4 ต้องไม่ถอดถอนการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ในเครื่องคอมพิวเตอร์ส่วนบุคคล

10.5.5 ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่มิได้ขึ้นทะเบียนอุปกรณ์กับผู้ดูแลระบบ มาใช้งานและเชื่อมต่อกับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับอนุญาตเป็นลายลักษณ์อักษรและนำมาขึ้นทะเบียนกับผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

ส่วนที่ 11 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

11.1 เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพร้อมใช้งาน

11.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

11.3 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เพื่อเปิดเข้าใช้งานเครื่องทุกครั้ง และควรกำหนดรหัสผ่านให้ยากต่อการคาดเดา และเก็บรักษาไว้เป็นความลับ

11.4 ตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ไม่น้อยกว่า 15 นาที เพื่อล็อกหน้าจอเมื่อไม่มีการใช้งาน และต้องใส่รหัสผ่านอีกครั้งเมื่อกลับมาใช้งาน

11.5 ต้องออกจากระบบ (Log Out) ทันทีเมื่อเลกใช้งาน

11.6 ต้องสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา ลงบนสื่อจัดเก็บที่ปลอดภัย เพื่อป้องกันการสูญหายของข้อมูล และจัดเก็บอย่างปลอดภัย หรือกำหนดรหัสการข้าสื่อบันทึกข้อมูล รวมถึงการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

11.7 การเคลื่อนย้ายคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการ

กระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือพลัดหลุดมือ เป็นต้น หลีกเลี่ยงการใส่เครื่องคอมพิวเตอร์พกพาไว้ในกระเป๋าเดินทาง เพราะอาจถูกกดทั เกิดความเสียหายได้

11.8 หลีกเลี่ยงการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดอยู่ กรณีต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

11.9 ความปลอดภัยทางด้านกายภาพ

1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

3) หลีกกเลี่ยงการวางเครื่องคอมพิวเตอร์พกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ และวางไว้หรือใช้งานในที่ที่มีแรงสั่นสะเทือนมาก

4) ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

5) หลีกเลี่ยงการใช้วัสดุ หรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนไม่วางของทับบนหน้าจอและแป้นพิมพ์ หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

6) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดด้วยความระมัดระวัง ควรเช็ดไปในแนวทางเดียวกัน ไม่ควรเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

7) ดูแลบำรุงรักษาเครื่อคอมพิวเตอร์แบบพกพาให้อยู่ในสภาพร้อมใช้งาน พักเครื่องเมื่อต้องใช้เป็นระยะเวลานานเกินไป หรือในสภาพที่มีอากาศร้อนจัด

ส่วนที่12 การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)

12.1 ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ โดยผู้ดูแลระบบ ดังนี้

12.1.1 ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

12.1.2 ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

12.1.3 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติจากผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย ก่อนดำเนินการ

12.1.4 ไม่ติดตั้งซอร์สโค้ดคอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องอมพิวเตอร์แม่ข่ายที่ให้บริการ

12.1.5 กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบสารสนเทศ

ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

12.1.6 กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการซอฟต์แวร์ระบบสารสนเทศ เป็นต้น

12.1.7 วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

12.1.8 จัดเก็บซอฟต์แวร์เวอร์ชั่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ที่ไม่ได้ใช้งานไว้อย่างปลอดภัยเพื่ออ้างอิง

12.2 ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ

12.2.1 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดeเนินการเปลี่ยนแปลงระบบปฏิบัติการ

12.2.2 วางแผนเฝ้าระวังและทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

12.3 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

12.3.1 กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

12.3.2 ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

12.3.3 กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

12.3.4 กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ก่อนมีการติดตั้ง

12.3.5 การทดสอบซอฟต์แวร์ห้ามทดสอบบนระบบ และฐานข้อมูลที่ใช้งาน เลือกสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

12.4 มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

12.4.1 ผู้ให้บริการที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

12.4.2 ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

12.4.3 กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้อง

มีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

12.4.4 การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายก่อนทุกครั้ง

12.5 มาตรการควบคุมช่องโหว่ทางเทคนิค

12.5.1 กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน บริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้

1) ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน

2) สถานที่ที่ติดตั้ง

3) เครื่องแม่ข่ายที่ติดตั้ง

4) ผู้ผลิตซอฟต์แวร์

5) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

12.5.2 กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่าง เหมาะสมโดยทันที

12.5.3 กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบ

12.5.4 กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบ ดำเนินการ ดังนี้

1) มีการเฝ้าระวังและติดตามประเมินความเสี่ยงสำหรับช่องโหว่ของระบบ สารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไข ช่องโหว่ตามความเหมาะสม

2) ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน

3) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

12.5.5 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

12.5.6 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

1) ข้อมูลชื่อบัญชีผู้ใช้งาน

2) ข้อมูลวันเวลาที่เข้าถึงระบบ

3) ข้อมูลวันเวลาที่ออกจากระบบ

4) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

5) ข้อมูลการล็อกอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ

6) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

7) ข้อมูลการเปลี่ยนคอนฟิกกูเรชั่น (Configuration) ของระบบ

8) ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)

9) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

10) ข้อมูลไอพีแอดเดรส (IP Address) ที่เข้าถึง

11) ข้อมูลโพรโทคอล (Protocol) เครือข่ายที่ใช้

12) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

13) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

ส่วนที่ 13 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

13.1 ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

13.1.1 กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร โดยกำหนดพื้นที่ปฏิบัติงานพื้นที่ควบคุมเฉพาะให้ชัดเจน และควบคุม เพื่อกำหนดสิทธิการเข้าถึงพื้นที่ โดยผู้บริหารด้านเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย

13.1.2 กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร ดังนี้

1) ผู้เข้าใช้งานต้องเป็นผู้ที่ได้รับสิทธิการเข้าใช้งานพื้นที่เท่านั้น

2) ควบคุมการเข้าใช้งานในพื้นที่โดย แบบพิมพ์นิ้วมือ (Finger Scan)

3) ติดตั้งกล้องวงจรปิดเพื่อติดตาม/เฝ้าระวัง การเข้าพื้นที่ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

13.1.3 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

13.1.4 จัดให้มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน และมีความพร้อมในการใช้งานดังนี้

1) ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง

2) ติดตั้ง ระบบระงับเพลิง

3) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น

4) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำภายในห้อง เครื่องทำงานผิดปกติหรือหยุดการทำงาน

5) วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนอย่างสม่ำเสมอให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

13.2 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

13.2.1 หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงติดตั้งระบบป้องกันที่ปลอดภัย

13.2.2 ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

13.2.3 ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

13.2.4 ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่างๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

13.2.5 จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

13.2.6 ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

13.2.7 พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

13.2.8 ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

13.3 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

13.3.1 วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา

13.3.2 จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ส าหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

13.3.3 จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

13.3.4 ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำาการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบจะต้องอยู่นพื้นที่ทุกครั้ง

13.3.5 จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

13.4 การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

13.4.1 ต้องขออนุญาตจากผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอก หรือ นำไปซ่อมบำรุงภายนอก

13.4.2 ผู้ดูแลระบบจะต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าวกลับมาตามช่วงเวลาที่กำหนด และตรวจสอบอยู่ในสภาพดี

13.4.3 บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน และบันทึกส่งคืน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย

13.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off Premises)

13.5.1 กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

13.5.2 ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะเสี่ยงต่อการสูญหาย

13.5.3 เจ้าหน้าที่ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

13.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

13.6.1 ผู้บริหารด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย เป็นผู้อนุมัติในการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมามาใช้ โดยผู้ที่ต้องการกำจัด หรือ นำอุปกรณ์สารสนเทศกลับมาใช้ต้องยื่นเรื่องเป็นรายลักษณ์อักษรเพื่อขออนุมัติ

13.6.2 ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

ส่วนที่ 14 การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-mail)

14.1 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของโรงพิมพ์ตำรวจ ให้เหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยปีละครั้ง

14.2 ผู้ดูแลระบบรับเรื่องการขอใช้งานจดหมายอิเล็กทรอนิกส์ของงอค์กร โดยกำหนดสิทธิบัญชีรายชื่อผู้ใช้งาน e-mail รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งาน

14.3 กำหนดให้สามารถผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านใหม่ทันทีเมื่อได้รับรหัสผ่านครั้งแรก (Default Password) และต้องเปลี่ยนรหัสผ่านใหม่ทุก 180 วัน

14.4 ผู้ดูแลระบบไม่สามารถเข้ารหัสผ่านจดหมายอิเล็กทรอนิกส์เมื่อใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘x’ หรือ ‘o’ ในการพิมพ์แต่ละตัวอักษร

14.5 กำหนดให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง

14.7 ระบบจดหมายอิเล็กทรอนิกส์จะออกจากระบบ (Log out) เพื่อตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาภายในระยะเวลา 30 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

14.8 ผู้ใช้งานควรหลีกเลี่ยงค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

14.9 ผู้ใช้งานต้องระมัดระวังในการใช้e-mail เพื่อไม่ให้เกิดความเสียหายต่อ หน่วยงาน ได้แก่ การละเมิดสิทธิสร้างความร าคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์รวมทั้งไม่อนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้e-mail ผ่านระบบเครือข่ายของ หน่วยงาน

14.10 ผู้ใช้งานต้องไม่ใช้ที่อยู่อีเมล (E-mail Address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของอีเมล

14.11 หลังจากการใช้งาน e-mail เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้งเพื่อ ป้องกันบุคคลอื่นเข้าใช้งาน e-mail โดยไม่ได้รับอนุญาต

14.12 ผู้ใช้งานควรตรวจสอบเอกสารแนบจาก e-mail ก่อนท าการเปิด โดยใช้โปรแกรม ป้องกันไวรัส โดยเฉพาะการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

14.13 ผู้ใช้งานไม่เปิดหรือส่งต่อ e-mail หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

14.14 ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับ-ส่ง e-mail ที่ไม่เหมาะสม หรือข้อมูลอัน อาจทำให้เสียชื่อเสียง หรือข้อมูลทำให้เกิดความแตกแยกผ่านทาง e-mail

14.15 ผู้ใช้งานควรตรวจสอบตู้เก็บ e-mail (Inbox) ของตนเองทุกวัน และควรลบ e-mail ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่บน e-mail

ส่วนที่ 15 การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

15.1 อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

15.2 ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักในเรื่องความมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือข้อมูลความลับของหน่วยงาน

15.3 ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน

15.4 หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อหน่วยงาน ผู้ใช้งานต้องแจ้งต่อ หมวดนโยบายแผนและสารสนเทศ โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

หมวด 2 นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล

วัตถุประสงค์

1) เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง

2) เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

3) เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

1) หมวดนโยบายแผนและสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

ส่วนที่ 1 การสำรองข้อมูล (Back Up)

คัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

1.1 จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานพร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

1.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และวางแผน โดยการกำหนดความถี่ในการสำรองข้อมูล โดยพิจารณาจาก ความสำคัญของข้อมูล, ความถี่ในการเปลี่ยนแปลงข้อมูล โดยมีรายละเอียดการสำรองข้อมูล ดังนี้

1.2.1 กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ ดังนี้

1) ข้อมูลคอนฟิกกูเรชัน (Configuration) สำหรับระบบ

2) ฐานข้อมูล (Database) ในระบบสารสนเทศ

3) ซอฟต์แวร์ (Software) ต่างๆ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ ระบบงาน หรือซอฟต์แวร์อื่นๆ ที่สำคัญ

1.2.2 กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสม โดยแบ่งเป็น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

1.2.3 ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมสำหรับการกู้คืนระบบ

1.2.4 บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการวัน/เวลา ชื่อข้อมูลที่สำรอง สถานการณ์สำรองข้อมูล เป็นต้น

1.2.5 ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และปากพบว่าผิดปกติต้องจัดทำบันทึกและดำเนินการแก้ไขโดยทันที

1.2.6 ในกรณีที่จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล ต้องชี้บ่งสื่อบันทึกข้อมูลไว้อย่างชัดเจน โดยมีรายละเอียดของ ชื่อ วัน/เวลาสำรองข้อมูล ผู้รับผิดชอบ โดยสื่อสำรองข้อมูลจะต้องจัดเก็บไว้อย่างปลอดภัย และข้อมูลที่สำรองต้องเข้ารหัสเพื่อความปลอดภัย

1.2.7 จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้น้ำท่วม แผ่นดินไหว การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานในสถานที่ทำงานได้ เป็นต้น ทั้งนี้สอดคล้องตามแผนฉุกเฉินด้านสารสเทศที่กำหนดไว้

1.2.8 วางแผนทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ (restore) โดยการทดสอบต้องจัดทำบันทึกการทดสอลไว้เป็นหลักฐาน

ส่วนที่ 2 การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจตามแนวทางต่อไปนี้

2.1 จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

2.1.1 กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

2.1.2 ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้นรวมทั้งมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานใน สถานที่ทำงานได้เป็นต้น ทำให้ไม่สามารถเข้ามาใช้งานระบบสารสนเทศได้

2.1.3 กำหนดขั้นตอนปฏิบัติในการกู้คืน (Recover) ระบบสารสนเทศ และระยะเวลาในการกู้คืนระบบที่สอดคล้องตามเป้าหมายที่หน่วยงานกำหนดไว้

2.1.4 กำหนดขั้นตอนปฏิบัติในกู้คืนระบบ และการทดสอบแผนฉุกเฉิน

2.1.5 กำหนดช่องทางในการติดต่อเมื่อเกิดกรณีฉุกเฉิน ทั้งผู้รับผิดชอบภายในหน่วยงาน และผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำาเป็นที่จะต้องติดต่อผู้ให้บริการ

2.1.6 สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

2.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

2.3 กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

2.4 ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

2.5 ทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่ เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

หมวด 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

1) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความ มั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

2) เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

3) เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ แนวปฏิบัติ

ผู้รับผิดชอบ

1) หมวดนโยบายแผนและสารสนเทศ

2) ผู้ดูแลระบบที่ได้รับมอบหมาย

3) ผู้ตรวจสอบภายใน

แนวทางปฏิบัติ

1. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

1.1 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ 1 ครั้ง

1.2 ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

2. มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อย ดังนี้

2.1 มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

2.2 มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

2.3 มีการตรวจสอบและประเมินความเสี่ยงและให้จัดท รายงานพร้อมข้อเสนอแนะ

2.4 มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

2.4.1 กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่างเดียว

2.4.2 ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งการทำลายหรือลบข้อมูลโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างเหมาะสม

2.4.3 กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

2.4.4 กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อก (Log) แสดงการเข้าถึง วันและเวลาที่เข้าถึงระบบ

2.4.5 ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

หมวด 4 หน้าที่และความรับผิดชอบด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงสุด (CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน

แนวปฏิบัติ

ส่วนที่ 1 ระดับนโยบาย

1.1 ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) ของโรงพิมพ์ตำรวจ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบ คอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอัน เนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศ

1.2 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) โรงพิมพ์ตำรวจ เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้ สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.3 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของโรงพิมพ์ตำรวจ ผู้รับผิดชอบ ดังนี้

1.3.1 กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูล และเทคโนโลยีสารสนเทศ

1.3.2 ควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

1.3.3 วางแผน จัดทำทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียม ความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถด าเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์

ส่วนที่ 2 ระดับปฏิบัติงาน

ระดับผู้ปฏิบัติการประกอบด้วย ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน เป็นผู้รับผิดชอบตามภารกิจ ดังนี้

2.1 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นผู้รับผิดชอบ ดังนี้

2.1.1 ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.2 ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและ ภัยพิบัติ

2.1.3 ควบคุม ดูแล รักษาความปลอดภัย และบ ารุงรักษาระบบคอมพิวเตอร์ระบบเครือข่ายระบบสารสนเทศ ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

2.1.4 ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

2.1.5 ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2.1.6 ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพิมพ์ตำรวจ

2.2 ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด

แนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity)

วัตถุประสงค์

1. เพื่อให้โรงพิมพ์ตำรวจมีการกำกับดูแล นโยบาย กระบวนการ และเครื่องมือในการบริหารจัดการ ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk) และความเสี่ยงด้านภัยคุกคามทาง ไซเบอร์ (Cyber Risk) ที่สามารถระบุความเสี่ยง (identify) ป้องกัน (protect) ตรวจพบ (detect) รับมือ (respond) กู้ระบบคืนสู่สภาวะปกติ (recover) และสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง เพื่อให้การบริหารความเสี่ยงและความปลอดภัยในการนำระบบ IT มาใช้ในการดำเนินธุรกิจมีความครอบคลุมและสามารถป้องกันความเสียหายได้อย่างทันท่วงที

2. สร้างความน่าเชื่อถือให้กับธุรกิจ จากการที่องค์กรมีการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ ควบคุมความเสี่ยงด้านระบบ IT และสามารถรักษาความปลอดภัยของข้อมูลได้อย่างรัดกุม

โรงพิมพ์ตำรวจ ได้ตระหนักถึงความสำคัญของความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk) รวมถึงความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber risk) จึงได้กำหนดแนวทางการกำกับดูแลการบริหารจัดการความเสี่ยงด้าน IT (IT Risk Management) การรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ (IT security) การควบคุมความเสี่ยงของระบบ IT และเตรียมความพร้อมในการรับมือกับความเสี่ยงด้ายภัยคุกคามทางไซเบอร์ (Cybersecurity) เพื่อให้องค์กรสามารถนำไปใช้เป็นแนวทางในการควบคุมความเสี่ยงของตนเองและพัฒนาโครงสร้างพื้นฐานระบบ IT เตรียมความพร้อมเพื่อการขยายธุรกิจเข้าสู่การเป็น digital economy ตลอดจนใช้ในการพัฒนาการกำกับดูแลโรงพิมพ์ตำรวจ เพื่อให้ทันกับวิวัฒนาการของความเสี่ยงที่เปลี่ยนแปลงไปตามบริบทในการทาธุรกิจ รวมถึงกำหนดให้องค์กรมีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ (Information technology security incident management) และในกรณีที่โรงพิมพ์ตำรวจถูกโจมตีทางไซเบอร์ (Cyber attack) ในระดับที่ส่งผลกระทบอย่างมีนัยสำคัญ โรงพิมพ์ตำรวจต้องรายงานต่อผู้บริหารสูงสุด โดยไม่ชักช้าเมื่อเกิดเหตุการณ์ดังกล่าว และมีแผนรองรับการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ (incident response plan) ที่เกิดขึ้น เพื่อให้โรงพิมพ์ตำรวจสามารถดำเนินธุรกิจและให้บริการลูกค้าได้อย่างต่อเนื่อง

อย่างไรก็ตาม ระบบเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจยังคงมีความหลากหลายและแตกต่างกันค่อนข้างมาก ดังนั้น การมีมาตรฐานและแนวปฏิบัติเพื่อรักษาความปลอดภัยของระบบ IT และข้อมูลสารสนเทศจะช่วยให้โรงพิมพ์ตำรวจสามารถนำไปประยุกต์ใช้ในการกำกับดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศ ได้อย่างเหมาะสมกับขนาดและความซับซ้อนของระบบ IT ของโรงพิมพ์ตำรวจเอง รวมถึงสามารถนำไปใช้ในการกำหนดมาตรการควบคุมความเสี่ยงของตนเองได้อย่างมีประสิทธิภาพ

กรอบแนวทางปฏิบัติสาหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ มีจุดมุ่งหมายเพื่อทำให้แน่ใจว่า องค์กรสามารถบรรลุเป้าหมายที่กำหนดไว้ โดยนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุน และสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีมาใช้ได้อย่างมีประสิทธิภาพ การบริหารงานด้านเทคโนโลยีสารสนเทศที่ดีนั้นต้องมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากรและข้อมูลที่มีประสิทธิภาพเพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมายขององค์กร และการบริหารความเสี่ยงที่เหมาะสม รวมทั้งมีการรายงานและติดตามการดำเนินงาน เพื่อให้มั่นใจว่า เทคโนโลยีที่องค์กรนำมาใช้สามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจและสร้างศักยภาพในการแข่งขัน รวมทั้งเพิ่มมูลค่าให้กับองค์กร โดยองค์กรต้องพิจารณาดาเนินการอย่างน้อยดังต่อไปนี้

1. นโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

1.1 คณะกรรมการโรงพิมพ์ตำรวจและผู้บริหารระดับสูง มีหน้าที่ดูแลให้มีการกำหนดนโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร รวมทั้งทำหน้าที่ในการพิจารณาอนุมัตินโยบายดังกล่าว ทั้งนี้ องค์กรต้องทำการสื่อสารนโยบายดังกล่าว เพื่อสร้างความเข้าใจและให้สามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะ อย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานภายในองค์กร เพื่อให้มีการประสานงานและสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้

นโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

- การรักษาความถูกต้องปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ
- การควบคุมการเข้าถึงระบบสารสนเทศ และข้อมูล
- การรักษาความปลอดภัยของข้อมูล
- การติดตามตรวจสอบความผิดปกติและช่องโหว่ของระบบสารสนเทศ
- การบริหารจัดการระบบ IT ให้มีความพร้อมในการรองรับการดาเนินธุรกิจอย่างต่อเนื่อง

1.2 องค์กรต้องจัดให้มีการประเมินประสิทธิภาพของนโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยขององค์กร ทั้งนี้ การประเมินประสิทธิภาพ องค์กรสามารถกระทำได้โดยหน่วยงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศขององค์กร (IT Audit) หรือผู้ตรวจสอบภายนอก เพื่อปรับปรุงแก้ไขข้อบกพร่องของการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร

1.3 ในกรณีที่องค์กร มีการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการจากภายนอก (Outsource) องค์กรต้องจัดให้มีนโยบายเพื่อรองรับการใช้บริการดังกล่าว ซึ่งต้องครอบคลุมถึงวิธีการคัดเลือกและพิจารณาคุณสมบัติของผู้ให้บริการ และมีข้อกำหนดเกี่ยวกับการใช้บริการเพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศอย่างไม่เหมาะสม รวมถึงข้อกาหนดเกี่ยวกับการรักษาความลับของข้อมูลและไม่เปิดเผยข้อมูลที่มีความสำคัญ

นอกจากนี้ องค์กรต้องมีมาตรการเพื่อให้มั่นใจได้ว่าสามารถควบคุมการปฏิบัติงานของผู้ให้บริการจากภายนอกให้เป็นไปตามข้อตกลงที่กำหนดไว้ โดยสามารถตรวจสอบกระบวนการปฏิบัติงาน รวมทั้งมีแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ (incident response plan)

2. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องสอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงรวมขององค์กรและครอบคลุมในเรื่องดังต่อไปนี้

2.1 การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2.2 การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

2.3 การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

2.4 การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

2.5 การกำหนดตัวชี้วัดระดับความเสี่ยง รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดดังกล่าวต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

3. การรักษาความถูกต้องปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

3.12 องค์กรต้องกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติงานเป็นไปอย่างถูกต้องและปลอดภัย โดยกำหนดเป็นลายลักษณ์อักษรเพื่อให้พนักงานปฏิบัติการคอมพิวเตอร์ สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศ เช่น ขั้นตอนในการเปิด/ปิดระบบการประมวลผล การตรวจสอบประสิทธิภาพการทำงานของระบบ เป็นต้น

3.2 การรับ -ส่งข้อมูลสารสนเทศ (Information transfer) ทั้งภายในและภายนอกองค์กร องค์กรต้องรักษาความปลอดภัยของข้อมูลที่มีการรับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ โดยมีการป้องกันการเปลี่ยนแปลงแก้ไขหรือทำความเสียหายกับข้อมูล และโปรแกรมไม่ประสงค์ดี (malware) ที่ถูกส่งผ่านช่องทางการสื่อสาร มีการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) และการส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกองค์กร โดยการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศ

3.3 องค์กรต้องมีมาตรการป้องกันและตรวจสอบภัยคุกคามจากโปรแกรมที่ไม่ประสงค์ดี (Malware) โดยติดตั้งโปรแกรมป้องกัน Malware ให้ครอบคลุมทั้งเครื่องประมวลผลและเครื่องคอมพิวเตอร์ พร้อมทั้งปรับปรุงโปรแกรมป้องกันให้เป็นปัจจุบัน และสามารถแก้ไขระบบเทคโนโลยีสารสนเทศให้สามารถ

กลับมาใช้งานได้ตามปกติ นอกจากนี้ องค์กรต้องมีระบบหรือกระบวนการในการป้องกันเพื่อลดความเสี่ยงจากการทำ website เลียนแบบ (Phishing)

3.4 องค์กรต้องกำหนดให้มีการสำรองข้อมูลที่สำคัญทางธุรกิจ ระบบปฏิบัติการ โปรแกรมประยุกต์ ระบบงานคอมพิวเตอร์อย่างครบถ้วน และกำหนดเป้าหมายในการกู้คืนข้อมูล (Recovery Point Objective: RPO) เช่น ประเภท ของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ โดยองค์กรต้องจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกสถานที่เพื่อความปลอดภัย ในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย และต้องทำการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อย ปีละ 1 ครั้ง ทั้งนี้ องค์กรต้องมีการป้องกันความเสียหายของข้อมูลที่ทำการสำรองไว้ด้วย

การสำรองข้อมูล องค์กรต้องกาหนดวิธีปฏิบัติอย่างน้อยดังนี้

- ข้อมูลที่ต้องสารอง และความถี่ในการสารอง
- ประเภทสื่อที่ใช้ในการบันทึกข้อมูล (media
- จำนวนที่ต้องสำรอง (copy)
- ขั้นตอนและวิธีการสำรองข้อมูล
- สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล
- กระบวนการกู้คืนข้อมูลในกรณีที่ข้อมูลสูญหาย

ทั้งนี้ สถานที่ในการจัดเก็บข้อมูลสำรอง องค์กรต้องคำนึงถึงความมั่นคงปลอดภัยและต้องมีระยะห่างจากสำนักงานใหญ่เพียงพอที่จะไม่ได้รับผลกระทบเดียวกันและต้องไม่ใช้ระบบสาธารณูปโภค (น้ำประปา ไฟฟ้า อินเตอร์เน็ต) จากแหล่งเดียวกัน รวมถึงต้องมีการควบคุมสภาพแวดล้อมของห้องเก็บสื่อบันทึกข้อมูล และป้องกันความเสียหายของสื่อ

ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น กรณีที่จัดเก็บข้อมูลในสื่อบันทึกประเภทใด ต้องมีการเก็บอุปกรณ์และโปรแกรมที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

3.5 จัดเก็บและบันทึกหลักฐาน (logs) ต่าง ๆ ของการเข้าใช้งานระบบเทคโนโลยีสารสนเทศให้ครบถ้วนและเพียงพอสำหรับการตรวจสอบ โดยอย่างน้อยต้องครอบคลุมการเข้าถึงและใช้งานระบบสารสนเทศ (application log) การใช้งานแฟ้มข้อมูล และการใช้อินเทอร์เน็ตผ่านระบบเครือข่ายคอมพิวเตอร์ภายในขององค์กร (internet access log)

3.6 ควบคุมและจำกัดสิทธิการติดตั้งซอฟท์แวร์บนระบบงาน เพื่อให้ระบบปฏิบัติงานมีความถูกต้องครบถ้วนและน่าเชื่อถือ รวมถึงทาการทดสอบการเจาะระบบ (penetration test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอกก่อนทำการติดตั้งบนระบบงานขององค์กร เพื่อตรวจหาช่องโหว่ที่อาจเกิดขึ้น ของซอฟแวร์ที่จะติดตั้งใหม่อย่างเหมาะสม ในกรณีที่มีการติดตั้ง feature เพิ่มเติมบนระบบงานเก่า องค์กรต้องพิจารณาทาการทดสอบหาก feature ใหม่มีผลกระทบต่อระบบงานที่ใช้อยู่แล้ว

3.7 การใช้บริการ Cloud Computing จากผู้ให้บริการภายนอกด้านโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ และระบบงานสารสนเทศ เพื่อการจัดเก็บข้อมูล การประมวลผล หรือดำเนินการใด ๆ ที่เกี่ยวข้องกับข้อมูลขององค์กร

องค์กรต้องกำหนดหลักเกณฑ์วิธีการคัดเลือกผู้ให้บริการ และมาตรฐานการให้บริการของผู้ให้บริการ Cloud Computing อย่างชัดเจน โดยต้องให้ความสำคัญในเรื่องการรักษาความปลอดภัยของข้อมูล ความถูกต้องเชื่อถือได้ ของข้อมูลและระบบสารสนเทศ และความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ รวมถึงกำหนดคุณสมบัติของ ผู้ให้บริการ เช่น ฐานะการเงิน ความเพียงพอของการให้บริการเพื่อให้มั่นใจได้ว่าผู้ให้บริการสามารถให้บริการตามความต้องการขององค์กรได้อย่างต่อเนื่อง ทั้งนี้ องค์กรควรมีการติดตาม ประเมิน และทบทวนการให้บริการและคุณสมบัติของ ผู้ให้บริการ Cloud Computing เป็นประจำอย่างน้อยทุกปี

4. การควบคุมการเข้าถึงระบบสารสนเทศ และข้อมูล (access control) เพื่อป้องกันการถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาต อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

4.1 การควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ

องค์กรต้องกำหนดสิทธิในการเข้าถึงระบบและข้อมูลให้เหมาะสมตามความจำเป็นและหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการรั่วไหลของข้อมูลและแก้ไขฐานข้อมูลโดยไม่ได้รับอนุญาต โดยกำหนดให้ผู้ใช้งานต้องยืนยันตัวบุคคลโดยกำหนด Username และ Password เพื่อเข้าถึงข้อมูลได้ตามสิทธิที่กำหนด และบันทึกการเข้าถึงระบบโดยบัญชีผู้ใช้ทุกประเภท (access log)

ทั้งนี้ องค์กรต้องมีข้อกำหนดเกี่ยวกับผู้ใช้งานที่ได้รับสิทธิให้เข้าถึงระบบและข้อมูลในการดูแลการใช้สิทธิที่ได้รับ รวมถึงกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่นในการใช้งานระบบคอมพิวเตอร์และมีการอนุมัติจากผู้มีอำนาจทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นรวมถึงกาหนดระยะเวลาในการใช้งาน

4.2 การกำหนดมาตรการเพื่อสร้างความปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินสารสนเทศ

องค์กรต้องจัดพื้นที่ในการจัดวางทรัพย์สินสารสนเทศที่มีความสำคัญ เช่น ห้องเซิร์ฟเวอร์ ศูนย์คอมพิวเตอร์ เป็นต้น ให้มีความปลอดภัยและป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าถึงพื้นที่ดังกล่าว โดยต้องคำนึงถึงความปลอดภัยจากภัยธรรมชาติ และภัยคุกคามจากมนุษย์ และมีความมิดชิดรวมทั้งป้องกันมิให้มีการเปิดเผยข้อมูลและรายละเอียดของพื้นที่หวงห้ามต่อสาธารณะ องค์กรต้องกำหนดสิทธิการเข้าออกพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง และระบบการควบคุมการเข้าออกอย่างรัดกุม และองค์กรต้องบันทึกข้อมูลการเข้า - ออกห้องเซิร์ฟเวอร์ หรือ ศูนย์คอมพิวเตอร์ รวมถึงต้องจัดให้มีการรักษาความมั่นคงปลอดภัย เช่น มีระบบกล้องวงจรปิด เครื่องสแกนลายนิ้วมือ อุปกรณ์เตือนไฟไหม้ ถังดับเพลิงหรือระบบดับเพลิงแบบอัตโนมัติ ระบบไฟฟ้าสำรอง เป็นต้น ทั้งนี้ องค์กรต้องมีมาตรการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ มิให้เกิดการสูญหาย ถูกโจรกรรม ถูกเข้าถึง หรือถูกใช้งานโดยบุคคลที่ไม่เกี่ยวข้อง

5. การรักษาความปลอดภัยของข้อมูล

องค์กรต้องมีกระบวนการในการรักษาความปลอดภัยของข้อมูล ที่เพียงพอแก่การป้องกันไม่ให้บุคคลที่ไม่มีอำนาจเกี่ยวข้องเข้าถึง หรือสามารถเปลี่ยนแปลงแก้ไขข้อมูล หรือนำข้อมูลไปใช้ประโยชน์ในทางที่ผิดกฎหมาย โดยแนวทางการรักษาความปลอดภัยของข้อมูลอย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

5.1 องค์กรต้องทำการระบุว่า ข้อมูลอะไรบ้างที่เป็นข้อมูลที่สำคัญหรือเป็นข้อมูลความลับขององค์กร และทำการจัดประเภทข้อมูลตามระดับชั้นความลับและความสำคัญ เพื่อให้ข้อมูลที่สำคัญได้รับการปกป้องในระดับที่เหมาะสมตามระดับชั้นความลับ

5.2 กาหนดสิทธิ์ในการเข้าถึงข้อมูลที่สำคัญหรือข้อมูลความลับ เพื่อป้องกันการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต ทั้งนี้ ต้องเพียงพอสำหรับใช้ในการทำงานปกติและสอดคล้องกับหน้าที่การปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้อง การควบคุมที่มีประสิทธิภาพจะต้องสามารถป้องกันและจำกัดการเข้าถึงตามที่สิทธิที่กาหนดไว้ได้

5.3 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ องค์กรต้องทาการเข้ารหัสข้อมูล (cryptographic control) เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลให้สอดคล้องและเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้น

5.4 การจัดเก็บข้อมูลสำคัญหรือข้อมูลที่มีชั้นความลับ องค์กรต้องรักษาความปลอดภัยของข้อมูลโดยการเข้ารหัสข้อมูล (encryption) ที่สามารถป้องกันการนาข้อมูลสำคัญไปใช้ประโยชน์ในทางที่ผิดในกรณีข้อมูลรั่วไหล และสอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่มีความสำคัญ รวมทั้งกำหนดผู้รับผิดชอบในการบริหารจัดการการเข้ารหัสข้อมูล

6. การติดตามตรวจสอบความผิดปกติและช่องโหว่ของระบบสารสนเทศ

องค์กรต้องทำการประเมินช่องโหว่ (vulnerability assessment) กับระบบงานที่มีความสำคัญทุกระบบ อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ โดยอย่างน้อยต้องจัดให้มีกระบวนการประเมินหรือตรวจสอบหาช่องโหว่ของระบบ และมีมาตรการดำเนินการรองรับเพื่อปิดช่องโหว่ หรือกำหนดแผนรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ โดยองค์กรต้องกำหนดผู้รับผิดชอบในการจัดการเกี่ยวกับ ช่องโหว่ของระบบและดำเนินการปิดช่องโหว่ที่พบโดยไม่ชักช้า ทั้งนี้ ต้องมีการบันทึกและจัดเก็บหลักฐานเพื่อการตรวจสอบในการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ของระบบด้วย

7. การรักษาความพร้อมใช้งานของระบบสารสนเทศ และการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ

7.1 องค์กรต้องมีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ โดยอย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้

กำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ อย่างเป็นลายลักษณ์อักษร และประเมินเหตุการณ์หรือจุดอ่อนของการรักษา

ความปลอดภัยระบบสารสนเทศ เพื่อพิจารณาระดับความรุนแรงของเหตุการณ์และผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ และต้องจัดให้มีการทดสอบกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

7.2 องค์กรต้องกำหนดให้มีการบริหารความต่อเนื่องทางธุรกิจในด้านระบบสารสนเทศ

7.2.1 องค์กรต้องกำหนดแผนการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ เพื่อให้องค์กรสามารถกู้ระบบสารสนเทศหรือจัดหาระบบปฏิบัติการมาดำเนินการทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด และยังคงดำเนินธุรกิจได้อย่างต่อเนื่อง โดยมีรายละเอียดอย่างน้อยดังนี้

- จัดลำดับความสำคัญในการกู้คืนระบบงานให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น รวมถึงความสัมพันธ์ของแต่ละระบบงาน และการกำหนดระยะเวลาในการกลับคืนสภาพการดำเนินงานตามปกติของระบบงาน
- ขั้นตอนการแก้ไขปัญหาหรือตอบสนองต่อเหตุการณ์ในแต่ละสถานการณ์ที่เกิดขึ้น
- บุคคลที่ทำหน้าที่รับผิดชอบและมีอำนาจตัดสินใจ รวมถึงกำหนดเจ้าหน้าที่ผู้รับผิดชอบที่สามารถปฏิบัติงานได้ในแต่ละสถานการณ์ รวมทั้งมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด
- ระบุทรัพยากรที่จำเป็นสำหรับระบบงานที่สำคัญที่จำเป็นต้องใช้ เช่น ข้อมูล รายละเอียดของศูนย์คอมพิวเตอร์สำรอง สถานที่ตั้ง แผนที่ เครื่องรุ่นคอมพิวเตอร์ ระบบที่ใช้ในการปฏิบัติงาน (Systems) ข้อมูลและบันทึกต่าง ๆ (Records & Data) โดยองค์กรต้องมีระบบสารสนเทศที่อยู่ในสภาพพร้อมใช้งาน

7.2.2 องค์กรต้องมีการสื่อสารแผน DRP ให้แก่เจ้าหน้าที่ที่เกี่ยวข้องเพื่อรับทราบและสร้างความเข้าใจที่ตรงกัน เพื่อให้สามารถนำไปปฏิบัติได้อย่างถูกต้องเมื่อเกิดเหตุการณ์

7.2.3 ทำการทดสอบการปฏิบัติตามแผน DRP อย่างน้อยปีละ 1 ครั้ง โดยต้องกำหนดให้มีการทดสอบในลักษณะสถานการณ์ที่สอดคล้องกับลักษณะ ขอบเขต และความซับซ้อนในการดาเนินธุรกิจขององค์กร และเป็นสถานการณ์ที่มีความเป็นไปได้และสอดคล้องกับสถานการณ์ในปัจจุบันขององค์กร

ในปัจจุบันโรงพิมพ์ตำรวจจำเป็นต้องตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยของภัยคุกคามทางไซเบอร์ ซึ่งการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk) เพียงอย่างเดียวอาจจะยังไม่เพียงพอในการรับมือกับภัยคุกคามที่ไม่อาจคาดคิด ไม่แน่นอน ไม่สามารถคาดการณ์ได้ และที่ไม่รู้ (unknown, unpredictable, uncertain, unexpected) ดังนั้น เพื่อให้โรงพิมพ์ตำรวจตระหนักและให้ความสำคัญต่อ cyber risk ที่จะเกิดขึ้น โรงพิมพ์ตำรวจจึงได้กำหนดแนวทางปฏิบัติในเบื้องต้นที่องค์กรสามารถนำไปปรับใช้เพื่อให้การบริหารจัดการความเสี่ยงมีความครอบคลุมถึงความเสี่ยงด้านภัยคุกคามทางไซเบอร์มากขึ้น โดยมีรายละเอียดดังนี้

7. การกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์

7.1 องค์กรต้องกำหนดบทบาทหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงในการกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ เพื่อให้องค์กรมีมาตรฐานในการรักษาความปลอดภัย ที่สามารถระบุ (identify) ป้องกัน (protect) ตรวจพบ (detect) รับมือ (response) และสามารถกู้คืน (recovery) เพื่อกลับสู่สภาวะปกติได้ และสนับสนุนให้องค์กรมีขีดความสามารถที่เพียงพอเหมาะสมกับปริมาณและความซับซ้อนของระบบ IT ขององค์กร โดยกำหนดนโยบายการบริหารจัดการความเสี่ยงครอบคลุมความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber Risk) รวมถึงกำหนดให้มีการรายงานข้อมูลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ให้ผู้บริหารระดับสูง ที่ได้รับมอบหมายรับทราบเป็นประจำ

7.2 กำหนดให้มีหน่วยงานหรือทีมงานที่ทำหน้าที่รับผิดชอบในการประเมิน ติดตามดูแล ป้องกัน และรับมือกับภัยคุกคามทางไซเบอร์ และรายงานข้อมูลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ให้ผู้บริหารระดับสูงที่ได้รับมอบหมายรับทราบอย่างสม่ำเสมอ ทั้งนี้ องค์กรอาจพิจารณากำหนดให้มีเจ้าหน้าที่หรือทีมงานเฉพาะที่ทำหน้าที่รับผิดชอบในการรับมือและจัดการกับเหตุการณ์ผิดปกติทางไซเบอร์ได้ทันเวลาเพื่อลดผลกระทบที่จะเกิดขึ้น

7.3 องค์กรต้องจัดอบรมให้ความรู้เรื่องภัยคุกคามทางไซเบอร์ (Cybersecurity Awareness) ที่อาจเกิดขึ้นเพื่อให้พนักงานมีความรู้ความเข้าใจและตระหนักถึงความจำเป็นในการรักษาความปลอดภัยและเข้าใจถึงผลกระทบที่จะเกิดขึ้นตามมาหากเกิดเหตุการณ์ขึ้น รวมทั้งสื่อสารแนวทางการป้องกันและการรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์

7.4 กำหนดให้มีช่องทางในการประสานงานระหว่างหน่วยงานภายในและภายนอกองค์กรอย่างชัดเจน รวมถึงผู้ให้บริการจากภายนอก เพื่อกำหนดแนวทางในการรับมือและแก้ไขเหตุการณ์ทางด้านความปลอดภัยได้อย่างมีประสิทธิภาพและทันเวลา

8. การบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์

8.1 องค์กรต้องกำหนดนโยบายในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่ครอบคลุมการระบุความเสี่ยงด้านภัยคุกคามทางไซเบอร์ การป้องกัน การตรวจพบ การรับมือและการกู้คืน รวมทั้งทบทวนและอัพเดทข้อมูลภัยคุกคามทางไซเบอร์ใหม่ ๆ ตลอดเวลา เพื่อให้เท่าทันต่อการเปลี่ยนแปลงที่เกิดขึ้น โดยมีรายละเอียดดังนี้

8.1.1 การระบุ

องค์กรต้องทำการระบุว่า กระบวนการดำเนินงานและทรัพย์สินสารสนเทศใดบ้างที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ และต้องได้รับการรักษาความมั่นคงปลอดภัย เพื่อบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล ขององค์กรได้อย่างเหมาะสม

8.1.2 การป้องกัน

องค์กรต้องมีมาตรการป้องกันที่เหมาะสมเพื่อจำกัดผลกระทบของเหตุการณ์ภัยคุกคามไซเบอร์ ซึ่งครอบคลุมถึงเรื่องการควบคุมการเข้าถึง การฝึกอบรม และการสร้างความตระหนักให้แก่พนักงานและผู้ที่เกี่ยวข้อง ความปลอดภัยของข้อมูล และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ

ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี นอกจากนี้ องค์กรต้องทำการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบอิเล็กทรอนิกส์อย่างสม่ำเสมอเพื่อให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง รวมทั้งการเปลี่ยนแปลงแก้ไข Patch หรือ update software

8.1.3 การตรวจจับ

องค์กรต้องมีกระบวนการติดตามเฝ้าระวัง และตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง และแจ้งเตือนถึงสิ่งที่ผิดปกติต่าง ๆ รวมถึงการติดตามเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากทั้งภายในและภายนอก วิเคราะห์จุดอ่อนหรือช่องโหว่ของภัยคุกคามที่เกิดขึ้น เพื่อเป็นข้อมูลประกอบในการพิจารณาทบทวนแนวทางการป้องกันความเสี่ยงและผลกระทบที่จะเกิดขึ้นกับองค์กรในอนาคต

8.1.4 การตอบสนอง/การรับมือ

องค์กรต้องกำหนดแผนการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์และแนวทางแก้ไขปัญหา รวมถึงจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่องให้ครอบคลุมกรณีที่ผลกระทบหรือความเสียหายจากภัยคุกคามทางไซเบอร์ ทำให้การดำเนินงานหยุดชะงัก เพื่อให้สามารถรักษาระดับความปลอดภัยและการให้บริการอย่างต่อเนื่อง และองค์กรต้องทำการวิเคราะห์หาสาเหตุและตรวจหาหลักฐานของภัยคุกคามที่เกิดขึ้น รวมถึงมีกระบวนการสื่อสารกับลูกค้า ประชาชน และผู้มีส่วนได้เสียที่ชัดเจน เพื่อความเข้าใจที่ถูกต้องตรงกันต่อสถานการณ์ที่เกิดขึ้นขององค์กร

8.1.5 การกู้คืน

องค์กรต้องกำหนดแผนและกระบวนการในการกู้คืนระบบให้สามารถกลับมาดำเนินการได้ตามปกติภายในระยะเวลาที่กำหนด รวมถึงทาการทบทวนปรับปรุงแผนให้เป็นปัจจุบันเพื่อให้ทันต่อสถานการณ์และนำบทเรียนที่ได้รับ จากเหตุการณ์ภัยคุกคามที่เกิดขึ้น มาเป็นส่วนหนึ่งในการทบทวนแผนและกระบวนการกู้คืนระบบให้มีประสิทธิภาพยิ่งขึ้นเพื่อป้องกันปัญหาและผลกระทบที่จะเกิดขึ้นซ้ำในอนาคต

แนวทางในการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร (ISMS Audit)

ผู้สอบบัญชีควรมีความรู้เกี่ยวกับระบบสารสนเทศที่ใช้คอมพิวเตอร์อย่างเพียงพอ เพื่อวางแผน สั่งการ ควบคุมดูแล และสอบทานงานที่ได้ปฏิบัติ รวมทั้งต้องมีการพิจารณาว่าจeเป็นต้องใช้ผู้เชี่ยวชาญด้านระบบสารสนเทศเข้ามาช่วยในการตรวจสอบหรือไม่ เพื่อความเหมาะสมของกิจการและเป็นไปตามมาตรฐาน

ผู้สอบบัญชีอาจต้องใช้เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย เนื่องจากการที่ข้อมูลถูกเก็บไว้ในแฟ้มข้อมูลบนคอมพิวเตอร์การประมวลผลและวิเคราะห์ข้อมูลจำนวนมากบนคอมพิวเตอร์ จะมีผลกระทบกับงานตรวจสอบเป็นอย่างมาก เพราะการประมวลผลเป็นกระบวนการที่ทำโดยโปรแกรมที่ขาดร่องรอย จากการตรวจสอบที่มองด้วยตา ต่างจากการตรวจสอบข้อมูลของกิจการที่จัดทำบัญชีด้วยมือ (Manual) ที่ตรวจสอบได้จากเอกสารที่เป็นกระดาษเช่นแบบแต่ก่อน

ในการนำระบบสารสนเทศเข้ามาใช้ในองค์กรนั้น เพื่อสร้างความมั่นใจได้ว่าระบบฯ ที่นำมาใช้มีความปลอดภัยและถูกต้องจึงต้องมีการควบคุมและควบคู่ไปกับการตรวจสอบ โดยครอบคลุมในเรื่องทั่วไปเกี่ยวกับระบบสารสนเทศขององค์กรดังนี้

- การควบคุมกระบวนการพัฒนาระบบงาน (Implementation controls) ตรวจสอบกระบวนการพัฒนาระบบงานในจุดต่างๆ เพื่อให้มั่นใจได้ว่ากระบวนการพัฒนาฯ อยู่ในความควบคุมและการบริหารที่ดี การตรวจสอบการพัฒนาซอฟต์แวร์ควรที่จะมีการตรวจสอบทบทวนอย่างเป็นทางการ ในแต่ละขั้นตอนการพัฒนาซอฟต์แวร์ที่สำคัญ เพื่อเปิดโอกาสให้ผู้ใช้และผู้บริหารมีโอกาสยอมรับหรือปฏิเสธระบบงานเป็นระยะก่อนที่ระบบงานจะพัฒนาเสร็จเรียบร้อย การตรวจสอบระบบงานควรจะตรวจการเข้าไปมีส่วนร่วมของผู้ใช้ในแต่ละขั้นตอนของการพัฒนาฯ และนำทฤษฎีการวิเคราะห์ค่าใช้จ่ายผลตอบแทนมาใช้ศึกษาความเป็นไปได้ของโครงการ การตรวจสอบจะต้องคำนึงถึงการประกันคุณภาพในระหว่างที่ทำการพัฒนา การเปลี่ยนแปลงระบบงาน และการทดสอบระบบงาน รวมทั้งเอกสารประกอบระบบงานนั้น
- การควบคุมซอฟต์แวร์ (Software Control) มีความจำเป็นสำหรับซอฟต์แวร์ประเภทต่าง ๆ ที่นำมาใช้ประกอบระบบงาน การควบคุมซอฟต์แวร์ตรวจสอบการใช้ซอฟต์แวร์ระบบและป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้งานเนื่องจากซอฟต์แวร์ระบบมีความสำคัญต่อการควบคุมการทำงานของซอฟต์แวร์อื่น ๆ และเป็นตัวที่เข้าไปแก้ไขเปลี่ยนแปลงข้อมูลโดยตรง
- การควบคุมทางกายภาพ (Physical hardware controls) เป็นการป้องกันทางกายภาพเพื่อไม่ให้ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ และตรวจสอบความผิดปกติของอุปกรณ์ทุกชนิด การป้องกันนี้รวมไปถึงการป้องกันอัคคีภัย การป้องกันไม่ให้อุณหภูมิ

และความชื้นในห้องเก็บอุปกรณ์สูงหรือต่ำเกินไป การป้องกันข้อมูลเสียหายด้วยการทำสำเนาข้อมูล การรักษาให้ฮาร์ดดิกส์สามารถให้บริการได้ตลอดเวลาที่ต้องการ เป็นต้น

- การควบคุมการปฏิบัติงานเครื่องคอมพิวเตอร์ (Computer operations controls) ประยุกต์ใช้กับงานของฝ่ายคอมพิวเตอร์เพื่อให้ขั้นตอนการปฏิบัติเกี่ยวกับอุปกรณ์บันทึกข้อมูลและการประมวลผลข้อมูลเป็นไปตามขั้นตอนที่กำหนด ได้แก่ การจัดสภาพแวดล้อมให้เหมาะสมกับการทำงานของคอมพิวเตอร์ การใช้ซอฟต์แวร์ การทำสำเนาข้อมูลและการฟื้นสภาพข้อมูลในกรณีที่โปรแกรมไม่ทำงานตามปกติ เป็นต้น
- การควบคุมความปลอดภัยข้อมูล (Data security controls) เป็นการปกป้องข้อมูลที่มีค่ายิ่งขององค์กรที่เก็บอยู่ในดิกส์หรือเทปหรืออุปกรณ์ใดก็แล้วแต่ ให้พ้นจากการใช้งาน การเปลี่ยนแปลง และการทำลายโดยบุคคลที่ไม่ได้รับอนุญาต การปกป้องนี้ต้องทำทั้งในขณะที่แฟ้มข้อมูลกำลังถูกใช้งานและเก็บรักษาไว้ ในสภาพการทำงานที่ข้อมูลมีการป้อนเข้ามาจากเครื่องเทอร์มินอล ข้อมูลที่แปลกปลอมเข้ามาจะต้องถูกกำจัดออกจากระบบ
- ระเบียบวินัยผู้บริหาร มาตรฐาน และขั้นตอนการปฏิบัติงาน (Administrative disciplines, standards, and procedures) หมายถึงการกำหนดมาตรฐาน กฎเกณฑ์ ขั้นตอนการปฏิบัติงาน และวินัยในการรักษาความปลอดภัย เพื่อให้มั่นใจได้ว่าการรักษาความปลอดภัยทั่วไปและการรักษาความปลอดภัยโปรแกรมประยุกต์ได้รับการจัดตั้งและนำไปปฏิบัติอย่างจริงจัง

ปัจจุบันการดำเนินธุรกิจกำลังเข้าสู่ยุค digital โดยอาศัยเทคโนโลยีสารสนเทศเป็นตัวขับเคลื่อน และมีบทบาทสำคัญเป็นโครงสร้างพื้นฐานที่ช่วยเสริมสร้างประสิทธิภาพในกระบวนการดำเนินงานให้รองรับกลยุทธ์ทางธุรกิจ อีกทั้งการพัฒนานวัตกรรมด้านการพิมพ์ยังเป็นกลไกในการช่วยลดต้นทุนและเพิ่มศักยภาพ เพื่อสามารถให้บริการลูกค้าได้อย่างสะดวกรวดเร็ว ตอบสนองความต้องการของลูกค้าที่หลากหลายได้อย่างทั่วถึง การใช้เทคโนโลยีสารสนเทศจึงนับเป็นโจทย์ที่ท้าทาย ในปัจจุบันที่มีความผันผวนสูงและยากต่อการคาดเดา ตั้งแต่การกำหนดยุทธศาสตร์ในการพัฒนาเทคโนโลยีสารสนเทศ เพื่อเป็นตัวขับเคลื่อนธุรกิจ รวมทั้งการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีที่ต้องปรับตัวให้เท่าทัน และความเสี่ยงในการเผชิญภัยคุกคามทางไซเบอร์ที่นับวันมีแนวโน้มเพิ่มขึ้นมีวิวัฒนาการที่ซับซ้อนขึ้น ส่งผลกระทบที่มีความรุนแรงและเป็นวงกว้างมากขึ้น ดังเช่น เหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

จึงเห็นได้ว่าปัจจุบันโรงพิมพ์ตำรวจ กำลังเผชิญกับความเสี่ยงด้านเทคโนโลยีสารสนเทศในหลายมิติมากขึ้น หากไม่มีการปรับตัวให้เท่าทันกับการเปลี่ยนแปลง หรือไม่มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เพียงพอ อาจนำไปสู่ความเสี่ยงด้านอื่นที่สำคัญด้วย โดยปัจจุบันความเสี่ยงด้านเทคโนโลยีสารสนเทศไม่เป็นเพียงส่วนหนึ่งของความเสี่ยงด้านปฏิบัติการอีกต่อไป แต่กลายเป็นหนึ่งในความเสี่ยงทางธุรกิจที่สำคัญที่สามารถส่งผลกระทบต่อความเชื่อมั่นของลูกค้าที่มีต่อการให้บริการ รวมทั้งอาจส่งผลกระทบต่อกลยุทธ์ทางธุรกิจ การปฏิบัติตามกฎระเบียบต่าง ๆ ภาพลักษณ์ ชื่อเสียงของโรงพิมพ์ตำรวจจึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบและต่อเนื่อง ซึ่งโรงพิมพ์ตำรวจตระหนักถึงความสำคัญและความจำเป็นในการยกระดับความพร้อมรับมือต่อความเสี่ยงที่โรงพิมพ์ตำรวจกำลังเผชิญ เพื่อให้โรงพิมพ์ตำรวจมีการกำกับดูแลและบริหารจัดการทรัพยากรเทคโนโลยีสารสนเทศทั้งบุคลากร กระบวนการ และการนำเทคโนโลยีสารสนเทศมาใช้ภายใต้การบริหารความเสี่ยงอย่างเหมาะสมและเพียงพอรองรับตามระดับความเสี่ยงที่โรงพิมพ์ตำรวจมี โดยเริ่มตั้งแต่คณะกรรมการโรงพิมพ์ตำรวจ และผู้บริหารระดับสูงที่ให้ ความสำคัญในการผลักดันและยกระดับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยสร้างวัฒนธรรมและพฤติกรรมร่วมของทุกคนในองค์กรให้ตระหนักถึงความเสี่ยงอย่างรอบด้าน และเป็นรูปธรรม การสร้างธรรมาภิบาลที่ดีในองค์กรโดยมีโครงสร้างและบทบาทหน้าที่ความรับผิดชอบอย่างเหมาะสม การกำหนดกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ชัดเจน เพื่อให้มีการประเมิน และติดตามความเสี่ยง อย่างต่อเนื่อง และเท่าทันกับความเสี่ยงรูปแบบใหม่ที่อาจเกิดขึ้น การขับเคลื่อนธุรกิจโดยคำนึงถึงการใช้เทคโนโลยี สารสนเทศอย่างเหมาะสมและปลอดภัย รวมถึง การดูแลให้มี บุคลากรของโรงพิมพ์ตำรวจมีความรู้ความเชี่ยวชาญอย่างเพียงพอ

หลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สรุปหลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีดังนี้

1. การใช้เทคโนโลยีสารสนเทศสอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจและการเปลี่ยนแปลง

ปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการดำเนินธุรกิจของสถาบันการเงินมากขึ้น โดยเป็นโครงสร้างพื้นฐานที่สำคัญที่รองรับกลยุทธ์ในการดำเนินธุรกิจ ช่วยเพิ่มประสิทธิภาพ ลดต้นทุนในการดำเนินงาน และเพิ่มศักยภาพในการแข่งขัน ตอบสนองต่อความต้องการของลูกค้าที่ต้องการผลิตภัณฑ์และบริการที่หลากหลายได้อย่างสะดวกและรวดเร็ว นอกจากนี้โรงพิมพ์ตำรวจยังต้องเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศให้พร้อมรับการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็วเพื่อรองรับการดำเนินธุรกิจในอนาคต

2. คณะกรรมการโรงพิมพ์ตำรวจ และผู้บริหารระดับสูงมีบทบาทสำคัญในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องมีการกำกับดูแลในระดับองค์กร โดยเป็นความรับผิดชอบ ของคณะกรรมการโรงพิมพ์ตำรวจ ที่ต้องสนับสนุนและผลักดันให้องค์กรมีกลยุทธ์และนโยบายด้านเทคโนโลยีสารสนเทศที่เพิ่มประสิทธิภาพให้แก่การดำเนินธุกิจ ความสามารถในการแข่งขัน มีความมั่นคงปลอดภัยและพร้อมรับมือภัยคุกคามทางเทคโนโลยีและภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมทั้งผลักดันให้องค์กรมีการสร้างความตระหนักในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness) อย่างต่อเนื่องและมีประสิทธิภาพ

3. ความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงในระดับองค์กร (enterprise wide risk)

เนื่องจากเทคโนโลยีสารสนเทศกลายเป็นโครงสร้างพื้นฐานสำคัญรองรับกระบวนการทางธุรกิจและการปฏิบัติงาน ด้านต่าง ๆ ของโรงพิมพ์ตำรวจ ดังนั้นการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ไม่ได้เป็นความรับผิดชอบอยู่เพียงหน่วยงาน ด้านเทคโนโลยีสารสนเทศเท่านั้น แต่เป็นเรื่องที่บุคลากรทุกระดับและทุกฝ่ายในองค์กรต้องให้ความตระหนักและมีแนวทางการบริหารความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศครอบคลุมทั้งในเชิงกลยุทธ์และเชิงปฏิบัติการเพื่อให้มีการป้องกัน ติดตาม และรับมือความเสี่ยงที่อาจเกิดขึ้น ด้วยเหตุนี้โรงพิมพ์ตำรวจ จำเป็นต้องมีกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างครอบคลุมทั่วทั้งองค์กรและเหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ โดยครอบคลุมการกำหนดนโยบายและบทบาท หน้าที่ความรับผิดชอบ การพัฒนากระบวนการและเครื่องมือ รวมถึงการพัฒนาความรู้และความเชี่ยวชาญในด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเพียงพอและทั่วถึง

4. มีการกำกับดูแลเป็นไปตามหลัก 3 lines of defence

โครงสร้างการกำกับดูแลการปฏิบัติงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศจำเป็นต้องสอดคล้อง ตามหลัก 3 lines of defence เพื่อให้สอดคล้องตามหลักการถ่วงดุล (check and balance) และมีการแบ่งแยกหน้าที่ ความรับผิดชอบอย่างชัดเจน (segregation of duties) ในการปฏิบัติงานการบริหารความเสี่ยง การกำกับดูแลการปฏิบัติ ตามกฎหมายและหลักเกณฑ์ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ

5. การรักษาความมั่นคงปลอดภัยและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศสอดคล้องกับความเสี่ยงที่เพิ่มขึ้น

ความเสี่ยงที่เกิดจากเทคโนโลยีสารสนเทศหากไม่ได้รับการบริหารจัดการและควบคุมอย่างเพียงพออาจทำให้เกิดช่องโหว่ด้านการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบในการให้บริการ แก่ธุรกิจและการดำเนินงานของโรงพิมพ์ตำรวจ ซึ่งอาจนำไปสู่ความเสี่ยงด้านความน่าเชื่อถือ ชื่อเสียง ภาพลักษณ์ การปฏิบัติ ตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

6. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศอย่างรัดกุมและมีประสิทธิภาพ

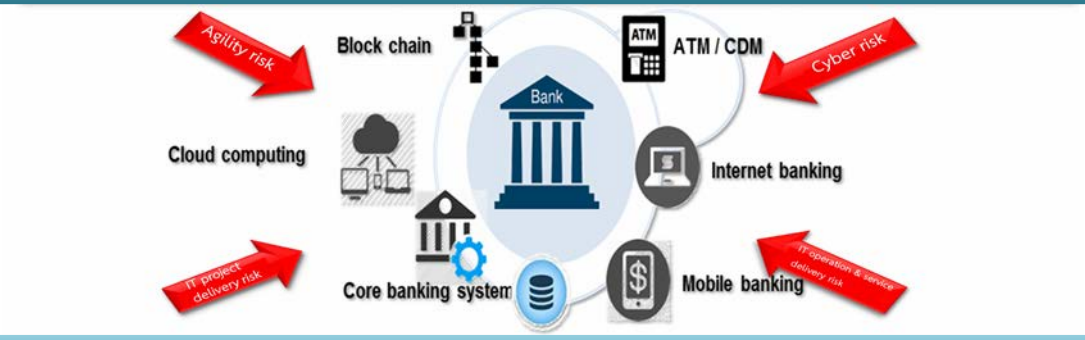
ความต้องการของลูกค้าที่ต้องการผลิตภัณฑ์และบริการที่หลากหลาย รวมทั้งการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศที่เป็นไปอย่างรวดเร็ว ทำให้โรงพิมพ์ตำรวจต้องบริหารจัดการทรัพยากรที่มีอยู่อย่าง จำกัดให้มีประสิทธิภาพสูงสุด ดังนั้น หากโรงพิมพ์ตำรวจไม่สามารถบริหารจัดการโครงการพัฒนาระบบได้อย่างมีประสิทธิภาพ ทำให้ไม่สามารถส่งมอบโครงการได้ตามเป้าหมายที่กำหนด ส่งผลให้เกิดความเสี่ยงที่โครงการด้านเทคโนโลยีสารสนเทศไม่แล้วเสร็จตามกำหนดเวลา โครงการไม่มีคุณภาพ รวมถึงโครงการไม่สอดรับกับกลยุทธ์ทางธุรกิจของโรงพิมพ์ตำรวจ นอกจากนี้ในบางกรณีอาจส่งผลให้โรงพิมพ์ตำรวจไม่สามารถปฏิบัติได้ตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องของผู้กำกับดูแลได้

7. มีการพัฒนาความรู้ความสามารถ (capability) ของบุคลากร

ด้วยวิวัฒนาการของเทคโนโลยีและความเสี่ยงซึ่งมีความซับซ้อนมากขึ้นโรงพิมพ์ตำรวจจำเป็นต้องมีการพัฒนาความรู้ด้านเทคโนโลยีอย่างต่อเนื่อง เพื่อเพิ่มมุมมองความรู้และความเชี่ยวชาญของบุคลากรในการระบุ ประเมิน ควบคุม ติดตาม และรับมือความเสี่ยงจากภัยที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ นอกจากนี้ การดำเนินธุรกิจในยุคดิจิทัล ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศไม่ได้จำกัดอยู่เพียงระดับปฏิบัติการเท่านั้น แต่ยังส่งผลต่อการดำเนินกลยุทธ์ของธุรกิจ ดังนั้น คณะกรรมการ ผู้บริหารระดับสูง และบุคลากรทุกระดับจึงจำเป็นต้องได้รับการพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศและความเสี่ยงต่อธุรกิจรวมถึงติดตามภัยคุกคามทางไซเบอร์ เพื่อให้มีความรู้เท่าทันภัยคุกคามใหม่ ๆ

แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

โรงพิมพ์ตำรวจ กำลังเผชิญความเสี่ยงที่เกี่ยวข้องกับดทคโนโลยีสารสนเทศ



การเปลี่ยนแปลงสภาพแวดล้อมทางธุรกิจและเทคโนโลยีอย่างรวดเร็ว

สภาพแวดล้อมการเปลี่ยนแปลงธุรกิจเป็นไปอย่างรวดเร็ว มีการนำนวัตกรรมและเทคโนโลยีใหม่มาใช้ในการเพิ่มประสิทธิภาพและปรับปรุงผลิตภัณฑ์ การบริหารลูกค้าในหลากหลายรูปแบบ ซึ่งโรงพิมพ์ตำรวจต้องมีการเตรียมการให้เท่าทันกับการเปลี่ยนแปลงในมิติต่างๆ เพื่อพร้อมแข่งขันในตลาดธุรกิจด้านการพิมพ์

ภัยคุกคามทางไซเบอร์ มีแนวโน้มเพิ่มขึ้นและซับซ้อนมากขึ้น

ภัยคุกคามทางไซเบอร์ ปัจจุบันมีแนวโน้มที่เพิ่มมากขึ้น ซับซ้อนมากขึ้น และแพร่กระจายได้อย่างรวดเร็ว โรงพิมพ์ตำรวจจึงจำเป็นต้องจัดให้มีมาตรการความปลอดภัยที่รัดกุม และเตรียมการให้พร้อมรับมือภัยคุกคามรูปแบบต่าง ๆ ที่อาจเกิดขึ้นเพื่อความมั่นคงปลอดภัยของโรงพิมพ์ตำรวจ และลูกค้า รวมทั้งเพื่อช่วยลดความเสี่ยงและผลกระทบเมื่อเกิดเหตุ

ความเสี่ยงด้านปฏิบัติการ IT ที่รองรับการดำเนินธุรกิจ

ระบบ IT ถือเป็นโครงสร้างพื้นฐานหลักที่ใช้รองรับการให้บริการของโรงพิมพ์ตำรวจ ซึ่งหากมีการบริหารจัดการและควบคุม ทั้งด้านบุคลากร กระบวนการ และระบบที่ไม่เพียงพอ อาจทำให้เกิดช่องโหว่ต่อการรักษาความปลอดภัย ความถูกต้อง เชื่อถือได้ของระบบและข้อมูล รวมถึงความพร้อมใช้งานของระบบในการให้บริการ

การบริหารจัดการโครงการด้าน IT มีผลกระทบต่อการดำเนินธุรกิจ

โรงพิมพ์ตำรวจมีการลงทุนโครงการด้าน IT ซึ่งต้องใช้ทรัพยากรทั้งเงินทุน บุคลากร และระยะเวลาในการดำเนินโครงการเพื่อบรรลุตามโรงพิมพ์ตำรวจ ซึ่งหากโรงพิมพ์ตำรวจไม่สามารถบริหารจัดการโครงการได้อย่างมีประสิทธิภาพ รวมถึงไม่มีการกำกับดูแล และควบคุมติดตามการบริการโครงการอย่างเพียงพอ อาจทำให้โครงการไม่สำเร็จลุล่วงตามแผน และเป้าหมายที่กำหนดจนส่งผลกระทบต่อการดำเนินธุรกิจของโรงพิมพ์ตำรวจ

ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

1. การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของโรงพิมพ์ตำรวจ

วัตถุประสงค์ เพื่อให้คณะกรรมการของโรงพิมพ์ตำรวจกำกับดูแลและสนับสนุนให้องค์กรมีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเพียงพอเหมาะสมและสอดคล้องกับการดำเนินธุรกิจ

1.1.1 คณะกรรมการโรงพิมพ์ตำรวจประกอบด้วยกรรมการที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ อย่างน้อย 1 ท่าน เพื่อให้คณะกรรมการโรงพิมพ์ตำรวจสามารถกำหนดทิศทางและกำกับดูแลให้โรงพิมพ์ตำรวจมีการใช้เทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์การดำเนินธุรกิจของโรงพิมพ์ตำรวจ มีความรู้เท่าทันความเสี่ยงและพัฒนาการด้านเทคโนโลยีที่เปลี่ยนแปลงไป

1.1.2 ดูแลให้มีการใช้เทคโนโลยีที่สอดรับกับกลยุทธ์ในการดำเนินธุรกิจของโรงพิมพ์ตำรวจ และดูแลให้การใช้เทคโนโลยีให้มีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต

1.1.3 ดูแลให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในฐานะที่เป็นความเสี่ยงที่สำคัญโดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของโรงพิมพ์ตำรวจ

1.1.4 ดูแลให้มีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งรวมถึงนโยบายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยนโยบายดังกล่าวต้องสอดคล้องกับลักษณะ การดำเนินธุรกิจ ความซับซ้อนของเทคโนโลยีสารสนเทศและความเสี่ยงที่เกี่ยวข้อง รวมทั้งทำหน้าที่ในการอนุมัตินโยบายดังกล่าวด้วย

1.1.5 ดูแลให้มีมาตรฐาน ระเบียบวิธีปฏิบัติ กระบวนการ เครื่องมือ และบุคลากรในการรักษาความมั่นคงปลอดภัย และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายข้อ 1.1.4 รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและประเมินประสิทธิภาพนโยบายดังกล่าวอย่างน้อย ปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.1.6 ดูแลให้มีการติดตาม ตรวจสอบ และรายงานต่อคณะกรรมการโรงพิมพ์ตำรวจ คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงของโรงพิมพ์ตำรวจอย่างเหมาะสม ในเรื่องที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น ผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของโรงพิมพ์ตำรวจ ข้อมูลเกี่ยวกับปัญหาหรือเหตุการณ์ทางด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของโรงพิมพ์ตำรวจ

1.1.7 ดูแลและสนับสนุนให้มีการสื่อสารกับบุคลากรของ โรงพิมพ์ตำรวจ เพื่อให้ตระหนักถึงความสำคัญของความเสี่ยงและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งเข้าใจการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เพื่อช่วยลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.1.8 คณะกรรมการโรงพิมพ์ตำรวจ ต้องได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศอย่างเพียงพอตามระยะเวลาที่เหมาะสม เพื่อให้มีความรู้ความเข้าใจด้านเทคโนโลยีสารสนเทศที่เพียงพอต่อการกำกับดูแลและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ ให้ทันกับภัยคุกคามใหม่ รวมถึงการพิจารณาเชิงกลยุทธ์ในการนำเทคโนโลยีมาใช้ในการขับเคลื่อนธุรกิจ

1.2 โครงสร้างการกำกับดูแล

วัตถุประสงค์ เพื่อให้มีโครงสร้างและบทบาทหน้าที่ในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมสอดคล้องตามหลัก 3 lines of defence

คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.2.1 โรงพิมพ์ตำรวจควรจัดตั้งคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึง การถ่วงดุลอ านาจอย่างเป็นอิสระ อย่างน้อยครอบคลุม

• คณะกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

(เช่น คณะอนุกรรมการด้านสารสนเทศ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนด กลยุทธ์ นโยบาย และแผนงานด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์ของโรงพิมพ์ตำรวจ รวมทั้งกำกับดูแลและติดตามการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนี้โรงพิมพ์ตำรวจอาจพิจารณาให้มีโรงพิมพ์ตำรวจ ที่ดูแลงานเฉพาะด้านเพิ่มเติม หากเห็นว่างานดังกล่าวมีนัยสำคัญ หรือมีผลกระทบสูงต่อโรงพิมพ์ตำรวจ เช่น คณะกรรมการหรืออนุกรรมการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

• คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(เช่น คณะอนุกรรมการบริหารความเสี่ยง หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งกำกับดูแลและติดตามให้เป็นไปตามนโยบายที่กำหนดไว้ โดยมีการเชื่อมโยงกับความเสี่ยงในภาพรวมของโรงพิมพ์ตำรวจ (enterprise risk management)

• คณะกรรมการกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ

(เช่น คณะกรรมการตรวจสอบ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อให้โรงพิมพ์ตำรวจมีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเป็นอิสระ ครอบคลุมถึงการปฏิบัติงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

โครงสร้างองค์กร

1.2.2 โรงพิมพ์ตำรวจ ควรจัดให้มีโครงสร้างองค์กรและหน้าที่ความรับผิดชอบเป็นลายลักษณ์อักษร โดยสอดคล้องตามหลักการถ่วงดุล (check and balance) และการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจน ระหว่างการทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ

1.2.3 โรงพิมพ์ตำรวจ ควรดูแลให้มีทรัพยากรเพียงพอที่จะสนับสนุนการปฏิบัติงาน การบริหารความเสี่ยง การกำกับดูแล การปฏิบัติตามกฎหมายและหลักเกณฑ์ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น จัดให้มีบุคลากร ที่มีความรู้ความเชี่ยวชาญและมีเครื่องมือหรือระบบที่ช่วยสนับสนุนการปฏิบัติงาน เป็นต้น

1.2.4 โรงพิมพ์ตำรวจ อาจพิจารณาจัดให้มีผู้บริหารระดับสูงหรือหัวหน้าสายงานที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ (IT security) โดยควรมีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และควรเป็นผู้ที่มีความรู้ความสามารถด้านเทคโนโลยีสารสนเทศและด้านการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ เช่น ได้รับการรับรองความรู้ความสามารถ ตามมาตรฐานสากล เป็นต้น

1.2.5 หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ใช้งานระบบเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 1st line of defence) เช่น หน่วยงานด้านเทคโนโลยีสารสนเทศ หน่วยงานอื่นที่เป็นผู้ใช้งานระบบ เป็นต้น

• หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ มีหน้าที่ปฏิบัติงานตามที่ได้รับมอบหมาย รวมทั้งประเมินความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ จัดให้มีแนวทางการควบคุมติดตาม และรายงานการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายและผู้บริหารระดับสูงที่เกี่ยวข้อง อย่างน้อยครอบคลุม

- รายงานผลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations) เช่น สถานะความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศ เหตุการณ์ผิดปกติ และปัญหาด้านเทคโนโลยีสารสนเทศ ระดับการให้บริการงานด้านเทคโนโลยีสารสนเทศ เป็นต้น

- รายงานความคืบหน้า ปัญหา และอุปสรรคในการดำเนินโครงการด้านเทคโนโลยีสารสนเทศ ในภาพรวมและรายโครงการที่สำคัญ

- รายงานการติดตามและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งแนวโน้มความเสี่ยงและภัยคุกคามที่อาจจะเกิดขึ้นและส่งผลกระทบต่อโรงพิมพ์ตำรวจ

- รายงานผลการประเมินความเสี่ยง การติดตามความเสี่ยง และแนวทางการควบคุมที่เกี่ยวข้อง

- รายงานความคืบหน้าการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

- รายงานผลการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก

• ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ มีหน้าที่ปฏิบัติตามนโยบายและระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งมีส่วนร่วมรับผิดชอบในการประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องจากการใช้งานระบบ

1.2.6 หน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 2nd line of defence) เช่น คณะทำงานบริหารความเสี่ยง และหน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและ หลักเกณฑ์ เป็นต้น

• หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง มีหน้าที่กำหนดกรอบและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สนับสนุนให้มีการประเมินความเสี่ยงเป็นไปตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยงและทบทวนการควบคุมความเสี่ยงด้านเทคโนโลยี สารสนเทศให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ของหน่วยงานที่ทำหน้าที่เป็น 1st line of defence โดยมีการรวบรวมและเชื่อมโยงความเสี่ยงด้านเทคโนโลยีสารสนเทศกับความเสี่ยงด้านอื่นของโรงพิมพ์ตำรวจ และนำสนอผลการบริหารความเสี่ยงต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยง

• หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ มีหน้าที่กำหนดกระบวนการติดตามดูแล ให้คำปรึกษา สอบทาน และรายงานการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง และนำเสนอต่อคณะกรรมการที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยระบบการชำระเงิน เป็นต้น เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

1.2.7 หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 3rd line of defence) ซึ่งอาจเป็นผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น หน่วยงานตรวจสอบภายใน เป็นต้น

• หน่วยงานที่ทำหน้าที่ตรวจสอบ มีหน้าที่ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงของหน่วยงานที่ทำหน้าที่ 1st line และ 2nd line of defence รวมถึงงานอื่น ๆ ที่เกี่ยวข้อง เช่น การใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ เป็นต้น เพื่อสอบทานให้มั่นใจว่า มีการปฏิบัติที่เป็นไปตามนโยบาย มาตรฐาน และระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศ

• กรณี โรงพิมพ์ตำรวจ มีข้อจำกัดด้านบุคลากรที่ไม่เพียงพอหรือมีความรู้ความเชี่ยวชาญด้านการตรวจสอบเทคโนโลยีสารสนเทศที่ไม่เพียงพอ อาจพิจารณาว่าจ้างผู้ตรวจสอบภายนอกที่มีความเป็นอิสระ และได้รับมาตรฐานสากลที่ยอมรับโดยทั่วไปในการตรวจสอบเทคโนโลยีสารสนเทศ ดำเนินการแทนได้

• มีกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมอย่างน้อย ดังนี้

- การวางแผนงานและกำหนดขอบเขตการตรวจสอบ (planning and scoping) ครอบคลุม และสอดคล้องกับความสำคัญและความเสี่ยงของการใช้งานเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยแผนงานและขอบเขตการตรวจสอบต้องได้รับความเห็นชอบจากคณะกรรมการตรวจสอบ และมีการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

- การตรวจสอบ (execution) อย่างน้อยปีละ 1 ครั้งตามแผนงานและขอบเขตที่กำหนด และพิจารณาให้มีการตรวจสอบเมื่อมีเหตุการณ์ผิดปกติในงานด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ นอกจากนี้แนวทางการตรวจสอบควรเป็นไปตามมาตรฐานที่โรงพิมพ์ตำรวจกำหนด ซึ่งสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องรวมถึงมาตรฐานสากลที่ยอมรับโดยทั่วไป

- การวิเคราะห์ (analysis) นำข้อมูลที่ได้จากการตรวจสอบมาวิเคราะห์ เพื่อสรุปผลการตรวจสอบ และอาจพิจารณาการขยายขอบเขตการตรวจสอบเพิ่มเติม หากมีความจำเป็น เช่น พบข้อบ่งชี้ถึงความเสี่ยงที่อาจกระทบต่อโรงพิมพ์ตำรวจ อย่างมีนัยสำคัญ

- การรายงานและติดตามผลการตรวจสอบ (reporting and follow up) มีการสรุปผลการตรวจสอบและประเด็นที่ต้องแก้ไขกับผู้บริหารของหน่วยงานผู้รับตรวจและจัดทำรายงานผลการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการตรวจสอบและแจ้งให้ผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบ ตลอดจนจัดเก็บรายงานผลการตรวจสอบไว้ที่โรงพิมพ์ตำรวจ พร้อมไว้สำหรับการตรวจสอบ นอกจากนี้โรงพิมพ์ตำรวจต้องจัดให้มีการติดตามการแก้ไข ประเด็นที่ตรวจพบภายในระยะเวลาที่กำหนดและรายงานต่อคณะกรรมการตรวจสอบ

• โรงพิมพ์ตำรวจ ควรจัดให้มีผู้เชี่ยวชาญภายนอกที่เป็นอิสระทำหน้าที่ประเมินระบบหรือเทคโนโลยีที่มีความสำคัญ ซึ่งโรงพิมพ์ตำรวจเห็นว่ามีความจำเป็นต้องประเมิน แต่มีข้อจำกัดหรือผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจไม่สามารถประเมินได้ เช่น การประเมินระบบที่มีความซับซ้อนหรือมีการใช้เทคโนโลยีใหม่ หรือการประเมินความสามารถของระบบในการปรับเปลี่ยนเพื่อรองรับการทำธุรกิจของโรงพิมพ์ตำรวจในอนาคต ภายใต้สภาวะการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็ว

1.3 การบริหารจัดการบุคลากร

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีบุคลากรที่มีความรู้และความเชี่ยวชาญเพียงพอในการปฏิบัติงานที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศ โดยบุคลากรทุกระดับมีความตระหนักถึงการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศของ โรงพิมพ์ตำรวจ

1.3.1 มีกระบวนการบริหารจัดการบุคลากรอย่างเหมาะสม ครอบคลุม การคัดเลือกบุคลากรที่มีความรู้ความสามารถเพียงพอ การว่าจ้างบุคลากรที่เป็นไปตามข้อกำหนดหรือเงื่อนไขด้านความปลอดภัยเทคโนโลยีสารสนเทศ การพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ การเปลี่ยนแปลงหรือสิ้นสุดการว่าจ้างบุคลากร รวมทั้งการดูแลบุคลากรให้เพียงพอกับปริมาณการใช้เทคโนโลยีสารสนเทศ

1.3.2 โรงพิมพ์ตำรวจ อาจพิจารณาการได้รับการรับรองความรู้ความสามารถตามมาตรฐานที่รับรองทั่วไป (certificate) เฉพาะด้านที่เกี่ยวข้องกับงานด้านเทคโนโลยีสนเทศ เพื่อให้ได้บุคลากรที่มีคุณสมบัติเหมาะสม มีความรู้ หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

1.3.3 หน่วยงานทรัพยากรบุคคล ควรตรวจสอบประวัติของบุคลากรก่อนการว่าจ้างตามความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ เช่น ประวัติการศึกษา ประวัติการทำงาน ประวัติอาชญากรรม เป็นต้น

1.3.4 มีข้อกำหนดหรือเงื่อนไขการว่าจ้างงาน โดยกล่าวถึงบทบาทหน้าที่ความรับผิดชอบ การปฏิบัติตามนโยบาย และข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ

1.3.5 ให้บุคลากรและผู้ให้บริการภายนอกที่ได้รับการว่าจ้างทำความเข้าใจ รับทราบและลงนามยอมรับเงื่อนไข การว่าจ้างงาน นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ และข้อตกลง การไม่เปิดเผยข้อมูลก่อนเริ่มปฏิบัติงาน

1.3.6 กำหนดโปรแกรมการอบรมและพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ (training program) ที่ครอบคลุมการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ให้แก่บุคลากรทุกระดับ โดยมีการวัดประสิทธิผล ของหลักสูตรฝึกอบรมที่จัดขึ้น เช่น

• หลักสูตรฝึกอบรมบุคลากรที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (1st line of defence) ให้มีความรู้ และความเชี่ยวชาญที่เพียงพอต่อการปฏิบัติงานและการใช้งาน

• หลักสูตรฝึกอบรมบุคลากรที่เกี่ยวข้องกับงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (2nd line of defence) และการตรวจสอบด้านเทคโนโลยีสารสนเทศ (3rd line of defence) ให้มีความรู้และความเชี่ยวชาญเพียงพอที่จะระบุ ประเมิน และให้ข้อเสนอแนะในการปรับปรุงประสิทธิภาพของการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่หน่วยงานที่ทำหน้าที่ 1st line of defence

1.3.7 กำหนดโปรแกรมในการเสริมสร้างความตระหนัก (awareness program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น โดยโปรแกรมดังกล่าวควรครอบคลุมตั้งแต่ระดับคณะกรรมการ ผู้บริหาร ระดับสูง และบุคลากรทุกระดับ รวมถึงบุคคลภายนอกที่เกี่ยวข้อง รวมทั้งมีการจัดกิจกรรมเสริมสร้างความตระหนักอย่างต่อเนื่อง นอกจากนี้โรงพิมพ์ตำรวจ ควรจัดให้มีการประชาสัมพันธ์เพื่อสร้างความรู้หรือสร้างความตระหนักในการใช้งานบริการทางอิเล็กทรอนิกส์อย่างปลอดภัย ให้แก่ลูกค้าของโรงพิมพ์ตำรวจ ทราบอย่างสม่ำเสมอด้วย

1.3.8 มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงาน เช่น การคืนสินทรัพย์ของโรงพิมพ์ตำรวจ การบริหารจัดการสิทธิ์ต้องมีการปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องมีการสื่อสารให้ผู้เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ์หน้าที่ และความรับผิดชอบ เป็นต้น

1.4 นโยบายที่เกี่ยวข้องกับการก ากับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและ สอดคล้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ

1.4.1 โรงพิมพ์ตำรวจ ควรกำหนดให้มีนโยบายเป็นลายลักษณ์อักษรและอยู่ใต้กรอบหลักการที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และ ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ อย่างน้อยครอบคลุมนโยบายดังต่อไปนี้

• นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

• นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

• นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ

1.4.2 นโยบายดังกล่าวควรสอดคล้องกับกลยุทธ์ในการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจ นโยบายการบริหารความเสี่ยงของโรงพิมพ์ตำรวจ รวมทั้งสอดคล้องกับแนวทางบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัย ตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

1.4.3 นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการของโรงพิมพ์ตำรวจ และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งควรจัดให้มีการชี้แจงและสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและมีการควบคุมดูแลให้มีการปฏิบัติตามนโยบายได้อย่างถูกต้องครบถ้วน

1.4.4 นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ควรรวมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมอย่างน้อย

• การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
• การรักษาความมั่นคงปลอดภัยของข้อมูล
• การควบคุมการเข้าถึง
• การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
• การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร
• การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
• การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ
• การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ
• การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
• การบริหารจัดการผู้ให้บริการภายนอก

1.4.5 นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมอย่างน้อย

• โครงสร้างองค์กร บทบาทหน้าที่ของผู้เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

• จัดทำหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

(1) การประเมินความเสี่ยง (risk assessment)

(1.1) การระบุความเสี่ยง (risk identification)

โรงพิมพ์ตำรวจ ควรจัดให้มีการระบุเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้น หรือที่เกิดขึ้นจริง รวมถึงภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ ที่ส่งผลกระทบต่อการดำเนินธุรกิจของโรงพิมพ์ตำรวจ โดยเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรระบุ อย่างน้อยครอบคลุม

• ผู้กระทำให้เกิดความเสี่ยงและเหตุการณ์ความเสี่ยง เช่น ผู้ไม่ประสงค์ดี ภัยคุกคาม หรือช่องโหว่ เป็นต้น

• ประเภทของความเสี่ยง เช่น ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ ความเสี่ยงด้านโปรแกรม ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงด้านการบริหารโครงการ เป็นต้น

• วัน เวลา สถานที่ ช่วงเวลาหรือระยะเวลาที่เกิดเหตุการณ์ผิดปกติหรือความเสี่ยง ด้านเทคโนโลยีสารสนเทศ (ถ้ามี)

• สาเหตุของการเกิดเหตุการณ์ เช่น กระบวนการปฏิบัติงาน ระบบงาน บุคลากร ปัจจัยภายนอก เป็นต้น

• ผลกระทบต่อทรัพย์สิน ทรัพยากร การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และการดำเนินธุรกิจของโรงพิมพ์ตำรวจ

ทั้งนี้ ผู้ที่มีส่วนร่วมในการระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศควรมีความรู้ และความเข้าใจถึงเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ได้ระบุไว้เป็นอย่างดี

(1.2) การวิเคราะห์ความเสี่ยง (risk analysis)

โรงพิมพ์ตำรวจ ควรจัดให้มีการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม โดยควรดำเนินการ ดังนี้

• กำหนดเจ้าของความเสี่ยงด้านเทคโนโลยีสารสนเทศ (risk owner)

• ระบุการควบคุมที่มีอยู่ในปัจจุบัน (existing control)

• พิจารณาและค้นหาสาเหตุและสถานการณ์ที่เป็นไปได้

• วิเคราะห์ผลกระทบที่เกิดขึ้นจากเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(1.3) การประเมินค่าความเสี่ยง (risk evaluation)

โรงพิมพ์ตำรวจ ควรประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ เพื่อจัดลำดับในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยควรดำเนินการ ดังนี้

• กำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบ เช่น ด้านการเงิน ด้านปฏิบัติการ เป็นต้น

• กำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)

• ประเมินค่าโอกาสและผลกระทบของเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น เพื่อระบุ ระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

• จัดลำดับความเสี่ยงด้านเทคโนโลยีสารสนเทศแสดงในแผนภาพความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2) การจัดการความเสี่ยง (risk treatment)

โรงพิมพ์ตำรวจ ควรจัดให้มีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรครอบคลุมอย่างน้อย ดังนี้

• กำหนดแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการเลือก แนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมสำหรับโรงพิมพ์ตำรวจ เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง การลดหรือบรรเทาโอกาสเกิดความเสี่ยง การลดหรือบรรเทาผลกระทบที่เกิดขึ้น การแบ่ง หรือโอนความเสี่ยงให้หน่วยงานอื่น การยอมรับความเสี่ยงไว้โดยแจ้งเหตุผลให้ผู้บริหารทราบ เพื่อตัดสินใจในการยอมรับความเสี่ยง เป็นต้น

• ระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ ระยะเวลาที่ใช้ในการดำเนินการ

• ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้

• จัดทำแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดลำดับความสำคัญ ในการดำเนินการ

• นำเสนอและขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

• ดำเนินการสื่อสารแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

นอกจากนี้โรงพิมพ์ตำรวจควรจัดให้มีการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ให้สอดคล้องกับความสำคัญของงานเทคโนโลยีสารสนเทศ แต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

(3) การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

โรงพิมพ์ตำรวจ ควรกำหนดผู้รับผิดชอบและจัดให้มีกระบวนการในการติดตามดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศตามที่กำหนดและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรจัดให้มีการจัดเก็บและบันทึกข้อมูลอย่างเป็นระบบ เพื่อใช้ติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพ ครอบคลุมอย่างน้อย

• การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

• ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อ จำกัดที่เกิดขึ้น

• ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นกับโรงพิมพ์ตำรวจ และองค์กรอื่น

• รายงานความคืบหน้าของแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามรอบที่กำหนด

(4) การรายงานความเสี่ยง (risk reporting)

โรงพิมพ์ตำรวจ ควรจัดให้มีกระบวนการนำเสนอผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ พร้อมทั้งรายงานผลการประเมินและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยเชื่อมโยง กับความเสี่ยงในระดับองค์กร รวมทั้งรายงานแนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้น ต่อคณะกรรมการโรงพิมพ์ตำรวจ หรือโรงพิมพ์ตำรวจ ที่ได้รับมอบหมาย อย่างน้อยไตรมาสละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าโรงพิมพ์ตำรวจมีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและต่อเนื่อง โดยการรายงานควรครอบคลุมอย่างน้อย

• สถานะและผลลัพธ์การดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศประจำปี

• ผลการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับ ความเสี่ยงในระดับองค์กร

• รายงานดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ และรายงานสรุปเหตุการณ์ผิดปกติ

• แนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นกับโรงพิมพ์ตำรวจ

• ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง

ทั้งนี้ โรงพิมพ์ตำรวจ ควรจัดให้มีการทบทวนหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.4.6 นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT outsourcing policy) โดยครอบคลุมอย่างน้อย

• หลักเกณฑ์การแบ่งประเภทของการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

• แนวทางการบริหารจัดการความเสี่ยง แนวทางการคัดเลือกผู้ให้บริการ และแนวทางการประเมิน ประสิทธิภาพของผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

• แนวทางการรักษาความมั่นคงปลอดภัยของระบบงานและข้อมูล

• การรายงานผลการประเมินความเสี่ยงและประสิทธิภาพการดำเนินงานของผู้ให้บริการภายนอก ด้านงานเทคโนโลยีสารสนเทศ

• การตรวจสอบผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

• การคุ้มครองผู้ใช้บริการของโรงพิมพ์ตำรวจ จากการใช้บริการผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

2. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

2.1 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างครบถ้วนและควบคุม ดูแลทรัพย์สินด้านเทคโนโลยีสารสนเทศให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

2.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ครอบคลุม การจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน

2.1.2 จัดให้มีหน่วยงานผู้รับผิดชอบในการจัดทำปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ และบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมทั้งวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน หรือสิ้นสุดการให้บริการ จากผู้ผลิตได้อย่างเหมาะสมทันการณ์

2.1.3 มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ และซอฟต์แวร์ ที่รองรับระบบเทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจ อย่างครบถ้วนและเป็นลายลักษณ์อักษร โดยครอบคลุมอย่างน้อย ดังนี้

- ชื่อเครื่องแม่ข่าย
- ชื่อระบบปฏิบัติการ (operating system) และเวอร์ชัน
- ชื่อระบบงาน (application) และเวอร์ชัน
- เจ้าของทรัพย์สิน (owner)
- ประเภทของอุปกรณ์ ยี่ห้อ รายละเอียดทางเทคนิค (specification)
- หมายเลขอ้างอิงของฮาร์ดแวร์ (serial number) และหมายเลขอ้างอิงของซอฟต์แวร์ (software license)
- สถานที่ตั้ง
- วันที่เริ่มติดตั้ง
- ประเภทการครอบครอง (ซื้อหรือเช่า)
- รายละเอียดผู้ให้บริการหรือผู้บำรุงรักษา
- วันที่บำรุงรักษาล่าสุด
- วันสิ้นสุดการใช้งานตามสัญญา (warranty) และวันสิ้นสุดการรับประกันการใช้งาน (support contract)
- วันสิ้นสุดการให้บริการจากผู้ผลิต (end of support)

2.1.4 มีการปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับทะเบียนรายการอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

2.1.5 มีกระบวนการในการยกเลิกและเรียกคืนทรัพย์สิน (return asset) เมื่อสิ้นสุดการใช้งาน ครอบคลุมทั้งทรัพย์สิน ด้านเทคโนโลยีสารสนเทศที่ใช้งานภายในโรงพิมพ์ตำรวจ และกรณีที่ผู้ให้บริการภายนอกมีการใช้งานทรัพย์สินของโรงพิมพ์ตำรวจ ทันทีที่มีการยกเลิกสัญญาจ้างด้วย

2.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีการรักษาความมั่นคงปลอดภัยและความลับของข้อมูล ครอบคลุมการรับส่งข้อมูล ผ่านเครือข่ายสื่อสาร การจัดเก็บ หรือใช้งานบนระบบ และสื่อบันทึกข้อมูลต่าง ๆ

การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

2.2.1 กำหนดให้มีเจ้าของข้อมูล (information owner) รับผิดชอบในการกำหนดผู้ใช้งาน สิทธิการเข้าถึงและ การใช้งานข้อมูลอย่างปลอดภัย

2.2.2 กำหนดหลักเกณฑ์การจัดชั้นความลับของข้อมูล (information classification) โดยควรระบุชั้นความลับ ของข้อมูล (labeling) อย่างชัดเจน

2.2.3 กำหนดแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลที่สอดคล้องตามชั้นความลับครอบคลุม

- ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint)
- ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit)
- ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest)

2.2.4 กำหนดแนวทางการควบคุมดูแลรักษาความปลอดภัยสื่อบันทึกข้อมูลระหว่างขนส่ง (physical media transfer) เพื่อให้มีการควบคุมการเข้าถึงสื่อที่มีข้อมูลสำคัญในระหว่างการขนส่ง

2.2.5 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการทำลายข้อมูล ครอบคลุม ขอบเขต หน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการทำลายข้อมูลให้สอดคล้องกับระดับความสำคัญของข้อมูล โดยมีกระบวนการควบคุมการทำลายข้อมูลที่ครอบคลุมการอนุมัติจากหน่วยงานเจ้าของข้อมูล ก่อนดำเนินการ การควบคุมการทำลายในลักษณะ dual control การสอบทานการปฏิบัติงานโดยหัวหน้างาน รวมทั้งจัดให้มีการจัดทำทะเบียนการทำลายข้อมูลสำคัญ โดยระบุผู้รับผิดชอบในการทำลายข้อมูล วันที่ เวลา ชนิดของสื่อบันทึกข้อมูล serial number และวิธีการที่ใช้ทำลายข้อมูล

การบริหารจัดการการเข้ารหัส ข้อมูล (cryptography)

2.2.6 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูล ครอบคลุม ขอบเขตหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการเข้ารหัสข้อมูลที่สอดคล้อง ตามระดับความสำคัญของข้อมูล และการบริหารจัดการกุญแจเข้ารหัสข้อมูล

2.2.7 กำหนดให้มีการเข้ารหัสข้อมูลสำคัญและช่องทางการสื่อสารที่ใช้รับส่งข้อมูลสำคัญกับภายนอก

2.2.8 วิธีการเข้ารหัสข้อมูล ควรใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล เช่น การเข้ารหัส ข้อมูลแบบสมมาตร (เช่น AES) การเข้ารหัสข้อมูลแบบอสมมาตร (เช่น public key cryptography) เป็นต้น โดยมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอ

2.2.9 การบริหารจัดการกุญแจเข้ารหัสข้อมูล ควรกำหนดกระบวนการที่มีความรัดกุม ปลอดภัย ครอบคลุมตั้งแต่ การสร้างและติดตั้ง การจัดเก็บ และการยกเลิกกุญแจเข้ารหัสข้อมูล

การสร้างและติดตั้งกุญแจเข้ารหัสข้อมูล

• มีการควบคุมสภาพแวดล้อมในการสร้างรหัสที่มีความรัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (Certification Authority) ที่น่าเชื่อถือ มีขั้นตอนการทำลายหลักฐานที่ใช้หลังจากสร้างกุญแจแล้วเสร็จ

• กุญแจเข้ารหัสข้อมูล จะต้องไม่มีพนักงานหรือบุคคลใดบุคคลหนึ่งรู้รหัสทั้งหมด

• กำหนดขนาดของกุญแจเข้ารหัสข้อมูลที่มีความยาวเพียงพอในการป้องกันการถูกถอดรหัส

• การแลกเปลี่ยนกุญแจต้องผ่านกระบวนการและช่องทางที่ปลอดภัย

• กำหนดไม่ให้ใช้กุญแจเข้ารหัสข้อมูลเดียวกันกับหลายระบบงาน

การจัดเก็บกุญแจเข้ารหัสข้อมูล

• มีการรักษาความปลอดภัยของกุญแจเข้ารหัสข้อมูลทั้งด้าน physical และ logical โดยใช้อุปกรณ์ รักษาความปลอดภัย หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน

• มีการสำรองข้อมูลกุญแจเข้ารหัสข้อมูล โดยวิธีการเก็บรักษากุญแจเข้ารหัสข้อมูลชุดสำรองต้องมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสข้อมูลชุดหลัก

การเปลี่ยนและเพิกถอนกุญแจเข้ารหัสข้อมูล

• กำหนดเกณฑ์และแนวทางในการเปลี่ยนและเพิกถอนกุญแจเข้ารหัสข้อมูล เช่น กรณีกุญแจหมดอายุล้าสมัย หรือไม่ปลอดภัย เป็นต้น

• กำหนดกระบวนการทำลายกุญแจ โดยต้องมั่นใจว่าไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก

2.3 การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีการบริหารจัดการบัญชีสิทธิ์สูงและสิทธิ์ของผู้ใช้งานมีประสิทธิภาพเป็นไปตามหลัก ความจำเป็นของการใช้งานและสอดคล้องกับหลักการแบ่งแยกงานด้านเทคโนโลยีสารสนเทศที่ดี โดยสามารถป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2.3.1 แนวทางการควบคุมการเข้าถึงให้โรงพิมพ์ตำรวจปฏิบัติตามแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก

2.4 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีการรักษาความมั่นคงปลอดภัยและความพร้อมใช้งานของศูนย์คอมพิวเตอร์ และพื้นที่สำคัญที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเพียงพอรองรับธุรกิจอย่างต่อเนื่อง

2.4.1 โรงพิมพ์ตำรวจ ควรจัดให้ศูนย์คอมพิวเตอร์สำรองแยกออกจากศูนย์คอมพิวเตอร์หลัก ซึ่งควรมีระยะห่างที่เพียงพอ และไม่ใช้ระบบสาธารณูปโภคจากแหล่งเดียวกัน เพื่อกระจายความเสี่ยงและป้องกันไม่ให้ได้รับผลกระทบเดียวกัน เช่น ระบบไฟฟ้าหรือระบบโทรคมนาคมขัดข้อง การประท้วงหรือจลาจล ภัยพิบัติทางธรรมชาติ เป็นต้น

2.4.2 โรงพิมพ์ตำรวจ ควรมีการรักษาสภาพแวดล้อมและการรักษาความปลอดภัยของศูนย์คอมพิวเตอร์สำรองอย่างเพียงพอ ตามนโยบายหรือมาตรฐานการรักษาความปลอดภัยของโรงพิมพ์ตำรวจ เพื่อไม่ให้ระบบเทคโนโลยีสารสนเทศที่สำคัญ มีความเสี่ยงต่อความพร้อมใช้งาน

2.4.3 แนวทางการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม ให้โรงพิมพ์ตำรวจ. ปฏิบัติตามแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices)

2.5 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีโครงสร้างของระบบเครือข่ายสื่อสารที่มั่นคงปลอดภัย มีการออกแบบระบบเครือข่าย สื่อสารที่เหมาะสมตามมาตรฐานสากล และมีการป้องกันหรือเฝ้าระวังการบุกรุกหรือภัยคุกคามในรูปแบบต่าง ๆ

2.5.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารในองค์กร และระหว่างเครือข่ายสื่อสารภายในองค์กรกับระบบเครือข่ายสื่อสารภายนอกองค์กรให้มีความมั่นคงปลอดภัย โดยควรจัดให้มีแนวทางป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหายหรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และมีกระบวนการตรวจสอบผู้ใช้งานอย่างเข้มงวด

2.5.2 แนวทางการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร ให้โรงพิมพ์ตำรวจปฏิบัติตามแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices)

2.6 การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

2.6.1 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีการบริหารจัดการการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศสอดคล้องตาม มาตรฐานสากล โดยมีการควบคุมที่รัดกุมปลอดภัยเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างครบถ้วนถูกต้อง

2.6.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร เพื่อควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศให้มีความรัดกุมเพียงพอ เช่น การนำระบบขึ้นใช้งานจริง การตั้งค่าระบบ การติดตั้ง patch บนระบบที่ให้บริการจริง เป็นต้น

2.6.1.2 กำหนดบทบาทหน้าที่และความรับผิดชอบของผู้บริหารที่ได้รับมอบหมายหรือคณะกรรมการบริหารจัดการ การเปลี่ยนแปลง (Change Advisory Board: CAB) ซึ่งควรประกอบด้วยผู้บริหารจากหน่วยงานเทคโนโลยี สารสนเทศ และหน่วยงานผู้ใช้งานเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อทำหน้าที่

ประเมินผลกระทบและพิจารณาเหตุผลความจำเป็นก่อนอนุมัติให้ดำเนินการเปลี่ยนแปลงระบบ ป้องกันการแก้ไขเปลี่ยนแปลง โดยไม่ได้รับอนุญาตและไม่ให้เกิดผลกระทบที่อาจเกิดกับระบบที่เกี่ยวข้อง โดยครอบคลุมอย่างน้อย ดังนี้

• ผลการประเมินความเสี่ยงและผลกระทบของการเปลี่ยนแปลง โดยมีหน่วยงานเจ้าของระบบและผู้มีหน้าที่เกี่ยวข้องทำการประเมินองค์ประกอบที่เกี่ยวข้อง ได้แก่ ระบบโครงสร้างพื้นฐาน เครือข่าย สื่อสาร และการเชื่อมต่อกับระบบอื่น เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้น ไม่กระทบต่อการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ ความพร้อมใช้ของระบบ

• ผลการทดสอบ เพื่อให้มั่นใจว่าระบบได้ผ่านการทดสอบอย่างครบถ้วนเหมาะสมตามมาตรฐานและระเบียบวิธีปฏิบัติของโรงพิมพ์ตำรวจ

• ข้อจำกัดหรือปัญหาต่าง ๆ ที่พบในระหว่างการทดสอบได้รับการแก้ไขอย่างเหมาะสม

• แผนย้อนกลับ (roll back plan) กรณีที่ทำการเปลี่ยนแปลงไม่สำเร็จ เพื่อรองรับปัญหาขัดข้อง ระหว่างการเปลี่ยนแปลง

• ตารางเวลาการเปลี่ยนแปลงใน เพื่อบริหารทรัพยากรและลดความเสี่ยง หรือผลกระทบที่อาจเกิดขึ้น

นอกจากนี้ ผู้บริหารที่ได้รับมอบหมาย ควรมีการติดตามผลหลังการเปลี่ยนแปลงระบบ เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้นเป็นไปตามวัตถุประสงค์ที่กำหนด

2.6.1.3 ผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการการเปลี่ยนแปลงควรมีการแบ่งแยกหน้าที่อย่างเหมาะสม เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ผู้มีสิทธิ์ร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น

2.6.1.4 มีหลักเกณฑ์ในการจัดประเภทการเปลี่ยนแปลงระบบตามความเสี่ยงและความสำคัญที่ชัดเจน เช่น การเปลี่ยนแปลงมาตรฐานที่ได้รับอนุมัติเป็นการทั่วไป การเปลี่ยนแปลงที่ต้องขออนุมัติตามกระบวนการปกติ และการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน โดยโรงพิมพ์ตำรวจควรกำหนดกระบวนการและขั้นตอนในการจัดการการเปลี่ยนแปลงตามแต่ละประเภทอย่างเหมาะสม

2.6.1.5 กรณีการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน ควรมีกระบวนการในการพิจารณาความเสี่ยง และผลกระทบ รวมถึงขออนุมัติจากผู้บริหารที่ได้รับมอบหมายให้สามารถตัดสินใจได้กรณีเร่งด่วน โดยภายหลังดำเนินการให้มีการรายงานผู้บริหารที่เกี่ยวข้องได้รับทราบโดยเร็ว

2.6.1.6 คำขอการเปลี่ยนแปลง ควรได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ เพื่อให้มั่นใจได้ว่าการขอเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมจากหน่วยงานเจ้าของระบบ

2.6.1.7 มีระบบหรือทะเบียนในการจัดเก็บคำขอเปลี่ยนแปลงและเอกสารรายละเอียดที่เกี่ยวข้องเพื่อใช้ควบคุมการปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการ และสามารถใช้ในการติดตามและสอบทานการปฏิบัติงานได้

2.6.1.8 มีการจัดเก็บการเปลี่ยนแปลงของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เช่น การนำระบบขึ้นใช้งานจริง การตั้งค่าระบบ การติดตั้ง patch บนระบบที่ให้บริการจริง เป็นต้น เพื่อควบคุมความเสี่ยงในการเปลี่ยนแปลงและลดข้อผิดพลาดที่อาจเกิดขึ้น

2.6.1.9 มีการประเมินผลกระทบหรือทำการทดสอบบนระบบที่มีสภาพแวดล้อมใกล้เคียงกับระบบที่ให้บริการจริง ก่อนนำไปตั้งค่าบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

2.6.2 การบริหารจัดการการตั้งค่าระบบ (system configuration management)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีกระบวนการควบคุมการเปลี่ยนแปลงการตั้งค่าระบบที่มีความรัดกุมปลอดภัย และเป็นไปตามมาตรฐาน

2.6.2.1 จัดทำเอกสาร minimum baseline standard เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ อย่างเป็นลายลักษณ์อักษร โดยมีการทบทวน ปรับปรุงเอกสารให้เป็นปัจจุบันอย่างสม่ำเสมอ

2.6.2.2 การเปลี่ยนแปลงการตั้งค่าบนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่โรงพิมพ์ตำรวจกำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.6.2.3 มีการจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบของทุกอุปกรณ์ ระบบและระบบงาน (system configuration version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.6.3 การบริหารจัดการ patch (patch management)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีการบริหารจัดการ patch โดยมีการควบคุมที่รัดกุมปลอดภัย และติดตั้ง ได้อย่างเหมาะสมทันการณ์

2.6.3.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในกระบวนการบริหารจัดการ patch ที่ครอบคลุม การตรวจสอบ ความถูกต้องของ patch และการประเมินความเสี่ยงและความจำเป็นในการติดตั้ง patch ใหม่จากผู้ผลิต อย่างเหมาะสมทันการณ์

2.6.3.2 มีการจัดเก็บการเปลี่ยนแปลงการติดตั้งของทุกอุปกรณ์ ระบบและระบบงาน (patch version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.6.3.3 มีกระบวนการทดสอบ patch ที่ออกใหม่ทุกครั้งก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

2.6.3.4 การติดตั้ง patch บนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่โรงพิมพ์ตำรวจกำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.6.3.5 มีการทบทวนและปรับปรุงกระบวนการบริหารจัดการ patch อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าโรงพิมพ์ตำรวจ สามารถทดสอบและติดตั้ง patch ด้านการรักษาความปลอดภัย ได้ทันต่อสถานการณ์ที่เปลี่ยนไปและสามารถรองรับความเสี่ยงที่เพิ่มขึ้นได้อย่างรวดเร็ว

2.6.4 การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัย สามารถใช้ติดตาม ตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน รวมทั้งใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด

2.6.4.1 มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารที่สำคัญด้วย วิธีการที่ปลอดภัย โดยมีรายละเอียดที่ครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด

· บันทึกร่องรอยกิจกรรมการทฎธุรกรรม (transaction log)

· บันทึกการเข้าถึง (access log)

· บันทึกการด าเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยต้องครอบคลุม

- การเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูล และการเปลี่ยนแปลงแก้ไขข้อมูล (update/ insert/ delete) ในตารางที่สำคัญ

- การเปลี่ยนแปลงการตั้งค่าความปลอดภัยของระบบ

- การเข้าถึง object ที่สำคัญของระบบ

- การเปลี่ยนแปลงแก้ไขบัญชีและสิทธิ์ของผู้ใช้งาน

2.6.4.2 มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารให้ตรงกับ เครื่องแม่ข่าย Network Time Protocol : NTP (clock synchronization) เพื่อให้ค่าเวลาในการบันทึก เหตุการณ์มีความถูกต้องในลักษณะ real-time ซึ่งเครื่องแม่ข่าย NTP ต้องรับสัญญาณนาฬิกาจากแหล่งที่มีความน่าเชื่อถือ

2.6.4.3 ข้อมูลการบันทึกเหตุการณ์ของอุปกรณ์สำคัญควรจัดเก็บไว้ที่เครื่องแม่ข่ายที่แยกเฉพาะ อย่างน้อยครอบคลุม access log และ activity log โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอในการป้องกันการเปลี่ยนแปลง แก้ไข หรือท าลาย

2.6.4.4 มีการสอบทานบันทึกการเข้าถึง (access Log) และบันทึกการดำเนินงาน (activity log) ของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีสิทธิ์สูงอย่างสม่ำเสมอ เช่น system administrator หรือ system operator เป็นต้น เพื่อให้มั่นใจได้ว่าผู้ปฏิบัติงานเข้าถึงและปฏิบัติงานตามขอบเขตหน้าที่ที่ได้รับมอบหมาย

2.6.5 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอรองรับ ต่อการดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

2.6.5.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติเรื่องการบริหารจัดการขีดความสามารถของระบบ เพื่อประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

ที่ครอบคลุมถึง ระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ

2.6.5.2 มีการประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศเพื่อวางแผนรองรับการใช้งานในอนาคต (capacity planning) โดยครอบคลุมทั้งระบบหลักและระบบสำรอง

2.6.5.3 มีกระบวนการหรือเครื่องมือในการติดตามประสิทธิภาพและความเพียงพอของการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศของระบบ เช่น ระบบ core banking ระบบการชำระเงิน ระบบที่ให้บริการทางการเงินอิเล็กทรอนิกส์ เป็นต้น เพื่อบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างทันท่วงที และสามารถตอบสนองความต้องการในการดำเนินงานทางธุรกิจอย่างต่อเนื่อง

2.6.5.4 มีการกำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (threshold และ trigger) ในระดับต่าง ๆ เพื่อให้มีการแจ้งเตือนผู้เกี่ยวข้องอย่างทันท่วงที และสามารถวิเคราะห์ปัญหาและแนวทางการรับมือที่เหมาะสม รวมถึงการประสานงานกับหน่วยงานทั้งภายในและภายนอกกรณีเกิดเหตุขัดข้อง

2.6.5.5 จัดทำรายงานความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศนำเสนอต่อโรงพิมพ์ตำรวจ ที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อม และความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง รวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการณ์

2.6.6 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring)

วัตถุประสงค์ เพื่อให้ โรงพิมพ์ตำรวจ สามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงที โดยมีกระบวนการติดตามดูแลความมั่นคงปลอดภัยของระบบรวมถึงเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง

2.6.6.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง

2.6.6.2 กำหนดกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยของระบบที่สำคัญอย่างทันท่วงที ครอบคลุมระบบงานและระบบเครือข่ายสื่อสารทั้งในเชิง physical และ logical เช่น ศูนย์คอมพิวเตอร์ และระบบที่ให้บริการทางอิเล็กทรอนิกส์ เป็นต้น เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม

2.6.6.3 มีกระบวนการหรือเครื่องมือในการรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ มีการวิเคราะห์และจัดการข้อมูล ภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุม ลักษณะการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้น เพื่อนำมาใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์

2.6.6.4 กำหนดให้มีผู้รับผิดชอบในการประสานงานแลกเปลี่ยนข้อมูลภัยคุกคาม ระหว่างโรงพิมพ์ตำรวจ และหน่วยงานที่เกี่ยวข้อง รวมทั้งมีกระบวนการและช่องทางในการรายงาน แลกเปลี่ยน ติดตาม เพื่อป้องกันรับมือและ แก้ไขภัยคุกคาม

2.6.6.5 ในกรณีที่พบภัยคุกคามที่ส่งผลกระทบอย่างมีนัยสำคัญ โรงพิมพ์ตำรวจควรจัดให้มีการรายงานผู้บริหารหรือโรงพิมพ์ตำรวจ ที่เกี่ยวข้อง รวมทั้งมีการรายงานหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมทั้งจัดให้มีกระบวนการ เพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่และป้องกันความเสี่ยงที่อาจเกิดขึ้นอีก

2.6.7 การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Test)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ ได้รับทราบถึงช่องโหว่ด้านการรักษาความปลอดภัยของระบบ และสามารถดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้อย่างทันการณ์

2.6.7.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ

การบริหารจัดการช่องโหว่ (Vulnerability Management)

2.6.7.2 มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ โดยโรงพิมพ์ตำรวจควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ให้ครอบคลุมทุกระบบงานอย่างสม่ำเสมอตามระดับความเสี่ยง สำหรับระบบบงานสำคัญควรจัดทำอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.6.7.3 มีการรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไข และนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

การทดสอบเจาะระบบ (Penetration Test)

2.6.7.4 มีการทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่มีความอิสระครอบคลุมระบบงานและระบบเครือข่ายกับระบบที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.6.7.5 มีการรายงานผลการทดสอบเจาะระบบไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไข และนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

2.6.7.6 มีกระบวนการรวบรวมและวิเคราะห์ช่องโหว่ทางด้านเทคนิคที่ตรวจพบ เพื่อกำหนดเป็นมาตรการรักษาความมั่นคงปลอดภัยของระบบงานที่จะมีการพัฒนาในอนาคต

2.6.8 การสำรองข้อมูล (Data Backup)

วัตถุประสงค์ เพื่อให้มั่นใจว่าโรงพิมพ์ตำรวจ มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหายจนไม่สามารถใช้งานได้ตามปกติ

2.6.8.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการสำรองข้อมูล เพื่อให้มีข้อมูลสำรองพร้อมใช้และมีความปลอดภัยโดยควรครอบคลุมอย่างน้อย

- วิธีการ เทคโนโลยีและรอบระยะเวลาที่ใช้ในการสำรองข้อมูล โดยควรสอดคล้องกับเป้าหมาย ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหายที่กำหนด

- รอบระยะเวลาและวิธีการทดสอบความพร้อมใช้ของข้อมูลสำรอง

2.6.8.2 มีกระบวนการสำรองทั้งระบบ (full backup) ทุกครั้งภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ และระบบงาน เพื่อให้ระบบสำรองมีความเป็นปัจจุบัน

2.6.8.3 มีระบบหรือทะเบียนควบคุมการจัดเก็บและเรียกใช้งานสื่อบันทึกข้อมูลตามประเภทของสื่อที่จัดเก็บ โดยมีการระบุข้อมูล ชื่อ วันที่ และช่วงเวลาที่จัดเก็บ ที่สามารถติดตามตรวจสอบได้

2.6.8.4 มีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกศูนย์คอมพิวเตอร์หลักหรือนอกสถานที่ปฏิบัติงานหลัก โดยมีการรักษาสภาพแวดล้อมและการควบคุมความปลอดภัยในการเข้าถึงข้อมูลที่จัดเก็บไว้เทียบเคียงกับศูนย์คอมพิวเตอร์หลัก

2.6.8.5 จัดให้มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วน ถูกต้อง พร้อมใช้งาน และปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติของโรงพิมพ์ตำรวจ

2.6.9 การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)

วัตถุประสงค์ เพื่อให้อุปกรณ์ที่ใช้ปฏิบัติงานมีความปลอดภัยและไม่เป็นช่องทางที่ทำให้ข้อมูลสำคัญของโรงพิมพ์ตำรวจรั่วไหลหรือมีการเข้าใช้งานโดยไม่ได้รับอนุญาต

2.6.9.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงานเป็นลายลักษณ์อักษร ทั้งอุปกรณ์ของโรงพิมพ์ตำรวจ และอุปกรณ์ส่วนตัว เช่น personal computer, notebook, tablet, smartphone, removable media เป็นต้น เพื่อให้โรงพิมพ์ตำรวจมีแนวทางที่ใช้ในการควบคุม ความเสี่ยงจากการใช้งานอุปกรณ์ดังกล่าว

2.6.9.2 กำหนด Security Baseline สำหรับอุปกรณ์ที่ใช้ปฏิบัติงานของโรงพิมพ์ตำรวจเพื่อป้องกันความเสี่ยงที่อุปกรณ์เหล่านั้น อาจเป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญ ตามระดับความเสี่ยงที่เหมาะสม โดยอย่างน้อยครอบคลุม ดังนี้

- ติดตั้งระบบปฏิบัติการและโปรแกรมพื้นฐานที่ใช้ในการปฏิบัติงานบนเครื่องคอมพิวเตอร์ (personal computer, notebook) โดยมีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้ผู้ใช้งาน สามารถติดตั้งโปรแกรมอื่น ๆ นอกเหนือจากโรงพิมพ์ตำรวจกำหนด

- ติดตั้งโปรแกรมรักษาความปลอดภัย เช่น anti-Virus/ anti-malware, Host-based Intrusion Prevention System (HIPS) เป็นต้น โดยมีการปรับปรุงประสิทธิภาพของการป้องกันโปรแกรมไม่ประสงค์ดี (malware) ให้เพียงพอและเป็นปัจจุบัน เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ ๆ

- ควบคุมไม่ให้มีการจัดเก็บข้อมูลที่มีระดับชั้นความลับสูงสุดในเครื่องคอมพิวเตอร์ของผู้ใช้งาน แต่หากมีความจำเป็นต้องจัดเก็บ ต้องมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ เช่น มีการเข้ารหัส เป็นต้น

- มีกระบวนการหรือเครื่องมือในการตรวจจับ (detect) คัดกรอง (filter) สกัดกั้น (block) เพื่อป้องกันข้อมูลสำคัญรั่วไหล

- จำกัดการเข้าถึง shared drive หรือ shared folder ตามความจำเป็นในการใช้งานเท่านั้น

· การควบคุมการใช้งานอินเตอร์เน็ต โดยโรงพิมพ์ตำรวจควรมีเครื่องมือในการควบคุมให้อุปกรณ์ที่สามารถเชื่อมต่ออินเตอร์เน็ตเข้าถึงเฉพาะเว็บไซต์ที่ได้รับอนุญาตเท่านั้น รวมถึงมีการจำกัดการดาวน์โหลดหรืออัพโหลดข้อมูลจากอินเตอร์เน็ต

- การควบคุมการใช้สื่อบันทึกข้อมูลพกพา (removable media) เช่น กำหนดแนวทางการอนุญาต ให้ใช้งาน Universal Serial Bus (USB) หรือ external harddisk เป็นต้น

- การควบคุมการใช้ Email เช่น กำหนดแนวทางการใช้งาน Email เป็นต้น

2.7 การจัดหาและการพัฒนาระบบ (System Acquisition and Development)

วัตถุประสงค์ เพื่อให้มั่นใจได้ว่ากระบวนการจัดหาและการพัฒนาระบบ มีการควบคุมการรักษาความปลอดภัย อย่างรัดกุมและสอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล

2.7.1 การจัดหาระบบ (System Acquisition)

2.7.1.1 มีหลักเกณฑ์การพิจารณาคัดเลือกระบบและผู้ให้บริการ เพื่อใช้เป็นแนวทางในการปฏิบัติงาน ซึ่งควรครอบคลุมอย่างน้อย ดังนี้

- รายละเอียดทั่วไป เช่น หมายเลขอ้างอิงของซอฟต์แวร์ (software license) ฟังก์ชันการ ทำงาน ประสิทธิภาพของระบบ เป็นต้น

- ความมั่นคงปลอดภัยของระบบ

- ฐานะการเงิน ชื่อเสียง และความสามารถด้านเทคนิค

- การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับ การยอมรับโดยทั่วไป (certificate)

- การสนับสนุนและการบำรุงรักษาระบบ

- ความน่าเชื่อถือของระบบและผู้ให้บริการ

2.7.1.2 โรงพิมพ์ตำรวจ ควรควบคุมดูแลผู้ให้บริการปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติการออกแบบและพัฒนาระบบ

2.7.1.3 โรงพิมพ์ตำรวจ กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการตรวจสอบและส่งมอบระบบเทคโนโลยีสารสนเทศ

2.7.2 การพัฒนาระบบเทคโนโลยีสารสนเทศ (System Development)

2.7.2.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างเป็นลายลักษณ์อักษร โดยคำนึงถึงการรักษาความมั่นคงปลอดภัย ครอบคลุมกระบวนการตั้งแต่จัดทำความต้องการ (requirement) การออกแบบ การพัฒนา และการทดสอบระบบก่อนใช้งานจริง

2.7.2.2 มีการสร้างความตระหนักและให้ความรู้กับผู้พัฒนาโปรแกรมอย่างสม่ำเสมอ เพื่อเสริมสร้างทักษะ ในด้านการออกแบบและพัฒนาโปรแกรมอย่างปลอดภัย

การออกแบบระบบ

2.7.2.4 จัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมการรักษาความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่โรงพิมพ์ตำรวจกำหนด (security specification) รวมทั้งจัดให้มีการสอบทานความถูกต้องครบถ้วนและ sign off จากผู้ที่เกี่ยวข้องก่อนเริ่มพัฒนาระบบ

2.7.2.5 จัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชันและเงื่อนไขต่าง ๆ ด้านประสิทธิภาพ รวมถึงการควบคุมความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที โรงพิมพ์ตำรวจกำหนด เพื่อเป็นแนวทางการพัฒนาระบบและสอบทานผลการทดสอบก่อนที่จะออกใช้งานจริง

การพัฒนาระบบ

2.7.2.6 มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) การทดสอบ (testing) และระบบที่ให้บริการจริง (production) ออกจากกัน เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นจากการนำระบบขึ้นใช้งานจริง

2.7.2.7 มีการควบคุมเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้มีความปลอดภัยเพียงพอ ตามระดับความเสี่ยงเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2.7.2.8 มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (development tools) และเครื่องมือแปลโปรแกรม (compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรม โดยไม่ได้รับอนุญาต

การทดสอบระบบ

2.7.2.10 บทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบควรเป็นไปตามหลักการแบ่งแยกหน้าที่อย่างเหมาะสม เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงาน ได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ควรแยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น

2.7.2.11 มีการทดสอบบนสภาพแวดล้อมใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงของการเปลี่ยนแปลงบน ระบบที่ให้บริการจริง

2.7.2.12 การทดสอบระบบที่ได้รับการพัฒนาหรือเปลี่ยนแปลง ควรครอบคลุม

- unit test
- system and integration test
- user acceptance test
- performance test
- security test ตาม security specification

ทั้งนี้ โรงพิมพ์ตำรวจ ควรจัดให้มีกระบวนการและเอกสารการ sign off ผลการทดสอบระบบจากฝ่ายงานที่เกี่ยวข้องก่อนนำระบบขึ้นใช้งานจริง

2.7.2.13 มีกระบวนการสอบทาน เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอ

2.7.2.14 การพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการ ระบบที่มีการเชื่อมโยงกับระบบอื่นจำนวนมาก โรงพิมพ์ตำรวจควรจัดให้มีการทดสอบประสิทธิภาพ เพื่อให้มั่นใจได้ว่าระบบมีเสถียรภาพเพียงพอในการรองรับการใช้งานจำนวนมาก

2.7.2.15 มีการทดสอบระบบรักษาความปลอดภัยควรครอบคลุมการประเมินช่องโหว่ ของระบบงาน และกรณีเป็นระบบที่เชื่อมต่อกับภายนอก ควรมีการทำทดสอบเจาะระบบ เพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขได้ก่อนเริ่มให้บริการจริง

2.7.2.16 มีการจัดทำคู่มือและอบรมผู้ใช้งานระบบ เพื่อให้มีความเข้าใจฟังก์ชันการทำงานและมีการใช้งานระบบอย่างปลอดภัย รวมถึงจัดให้มีคู่มือการดูแลระบบและอบรมผู้ดูแลระบบ เพื่อสามารถตรวจสอบและจัดการแก้ไขปัญหาได้

2.7.2.17 ระบบงานสำรองควรปรับปรุงให้มีความเป็นปัจจุบัน เพื่อให้มีความพร้อมใช้งานเมื่อเกิดเหตุฉุกเฉิน

2.8 การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management)

2.8.1 การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident Management)

วัตถุประสงค์ เพื่อให้ โรงพิมพ์ตำรวจ มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์อย่างเหมาะสมทันการณ์ ให้สามารถจัดการแก้ไขปัญหาให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจของ โรงพิมพ์ตำรวจ

2.8.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมตั้งแต่กระบวนการหรือเครื่องมือในการบันทึกเหตุการณ์ผิดปกติ การกำหนดประเภท การจัดระดับความรุนแรง การวิเคราะห์หาสาเหตุ การดำเนินการแก้ไข การติดตามแก้ไข การรายงานเหตุการณ์ผิดปกติ

2.8.1.2 กำหนดหลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติและรายงานความคืบหน้าเหตุการณ์ผิดปกติ ให้ผู้เกี่ยวข้อง ผู้บริหารระดับสูง คณะกรรมการที่เกี่ยวข้อง ได้รับทราบระดับความรุนแรงของเหตุการณ์ผิดปกติ

2.8.1.3 การจัดระดับความรุนแรงของปัญหา ควรพิจารณาอย่างน้อยให้ครอบคลุมผลกระทบต่อการให้บริการ ผลกระทบต่อผู้ใช้งาน โดยกรอบระยะเวลาในการแก้ไขเหตุการณ์ผิดปกติควรคำนึงถึงเป้าหมายระยะเวลา ในการกู้คืนระบบ และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ธุรกิจ หยุดชะงักเพื่อที่จะสามารถตัดสินใจใช้ แผนสำรองอย่างเหมาะสมทันการณ์

2.8.1.4 จัดทำแผนการรับมือกับเหตุการณ์ผิดปกติ (incident response plan) ตามความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์

โดยอย่างน้อยแผนควรระบุกระบวนการรับมือและช่องทางประสานงานจากผู้เชี่ยวชาญทั้งภายในและภายนอก และมีแนวทางการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบ

2.8.1.5 จัดทำรายงานเหตุการณ์ผิดปกติ เสนอต่อคณะอนุกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย โดยครอบคลุม วัน เวลา เหตุการณ์ ความเสียหาย การวิเคราะห์ สาเหตุที่แท้จริง การวิเคราะห์ผลกระทบ การแก้ไขปัญหาและแนวทางหรือแผนดำเนินการเพื่อป้องกัน เหตุการณ์ผิดปกติในอนาคต และในกรณีที่เป็นความเสียหายส่งผลกระทบต่อชื่อเสียงและการดำเนินธุรกิจ ของ โรงพิมพ์ตำรวจอย่างมีนัยสำคัญ ให้รายงานต่อคณะกรรมการของโรงพิมพ์ตำรวจทราบด้วย

2.8.1.6 ในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศ ซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน รวมถึงกรณีเทคโนโลยีสารสนเทศที่สำคัญของโรงพิมพ์ตำรวจถูกโจมตีหรือ ถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาต้องรายงานต่อผู้บริหาร ในตำแหน่งสูงสุดของโรงพิมพ์ตำรวจทราบ

2.8.2 การบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ (IT Problem Management)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีกระบวนการติดตามหาสาเหตุที่แท้จริง ให้มีแนวทางป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

2.8.2.1 มีมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ เพื่อให้มีการนำเหตุการณ์ผิดปกติที่ยังไม่ทราบสาเหตุที่แท้จริง เหตุการณ์ผิดปกติที่เกิดขึ้นซ้ำมาวิเคราะห์และพิจารณาแนวทางแก้ไขปัญหาจากสาเหตุที่แท้จริง (root cause)

2.8.2.2 มีกระบวนการหรือเครื่องมือในการบันทึกปัญหา หลักเกณฑ์ในการจัดประเภทปัญหา การจัดลำดับความสำคัญ วิเคราะห์ และจัดให้มีการติดตามการแก้ไขปัญหาเพื่อให้ปัญหาได้รับการแก้ไข

2.8.2.3 มีกระบวนการหรือเครื่องมือบันทึกปัญหาที่เคยเกิดขึ้น เพื่อให้เป็นแหล่งข้อมูลความรู้ให้สามารถสืบค้น เหตุการณ์ปัญหาและแนวทางการแก้ไขปัญหาได้ในภายหลังอย่างรวดเร็วและมีประสิทธิภาพ

2.9 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเกิดหยุดชะงักหรือเกิดความเสียหาย โดยที่ธุรกิจดำเนินการต่อไปได้อย่างต่อเนื่องและสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้

นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

2.9.1 กำหนดนโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยคำนึงความสอดคล้องกับนโยบายการบริหารความต่อเนื่องของธุรกิจและนโยบายการบริหารความเสี่ยงของโรงพิมพ์ตำรวจ

2.9.2 นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการของโรงพิมพ์ตำรวจ และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนฯ เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบาย การบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการดำเนินธุรกิจหรือทรัพยากรหรือโครงสร้างระบบ IT เป็นต้น

2.9.3 นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมอย่างน้อย

- บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการ ผู้บริหารระดับสูง และผู้เกี่ยวข้อง
- การประเมินความเสี่ยง
- การวิเคราะห์ผลกระทบทางธุรกิจและกำหนดเป้าหมายในการกู้คืนระบบเทคโนโลยีสารสนเทศ
- การจัดระดับความสำคัญของระบบงาน
- การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การทดสอบการปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

การจัดทำแผนฉุกเฉิน ด้านเทคโนโลยีสารสนเทศ

2.9.4 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยต้องได้รับการอนุมัติจากคณะกรรมการโรงพิมพ์ตำรวจ โดยจัดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.9.5 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศไว้ อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย

2.9.6 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรคำนึงถึงลักษณะการดำเนินธุรกิจ ความซับซ้อนของเทคโนโลยีสารสนเทศ เหตุการณ์ความเสียหายต่าง ๆ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจของโรงพิมพ์ตำรวจ เช่น ความเสี่ยงด้านปฏิบัติการ (operational risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการดำเนินธุรกิจ (interdependency risk) และความเสี่ยงที่มีผลกระทบต่อโรงพิมพ์ตำรวจผู้ใช้บริการ ผู้มีส่วนได้เสีย

2.9.7 กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมการดำเนินการ ดังนี้

(1) การประเมินความเสี่ยง (risk analysis) เพื่อให้โรงพิมพ์ตำรวจ สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการ อย่างเหมาะสมเพียงพอดังนี้

- ระบุเหตุการณ์ความเสี่ยง ที่อาจทำให้กระบวนการและระบบเทคโนโลยีสารสนเทศหยุดชะงัก ทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ เป็นต้น
- ประเมินความเสี่ยงโดยพิจารณาการควบคุมที่มีอยู่ รวมถึงผลกระทบและโอกาสที่จะเกิดขึ้น พร้อมทั้งกำหนดกระบวนการและทรัพยากรที่จะใช้ในการควบคุมความเสี่ยง
- จัดทำแผนในการจัดการความเสี่ยง เพื่อปรับปรุงกระบวนการและจัดเตรียมทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

(2) การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) เพื่อให้ทราบถึงความสำคัญของระบบเทคโนโลยีสารสนเทศที่มีผลต่อการดำเนินธุรกิจของโรงพิมพ์ตำรวจ รวมถึงผลกระทบจากการหยุดชะงักและความเชื่อมโยงของการดำเนินธุรกิจกับระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการดังนี้

- ระบุระบบเทคโนโลยีสารสนเทศทั้งหมดของโรงพิมพ์ตำรวจและทรัพยากรที่มีการเชื่อมโยงพึ่งพาระหว่างกัน

- วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของเทคโนโลยีสารสนเทศ โดยคำนึงถึงเป้าหมาย ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก

- กำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

(3) การจัดลำดับความสำคัญของระบบงาน โดยคำนึงถึงทรัพยากร ระยะเวลาในการกู้คืนระบบ เป้าหมายของระบบงานและข้อมูลที่ควรกู้ได้ภายหลังเกิดการหยุดชะงัก และทรัพยากรทางเทคโนโลยีสารสนเทศขั้นต่ำที่จำเป็นต้องใช้ในการกู้คืนระบบ ทั้งนี้ โรงพิมพ์ตำรวจควรพิจารณาระบบที่มีผลกระทบกับระบบโรงพิมพ์ตำรวจ

(4) การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โรงพิมพ์ตำรวจต้องมีการกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและแนวทางจัดเตรียมทรัพยากรระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามการจัดลำดับความสำคัญของระบบงาน โดยพิจารณาอย่างน้อยครอบคลุม

- เป้าหมายระยะเวลาที่ได้จากการวิเคราะห์ผลกระทบทางธุรกิจ

- ปัจจัยสำคัญที่สนับสนุนให้แผนเป็นไปตามกลยุทธ์ เช่น เทคโนโลยีในการสำรองและกู้คืนข้อมูล ความพร้อมใช้ของสถานที่ปฏิบัติงานสำรอง เป็นต้น เพื่อให้โรงพิมพ์ตำรวจมีทิศทางในการพัฒนาแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่บรรลุเป้าหมายที่กำหนดไว้

- ทรัพยากรและงบประมาณ เพื่อจัดเตรียมระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามแผนกลยุทธ์ และกิจกรรมที่ต้องดำเนินการทั้งหมด

(5) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรมีการระบุกระบวนการและขั้นตอนสนับสนุนการปฏิบัติที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ รวมทั้งมีความยืดหยุ่นในการตอบสนองต่อเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น อย่างน้อยครอบคลุม

- ชื่อแผน วัตถุประสงค์ ขอบเขต และความสัมพันธ์กับแผนอื่น ๆ ที่เกี่ยวข้อง

- ผังโครงสร้างของการบังคับบัญชาในการดำเนินงานตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบ และผู้ปฏิบัติที่ทำหน้าที่แทนในกรณีที่ผู้ปฏิบัติหน้าที่ไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึก การเปลี่ยนแปลงของแผน

- รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม แผนภาพระบบ เครือข่ายสื่อสาร เป็นต้น

- ขั้นตอนในการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ การตอบสนองต่อเหตุการณ์ฉุกเฉิน และแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบ

- ขั้นตอนในการดำเนินการกู้คืนระบบ โดยควรระบุรายละเอียดอย่างชัดเจนและเพียงพอ เพื่อให้สามารถใช้เป็น checklist ควบคุมไม่ให้มีการข้ามหรือละเลยขั้นตอนที่กำหนดไว้

ทั้งนี้ โรงพิมพ์ตำรวจ ควรจัดทำเอกสารหรือคู่มือประกอบการกู้คืนในแต่ละระบบ ในกรณีที่มีการปรับปรุง หรือเพิ่มเติมขั้นตอนนอกเหนือจากที่ระบุในแผนขณะปฏิบัติงานจริง โรงพิมพ์ตำรวจควรมีกระบวนการ รายงานและขออนุมัติจากผู้บริหารตามที่กำหนดในโครงสร้างการบังคับบัญชา พร้อมทั้งนำขั้นตอนดังกล่าวมาปรับปรุงแผนให้เป็นปัจจุบัน

- ขั้นตอนในการกลับคืนสู่ภาวะปกติ (return to normal) และการประกาศยกเลิกแผนฉุกเฉิน ด้านเทคโนโลยีสารสนเทศ

- แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ พร้อมเอกสารประกอบการทำงานภายใต้แผนฉุกเฉิน ด้านเทคโนโลยีสารสนเทศ ควรจัดเก็บไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้ในสถานที่ ปฏิบัติงานหลักและสไรอง

(6) การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โรงพิมพ์ตำรวจต้องจัดให้มีการสื่อสารแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และจัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้อง

- ในการสื่อสารแผนฯ ต้องมีการระบุแนวทางสื่อสารที่ชัดเจนให้บุคลากรทุกคนที่มีส่วนเกี่ยวข้องได้รับทราบถึงรายละเอียดในการจัดทำแผน ขั้นตอนการดำเนินงานตามแผน

· จัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยควรครอบคลุม วัตถุประสงค์ของแผน ขั้นตอนการปฏิบัติงานตามแผน การประสานงาน และการสื่อสารกันระหว่างกลุ่ม ขั้นตอนในการรายงาน ระบบรักษาความปลอดภัย กระบวนการเฉพาะ ของแต่ละกลุ่มดำเนินงาน และความรับผิดชอบของแต่ละบุคคล เป็นต้น

(7) การทดสอบ การปรับปรุง และการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

- จัดให้มีแผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปี โดยมีรายละเอียด อย่างน้อยครอบคลุมสถานการณ์จำลอง รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้อง ทั้งนี้แผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปีในภาพรวมควรได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย

- จัดให้มีการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศทั้งในระดับหน่วยงานและระดับองค์กร อย่างน้อยปีละ 1 ครั้ง โดยเฉพาะระบบงานหรือข้อมูลที่มีผลกระทบต่อการให้บริการลูกค้าหรือต่อโรงพิมพ์ตำรวจทั้งระบบ

- กรณีระบบงานมีการเชื่อมโยงเครือข่ายสื่อสารหรือใช้บริการจากหน่วยงานภายนอกโรงพิมพ์ตำรวจ ควรมีการทดสอบแผนฉุกเฉินร่วมกับหน่วยงานภายนอกที่เกี่ยวข้องด้วย เพื่อให้มั่นใจว่าระบบ

เทคโนโลยีสารสนเทศของโรงพิมพ์ตำรวจมีความพร้อมใช้งานร่วมกับระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก

- มีการรายงานผลการทดสอบต่อคณะกรรมการโรงพิมพ์ตำรวจ โดยมีรายละเอียดอย่างน้อยครอบคลุม วัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ระยะเวลาที่ใช้ในการกู้คืนระบบเทียบกับเป้าหมายที่กำหนด ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข

- โรงพิมพ์ตำรวจ ควรจัดให้มีการทบทวนและปรับปรุงแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อย ปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงบุคลากรที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผน การเปลี่ยนสภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศ เป็นต้น เพื่อให้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นปัจจุบัน

- โรงพิมพ์ตำรวจ อาจจัดให้มีการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศโดยหน่วยงานภายนอกหรือภายในที่มีความเป็นอิสระ เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผนให้สามารถใช้งานได้จริง

2.10 การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีแนวทางการบริหารจัดการผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศขอ โรงพิมพ์ตำรวจ หรือสามารถเข้าถึงข้อมูลสำคัญหรือลูกค้าของโรงพิมพ์ตำรวจ

2.10.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการผู้ให้บริการภายนอก เพื่อควบคุมให้มีการรักษาความมั่นคงปลอดภัยทรัพย์สินของโรงพิมพ์ตำรวจโดยอย่างน้อยครอบคลุม

- ก่อนใช้บริการโรงพิมพ์ตำรวจ ดำเนินการระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลหรือระบบเทคโนโลยีสารสนเทศที่ผู้ให้บริการภายนอกสามารถเข้าถึง โดยอย่างน้อยควรพิจารณาขอบเขต เหตุผลและความจำเป็นในการเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศ ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลง ผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจและการยกเลิกหรือสิ้นสุดสัญญา

- ข้อกำหนดในการรักษาความมั่นคงปลอดภัยของหน่วยงานภายนอก รวมถึง sub-contract ต้องปฏิบัติ โดยควรสอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยที่ โรงพิมพ์ตำรวจกำหนด

- ข้อตกลงการไม่เปิดเผยข้อมูล

- มีกระบวนการติดตาม ประเมิน ทบทวน และรายงานผลการปฏิบัติงานของหน่วยงานภายนอก

3. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management)

วัตถุประสงค์ เพื่อให้โรงพิมพ์ตำรวจ มีการบริหารจัดการความเสี่ยงของการดำเนินโครงการด้านเทคโนโลยีสารสนเทศ อย่างมีประสิทธิภาพและไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนกลยุทธ์ทางธุรกิจ

3.1 กำหนดกรอบการบริหารจัดการโครงการ ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางดำเนินโครงการจัดหาหรือพัฒนาระบบเทคโนโลยีสารสนเทศ โดยควรครอบคลุมดังนี้

3.1.1 โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจน เพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด

- คณะอนุกรรมการ มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแล ให้โครงการสำเร็จเป็นไปตามเป้าหมายที่กำหนด มีการติดตามความคืบหน้า ปัญหาและ อุปสรรคของโครงการ เพื่อให้คำแนะนำและพิจารณาตัดสินใจการดำเนินงานที่สำคัญ โดยควรประกอบด้วยผู้บริหารจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง และเจ้าของโครงการหรือผู้สนับสนุนโครงการมีส่วนร่วมในการตัดสินใจ รวมทั้งคณะอนุกรรมการควรมีการประชุมอย่างสม่ำเสมอ เพื่อควบคุมดูแลโครงการที่สำคัญให้เป็นไปตามแผนงานที่กำหนด

- หน่วยงานหรือทีมงานดูแลภาพรวมโครงการ มีบทบาทหน้าที่และความรับผิดชอบในการกำหนดรูปแบบ กระบวนการและเครื่องมือ ที่เป็นมาตรฐานในการบริหารจัดการและติดตามโครงการ รวมทั้งติดตามรายงานภาพรวม โครงการสำคัญของโรงพิมพ์ตำรวจ ให้กับคณะกรรมการโรงพิมพ์ตำรวจ และผู้บริหารระดับสูงที่เกี่ยวข้องได้รับทราบ เพื่อติดตามและสนับสนุนให้บริหารจัดการโครงการสำเร็จลุล่วงสอดคล้องกับเป้าหมาย ในระดับกลยุทธ์ของโรงพิมพ์ตำรวจตามแผนงานที่กำหนด

3.1.2 แนวทางการบริหารจัดการโครงการ ควรกำหนดครอบคลุมอย่างน้อย ดังนี้

- ระเบียบขั้นตอนการบริหารจัดการโครงการ ครอบคลุมตั้งแต่ก่อนเริ่มโครงการ การดำเนินการ และควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ

- ปัจจัยและเกณฑ์ในการประเมินหรือจัดระดับความสำคัญของโครงการที่ชัดเจน รวมถึงขอบเขต อำนาจหน้าที่ในการอนุมัติและกำกับดูแลโครงการตามระดับความสำคัญของโครงการ

- รูปแบบของเอกสารหรือผลลัพธ์ที่เป็นมาตรฐาน ที่ต้องส่งมอบในแต่ละขั้นตอนอย่างชัดเจน เช่น แผนการดำเนินโครงการ รายงานความคืบหน้า รายงานการปิดโครงการ เป็นต้น

การเริ่มโครงการ

3.2 มีการประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งเลือกใช้เทคโนโลยีที่เหมาะสม ทั้งนี้โครงการต้องมีเป้าหมายที่ชัดเจน (project objective) สอดคล้องกับกลยุทธ์ขององค์กรและคำนึงถึงการรักษาความมั่นคงปลอดภัย

3.3 มีแผนการดำเนินโครงการที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการอย่างน้อยครอบคลุม

- เป้าหมายโครงการ
- ทรัพยากร (resources) ที่ใช้
- บทบาทหน้าที่ ความรับผิดชอบของทีมงานในการดำเนินโครงการ โดยทีมงานจะต้องมีประสิทธิภาพ และมีความรู้ความเชี่ยวชาญเพียงพอในการดำเนินโครงการ

- ขอบเขตและระยะเวลาของการดำเนินโครงการในแต่ละขั้นตอน
- ผลงานที่จะส่งมอบในแต่ละขั้นตอน
- ข้อกำหนดเงื่อนไขที่เกี่ยวข้องกับโครงการ เช่น ข้อกำหนดของผู้ว่าจ้าง ภาระผูกพัน ข้อจำกัด เป็นต้น

3.4 มีการนเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อคณะกรรมการโรงพิมพ์ตำรวจ คณะอนุกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูง ตามขอบเขตในการอนุมัติที่กำหนดไว้

การดำเนินการและควบคุมโครงการ

3.5 มีการบันทึกและจัดเก็บข้อมูลโครงการของแต่ละโครงการอย่างเพียงพอเพื่อใช้ติดตามดูแลและสามารถตรวจสอบย้อนหลังได้

3.6 มีการประเมินและติดตามการดำเนินโครงการอย่างต่อเนื่องและครอบคลุมขอบเขต ระยะเวลา และทรัพยากร ที่วางแผนไว้ ในกรณีที่มีการเปลี่ยนแปลงขอบเขต ระยะเวลา และหรือทรัพยากร หรือยกเลิกโครงการ ควรมีการนำเสนอเพื่อขออนุมัติการเปลี่ยนแปลงหรือยกเลิกโครงการ

3.7 มีการรายงานความคืบหน้า ปัญหา อุปสรรคและข้อจำกัดในการดำเนินโครงการ ต่อคณะอนุกรรมการที่ดูแลโครงการหรือผู้บริหารที่ได้รับมอบหมายอย่างเป็นประจำ เพื่อสามารถให้คำแนะนำและแนวทางในการแก้ไขปัญหาที่จะลดความเสี่ยงที่อาจเกิดขึ้นอย่างทันท่วงที โดยโครงการที่ส่งผลกระทบต่อธุรกิจของโรงพิมพ์ตำรวจ อย่างมีนัยสำคัญ ควรนำเสนอแก่คณะกรรมการโรงพิมพ์ตำรวจด้วย

การปิดโครงการ

3.8 มีการสรุปประโยชน์ที่ได้รับจากโครงการเทียบกับเป้าหมายที่กำหนด

3.9 มีการรวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นสิ่งที่ได้เรียนรู้ใช้สำหรับวิเคราะห์ ปรับปรุง และพัฒนากระบวนการหรือเครื่องมือในการบริหารจัดการโครงการต่อไป ให้มีประสิทธิภาพมากขึ้น

การสอบทานโครงการ

3.10 มีการสอบทานโครงการที่สำคัญ โดยหน่วยงานอิสระ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของ โครงการ นโยบาย มาตรฐาน ระเบียบและวิธีปฏิบัติของโรงพิมพ์ตำรวจ รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

กระบวนการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (ISMS) ขององค์กร

Supplier (ผู้ส่งมอบ)	Input (ปัจจัยนำเข้า)	Process (กระบวนการ)	Output (ผลผลิต)	Customer (ผู้รับมอบ)
หน่วยงานภายใน - คณะอนุกรรมการด้านสารสนเทศ - ผู้บริหารโรงพิมพ์ตำรวจ - หมวดนโยบายแผนและสารสนเทศ - หน่วยงานต่าง ๆ ในโรงพิมพ์ตำรวจ	- ระบบงานต่างๆ - Network Diagram ของระบบงานต่างๆ - ข้อมูลระบบเครือข่าย - Network Diagram ของระบบเครือข่าย - ข้อมูลอุปกรณ์ต่าง ๆ ในห้องแม่ข่าย - ข้อมูลอุปกรณ์คอมพิวเตอร์หรือเทคโนโลยีภายในโรงพิมพ์ตำรวจ - โครงสร้างแผนผังขององค์กร - ข้อมูลบุคลากร - ข้อมูลความเสี่ยง - การบริหารจัดการด้านเทคโนโลยีดิจิทัล	เริ่มต้น ↓ ๑. ระบุผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการบริหารความมั่นคงปลอดภัยของสารสนเทศ และวิเคราะห์ถึงความต้องการ ความคาดหวังของแต่ละผู้มีส่วนได้ส่วนเสียที่สำคัญ ↓ ๒. จัดทำทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดแผนการสื่อสารที่คลอบคลุมเนื้อหาที่ต้องการไปยังผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร ↓ ๓. นำเสนอผู้บริหารเพื่อพิจารณา ↓ ๔. ดำเนินการสื่อสาร/ถ่ายทอดแนวทางปฏิบัติเกี่ยวกับการบริหารความมั่นคงปลอดภัยของสารสนเทศแก่ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องตามแนวทางที่วางไว้ ↓	๑. แนวทาง/คู่มือ/แผนการสื่อสารฯ ๒. ผลการรับรู้แนวทางการปฏิบัติตามกระบวนการฯ ๓. ผลการสอบทานการบริหารความมั่นคงปลอดภัยของสารสนเทศ ๔. การวัดประสิทธิผลและแนวทางการปรับปรุงการดำเนินงาน	- ผู้บริหารโรงพิมพ์ตำรวจ - คณะกรรมการโรงพิมพ์ตำรวจ - หน่วยงานต่าง ๆ ในโรงพิมพ์ตำรวจ - หมวดนโยบายแผนและสารสนเทศ - ผู้พัฒนาระบบ - ผู้ใช้งานระบบ

Supplier (ผู้ส่งมอบ)	Input (ปัจจัยนำเข้า)	Process (กระบวนการ)	Output (ผลผลิต)	Customer (ผู้รับมอบ)
		๕. ประเมินการรับรู้แนวทางปฏิบัติการการการบริหารความมั่นคงปลอดภัยของสารสนเทศของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องตามที่ได้ระบุไว้ ↓ ๖. ติดตามการบริหารความมั่นคงปลอดภัยของสารสนเทศอย่างต่อเนื่องและเป็นระบบ โดยกำหนดแนวทางการวัดผล วิเคราะห์ ปรับปรุง/ปรับโครงสร้าง และควบคุมกระบวนการ ↓ ๗. จัดเตรียมและดำเนินการสอบทานการบริหารความมั่นคงปลอดภัยของสารสนเทศ ↓ ๘. รายงานผลการสอบทานการบริหารความมั่นคงปลอดภัยของสารสนเทศ ↓ ๙. จัดให้มีการปรับปรุงการดาเนินงานให้ดีขึ้นอย่างต่อเนื่อง ตลอดจนสื่อสารถึงความจาเป็นและ ↓ สิ้นสุด		

กระบวนการบริหารจัดการบริหารความเสี่ยงความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร

Supplier (ผู้ส่งมอบ)	Input (ปัจจัยนำเข้า)	Process (กระบวนการ)	Output (ผลผลิต)	Customer (ผู้รับมอบ)
หน่วยงานภายใน - คณะอนุกรรมการด้านสารสนเทศ - ผู้บริหารโรงพิมพ์ตำรวจ - หมวดนโยบายแผนและสารสนเทศ - หน่วยงานต่าง ๆ ในโรงพิมพ์ตำรวจ	- ระบบงานต่างๆ - Network Diagram ของระบบงานต่างๆ - ข้อมูลระบบเครือข่าย - Network Diagram ของระบบเครือข่าย - ข้อมูลอุปกรณ์ต่าง ๆ ในห้องแม่ข่าย - ข้อมูลอุปกรณ์คอมพิวเตอร์หรือเทคโนโลยีภายในโรงพิมพ์ตำรวจ - โครงสร้างแผนผังขององค์กร - ข้อมูลบุคลากร - ข้อมูลความเสี่ยง - การบริหารจัดการด้านเทคโนโลยีดิจิทัล	เริ่มต้น ๑. ระบุและรวบรวมข้อมูลที่เกี่ยวข้องหรือใช้ในการระบุ วิเคราะห์ และการรายงานด้านความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ๒. ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล ที่ประกอบด้วย การระบุความเสี่ยงที่เป็นไปได้ทั้งหมด (Risk Universe) การกำหนดเหตุการณ์ความเสี่ยง (Risk Scenario) การระบุปัจจัยเสี่ยง (Risk factor) ๓. ประเมินความเสี่ยงด้านเทคโนโลยีดิจิทัล โดยกำหนดเกณฑ์ประเมินความเสี่ยงด้านโอกาสและผลกระทบ กำหนดระดับความเสี่ยงด้านเทคโนโลยีดิจิทัลที่สามารถยอมรับได้ (IT Risk Appetite) ประเมินค่าโอกาสและผลกระทบของเหตุการณ์ความเสี่ยงเพื่อนามาจัดลาดับความเสี่ยงด้านเทคโนโลยีดิจิทัล	- นโยบาย/แนวทาง/คู่มือการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล - แนวทาง/คู่มือ/แผนการสื่อสารฯ - ผลการรับรู้แนวทางการปฏิบัติตามกระบวนการฯ ความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลขององค์กร	- คณะอนุกรรมการด้านสารสนเทศ - ผู้บริหารโรงพิมพ์ตำรวจ - คณะกรรมการโรงพิมพ์ตำรวจ - หน่วยงานต่าง ๆ ในโรงพิมพ์ตำรวจ - ผู้พัฒนาระบบ - ผู้ใช้งานระบบ

Supplier (ผู้ส่งมอบ)	Input (ปัจจัยนำเข้า)	Process (กระบวนการ)	Output (ผลผลิต)	Customer (ผู้รับมอบ)
		๔. บริหารจัดการเพื่อตอบสนองต่อความเสี่ยงทางด้านเทคโนโลยีดิจิทัล (Risk Response) ที่ประกอบด้วยแนวทางในการจัดการ ควบคุม ป้องกัน ความเสี่ยงด้านเทคโนโลยีดิจิทัลที่เหมาะสมและสอดคล้องกับการประเมินความเสี่ยงองค์กร ↓ ๕. การกำหนดตัวชี้วัดความเสี่ยงด้านเทคโนโลยีดิจิทัล (IT Risk Indicator) เพื่อชี้วัดและติดตามแนวโน้มความเสี่ยงที่อาจจะเกิดขึ้น โดยมีทั้งตัวชี้วัดผลการดำเนินงาน (Performance indicator) และตัวชี้วัดนำ (Lead indicator) ↓ ๖. กำหนดนโยบาย/แนวทาง/คู่มือการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล ↓ ๗. ระบุผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลขององค์กร และวิเคราะห์ถึงความต้องการ ความคาดหวังของแต่ละผู้มีส่วนได้ส่วนเสียที่สำคัญ ↓ ๘. นำเสนอผู้บริหารเพื่อพิจารณา		

Supplier (ผู้ส่งมอบ)	Input (ปัจจัยนำเข้า)	Process (กระบวนการ)	Output (ผลผลิต)	Customer (ผู้รับมอบ)
		๙. ดำเนินการสื่อสาร/ถ่ายทอดแนวทางปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลขององค์กร ↓ ๑๐. ติดตามการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลขององค์กรอย่างต่อเนื่องและเป็นระบบ โดยการอธิบายการวัดผล วิเคราะห์ ปรับปรุง/ปรับโครงสร้าง และควบคุมกระบวนการ ↓ ๑๑. ติดตามการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลขององค์กรอย่างต่อเนื่องและเป็นระบบ โดยการอธิบายการวัดผล วิเคราะห์ ปรับปรุง/ปรับโครงสร้าง และควบคุมกระบวนการ ↓ ๑๒. จัดให้มีการปรับปรุงการดำเนินงานให้ดีขึ้นอย่างต่อเนื่อง ↓ สิ้นสุด		

สรุปและข้อเสนอแนะ

1. สรุป

ระบบบริหารจัดการความมั่นคงปลอดภัยด้านระบบสารสนเทศ เป็นส่วนหนึ่งของระบบบริหารจัดการความเสี่ยงขององค์กร ซึ่งมีกระบวนการตั้งแต่การ สร้าง นำมาใช้ ดำเนินการ ตรวจสอบติดตาม สอบทานบำรุงรักษา และการพัฒนาความมั่นคงปลอดภัยด้านระบบสารสนเทศ โดยคำนึงถึงโครงสร้างนโยบาย การวางแผน ความรับผิดชอบ การปฏิบัติ ขั้นตอน กระบวนการ และทรัพยากรขององค์กร

วัตถุประสงค์หลักของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ คือการกำหนดมาตรการที่ใช้สำหรับป้องกันผู้ที่ไม่ได้รับอนุญาตในการเข้าถึง ลบ แก้ไข หรือขัดขวางไม่ให้ผู้ที่ได้รับอนุญาตใช้งาน ได้รับความรู้ แนวคิด และข้อเท็จจริง ซึ่งการที่จะทำให้ระบบสารสนเทศมีความมั่นคงปลอดภัยนั้นจำเป็นต้องคำนึงถึงสิ่งต่าง ๆ ดังต่อไปนี้

1.1 ความลับของข้อมูล

1.2 ความถูกต้องสมบูรณ์ของข้อมูล

1.3 การมีอยู่ของข้อมูล

1.4 ผู้ใช้ไม่สามารถปฏิเสธการกระทำ

1.5 การมีตัวตนจริงของผู้ใช้ระบบ

1.6 การกำหนดสิทธิของผู้ใช้ระบบ

เพื่อสร้างความตระหนักถึงความสำคัญและกระตุ้นให้บุคลากรทุกระดับขององค์กรเล็งเห็นถึงความจำเป็นในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ ที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศซึ่งเป็นเครื่องมือที่สำคัญที่สุดในการให้บริการประชาชนและการตัดสินใจของผู้บริหาร ตลอดจนรัฐบาลผู้บริหารประเทศ

ระบบรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ จะทำให้เจ้าหน้าที่ที่เกี่ยวข้องทราบถึงแนวทางในการปฏิบัติ เพื่อหลีกเลี่ยงความเสี่ยงต่าง ๆ หรือลดความรุนแรงของผลเสียหายที่อาจเกิดขึ้นต่อระบบปฏิบัติราชการขององค์กร จากการวิเคราะห์และประสบการณ์พบว่าปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นได้นั้น ส่วนใหญ่เกิดจากสามสาเหตุหลัก คือ

1) ด้านเทคโนโลยี

2) ด้านกระบวนการทำงาน

3) ด้านบุคลากร

ซึ่งปัญหาทั้ง 3 ด้านข้างต้น หากองค์กรไม่ดำเนินการป้องกันและแก้ไข อาจทำให้องค์กรมีภาวะเสี่ยงต่อการเกิดภาวะคุกคาม อาจก่อให้เกิดปัญหา อุปสรรค หรือการสูญเสียโอกาส ซึ่งจะมีผลทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อหน่วยงานโดยเฉพาะอย่างยิ่งผลเสียต่อระบบสารสนเทศที่องค์กรต้องใช้ในการบริหารงาน และปฏิบัติงานโดยเฉพาะอย่างยิ่งด้านการให้บริการแก่ประชาชน

2. ข้อเสนอแนะ

องค์กร ควรเร่งจัดทำระบบบริหารความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้สามารถรองรับเหตุการณ์ด้านความมั่นคงปลอดภัยภายในองค์กร รวมทั้งเพื่อให้บุคลากรในหน่วยงานทราบถึงรูปแบบการดำเนินการที่เป็นรูปธรรม รวมถึงระเบียบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีขั้นตอนการดำเนินการดังต่อไปนี้

มอบหมายผู้รับผิดชอบในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.1 กำหนดนโยบายหรือแนวทางการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.2 แต่งตั้งคณะทำงานบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อดำเนินการดังต่อไปนี้

2.2.1 กำหนดโครงสร้างการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.2.2 ดำเนินการตามกระบวนการบริหารความเสี่ยงด้านระบบสารสนเทศ

1) ระบุความเสี่ยง

2) วิเคราะห์และประเมินความเสี่ยง

3) จัดลำดับความสำคัญของปัจจัยเสี่ยง

4) กำหนดกิจกรรมบริหารความเสี่ยง

5) จัดทำแผนบริหารความเสี่ยงของแต่ละปัจจัยเสี่ยงที่อยู่ในระดับที่มีนัยสำคัญ

6) สื่อสารทำความเข้าใจเกี่ยวกับแผนบริหารความเสี่ยงให้บุคลากรขององค์กรเพื่อให้สามารถนำไปปฏิบัติได้จริง

7) รายงานสรุปผล ข้อดี ข้อเสีย ปัญหา อุปสรรค และข้อเสนอแนะของการดำเนินการตามแผนบริหารความเสี่ยงต่อประธานคณะกรรมการบริหารความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร