

แผนปฏิบัติการด้านการส่งเสริม การรักษาความมั่นคงปลอดภัยไซเบอร์

ของสำนักงานนโยบายและแผนการขนส่งและจราจร
ประจำปีงบประมาณ พ.ศ. 2569 - 2570



โดย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร



แผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานนโยบายและแผนการขนส่งและจราจร
ปีงบประมาณ พ.ศ. ๒๕๖๙ - ๒๕๗๐

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

สารบัญ

เรื่อง	หน้า
บทสรุปผู้บริหาร	
คำนำ	
บทที่ ๑ บทนำ	๑
๑.๑ หลักการและเหตุผล	๑
๑.๒ วัตถุประสงค์	๒
๑.๓ นิยามและคำจำกัดความที่สำคัญ	๒
บทที่ ๒ นโยบาย แผน กฎหมาย กฎระเบียบที่เกี่ยวข้อง และมาตรฐานความปลอดภัย	๕
๒.๑ กฎหมาย กฎระเบียบ และข้อกำหนดด้านเทคโนโลยีดิจิทัล	๖
๒.๒ นโยบายและแผนที่เกี่ยวข้อง	๑๓
๒.๓ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	๑๖
บทที่ ๓ สถานภาพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช.	๒๒
๓.๑ สถานภาพด้านเทคโนโลยีสารสนเทศ	๒๒
๓.๒ สถานภาพด้านมาตรการระบบรักษาความมั่นคงปลอดภัยไซเบอร์	๒๔
บทที่ ๔ การวิเคราะห์สภาพแวดล้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช.	๒๗
๔.๑ ความต้องการด้านเทคโนโลยีสารสนเทศ	๒๗
๔.๒ การวิเคราะห์สภาพแวดล้อมด้วยการทำ SWOT Analysis	๓๒
และภาพรวมของระบบรักษาความมั่นคงปลอดภัยไซเบอร์	
บทที่ ๕ แผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช.	๔๑
๕.๑ มาตรการส่งเสริมงานด้านความมั่นคงปลอดภัยไซเบอร์	๔๑
๕.๒ เป้าหมายการดำเนินงาน	๔๒
๕.๓ แผนงาน/โครงการ/กิจกรรม ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ - ๒๕๗๐	๔๔
๕.๔ การติดตามประเมินผลการดำเนินงานตามแผนงาน	๔๘
บทที่ ๖ บทสรุปและข้อเสนอแนะ	๔๙
๖.๑ บทสรุป	๔๙
๖.๒ ปัจจัยความสำเร็จ	๔๙
๖.๓ ข้อเสนอแนะ	๕๐
เอกสารอ้างอิง	๕๑

สารบัญ (ภาพ)

ภาพที่	หน้า
๒-๑ แผนภาพวงจรการบริหารจัดการความมั่นคงปลอดภัย ตามขั้นตอน Plan-Do-Check-Act	๑๖
๓-๒ หลักการ CIA	๒๕
๔-๑ กรอบแนวทางระบบรักษาความปลอดภัย ตามมาตรฐาน NIST Cybersecurity Framework ๒.๐	๒๘
๔-๒ การวิเคราะห์สภาพแวดล้อมด้านความมั่นคงปลอดภัยไซเบอร์ ด้วย SWOT	๓๒
๔-๔ การวิเคราะห์สภาพแวดล้อมโดยใช้เครื่องมือ TOWS Matrix	๓๕

บทสรุปผู้บริหาร

สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) กระทรวงคมนาคม ตั้งขึ้นตามพระราชบัญญัติปรับปรุง กระทรวง ทบวง กรม พ.ศ. ๒๕๔๕ และพระราชกฤษฎีกาการโอนกิจการบริหารและอำนาจหน้าที่ของส่วนราชการ ให้เป็นไปตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. ๒๕๔๕ มีพันธกิจและภารกิจเกี่ยวกับการเสนอแนะนโยบาย มาตรการ มาตรฐานและจัดทำแผนหลัก แผนแม่บท และยุทธศาสตร์การพัฒนา ระบบการขนส่งและจราจร ศึกษา วิจัย พัฒนางานคมนาคม รวมทั้งการส่งเสริมความปลอดภัยและสิ่งแวดล้อมในระบบคมนาคมและการขนส่งของประเทศ ซึ่ง สนข. ได้ตระหนักถึงความสำคัญของการนำเทคโนโลยีดิจิทัลมาช่วยในการบริหารจัดการส่วนราชการ ให้เป็นหน่วยงานที่ทันสมัยและมีประสิทธิภาพ พร้อม “ยกระดับ สนข. ให้เป็นองค์กรดิจิทัล” จึงได้มีการจัดทำแผนปฏิบัติการดิจิทัล สำนักงานนโยบายและแผนการขนส่งและจราจร พ.ศ. ๒๕๖๖ - ๒๕๗๐ เป็นเครื่องมือในการกำหนดกรอบแนวทางในการขับเคลื่อนงานด้านดิจิทัลของ สนข. ให้สอดคล้องกับนโยบาย แผน และยุทธศาสตร์การพัฒนาด้านเทคโนโลยีดิจิทัลตามนโยบายภาครัฐในทุกระดับ

ตามแผนปฏิบัติการดิจิทัล สำนักงานนโยบายและแผนการขนส่งและจราจร พ.ศ. ๒๕๖๖ - ๒๕๗๐ ได้กำหนดเป้าหมายไว้ชัดเจน คือ “การเป็นองค์กรดิจิทัล (Digital Parliament)” ดังนั้น สิ่งสำคัญที่ต้องคำนึงถึง คือ การรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร ซึ่งในแผนปฏิบัติการดิจิทัล สนข. พ.ศ. ๒๕๖๖ - ๒๕๗๐ ได้มีการกำหนดยุทธศาสตร์ที่ ๕ ไว้ คือ การพัฒนาระบบการบริหารจัดการมุ่งสู่องค์กรดิจิทัล (Digital Management) ประกอบด้วย ๕ กลยุทธ์ คือ

๑. ส่งเสริมวัฒนธรรมการใช้เทคโนโลยีดิจิทัลแก่บุคลากร (Digital Culture)
 ๒. ปรับเปลี่ยนกระบวนการทำงานให้เป็นดิจิทัลโดยใช้ระบบบริหารจัดการรูปแบบดิจิทัล (Re-Process)
 ๓. สร้างความเชื่อมั่นต่อระบบการปฏิบัติงาน และการให้บริการว่าปลอดภัยจากภัยคุกคามทางไซเบอร์ (Infrastructure & Security)
 ๔. กำหนดแนวปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
 ๕. จัดทำ พัฒนา ปรับปรุงโครงสร้างพื้นฐานด้านดิจิทัลของ สนข. ให้มีความทันสมัยรองรับการดำเนินงานในรูปแบบดิจิทัลที่มีความมั่นคงปลอดภัย
- โดยมีเป้าประสงค์เชิงยุทธศาสตร์ คือ เชื่อมโยงกระบวนการทำงานระหว่างหน่วยงานภายในและภายนอก รวมทั้งความมั่นคงปลอดภัยไซเบอร์

ดังนั้น เพื่อให้การพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. เป็นไปอย่างมีประสิทธิภาพ และเป็นไปตามมาตรฐานสากล รองรับการให้บริการได้อย่างเท่าเทียมและทั่วถึง จึงได้มีการจัดทำแผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร พ.ศ. ๒๕๖๙ - ๒๕๗๐ เพื่อใช้เป็นกรอบแนวทางในการขับเคลื่อนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ต่อไป

คำนำ

ปัจจุบันเทคโนโลยีดิจิทัลมีการพัฒนาไปอย่างต่อเนื่อง ทำให้เทคโนโลยีต่าง ๆ เกิดความก้าวหน้าและเปลี่ยนแปลงไปอย่างรวดเร็ว อีกทั้งตามนโยบายของรัฐบาล ที่ได้ผลักดันให้เกิดการปรับเปลี่ยนไปสู่การเป็นรัฐบาลดิจิทัล (Digital Government) โดยกำหนดให้องค์กรและหน่วยงานภาครัฐมุ่งสู่ความเป็นเลิศในการใช้ระบบสารสนเทศและเทคโนโลยีดิจิทัลที่ทันสมัย ดังนั้น สนข. จึงมีการนำเทคโนโลยีดิจิทัลมาใช้ในการปฏิบัติงาน และมีการพัฒนาระบบสารสนเทศต่างเพื่อเพิ่มประสิทธิภาพในการปฏิบัติราชการของเจ้าหน้าที่และบุคลากร สนข. เตรียมความพร้อมสู่การเป็นรัฐบาลดิจิทัลอย่างเต็มรูปแบบ เพื่อตอบสนองนโยบายของรัฐบาลในการพัฒนาระบบงานด้านดิจิทัลของหน่วยงานภาครัฐ สิ่งสำคัญที่ต้องคำนึงเมื่อมีการนำระบบดิจิทัลมาใช้งานนั้น คือการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพราะหากระบบถูกการโจมตีด้วยภัยทางไซเบอร์ในรูปแบบต่าง ๆ ที่ไม่มีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จะทำให้ระบบสารสนเทศเกิดความเสียหายไม่สามารถใช้งานได้ และเกิดผลกระทบต่อการปฏิบัติราชการอย่างร้ายแรง เช่น ข้อมูลสูญหาย ระบบสารสนเทศหยุดการทำงาน เป็นต้น สนข. เล็งเห็นความสำคัญ จึงจำเป็นต้องมีการจัดทำแผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร พ.ศ. ๒๕๖๙ - ๒๕๗๐ เพื่อใช้เป็นกรอบกำหนดทิศทางของการพัฒนางานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และเป็นเครื่องมือในการป้องกันไม่ให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของ สนข. ต่อไป

บทที่ ๑

บทนำ

๑.๑ หลักการและเหตุผล

ภัยคุกคามทางไซเบอร์ (Cyber Threat) เป็นปัญหาสำคัญที่กำลังเกิดขึ้น และส่งผลให้หลายประเทศทั่วโลกเริ่มมีการตื่นตัว และตระหนักถึงภัยดังกล่าว ซึ่งกลุ่มผู้ไม่หวังดีจะใช้เครื่องมือ สื่อโซเชียลมีเดีย และเครือข่ายทางสังคมออนไลน์ต่าง ๆ เป็นเครื่องมือในการโจมตี และก่อให้เกิดภัยคุกคามทางไซเบอร์ขึ้น โดยจากรายงานของ World Economic Forum จะเห็นว่า หลายประเทศทั่วโลกมีความวิตกกังวลเกี่ยวกับภัยคุกคามทางไซเบอร์เป็นอย่างมาก โดยภัยคุกคามทางไซเบอร์ถูกจัดให้อยู่ในอันดับที่ ๔ ใน ๑๐ Trends ของโลก และในแต่ละปีก็มีแนวโน้มที่จะเพิ่มสูงขึ้น ดังนั้น การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) จึงเป็นเรื่องที่จำเป็นขององค์กรทุกองค์กรที่ต้องให้ความสำคัญเป็นอันดับต้น ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็นจะต้องดำเนินการเพื่อทำให้องค์กรปราศจากความเสียหาย และความเสียหายที่มีผลต่อความปลอดภัยของระบบสารสนเทศ และข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่าง ๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA ทั้ง ๓ ประการ ได้แก่

- ๑) การรักษาความลับของข้อมูล (Confidentiality)
- ๒) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity)
- ๓) ความพร้อมใช้งานของข้อมูล (Availability)

กล่าวได้ว่าความมั่นคงปลอดภัยไซเบอร์ ถือว่ามีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้น การที่จะทำให้ระบบสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีกระบวนการในการดำเนินการ ซึ่งกระบวนการเหล่านั้นเป็นกระบวนการที่ถูกกำหนดเอาไว้เป็นมาตรฐานและเป็นที่ยอมรับ โดยมีองค์กรหรือสถาบันที่มีชื่อเสียงเป็นผู้กำหนดเกณฑ์และแนวทางในการปฏิบัติ ซึ่งองค์กรสามารถเลือกมาตรฐานที่มีความเหมาะสมกับหน่วยงานของตน และอาจเพิ่มเติมหรือยกเว้นการปฏิบัติในบางส่วนได้หากมีเหตุผลเพียงพอ จากเหตุผลข้างต้น จึงนำมาสู่การจัดทำแผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) พ.ศ. ๒๕๖๔ - ๒๕๗๐ ซึ่งเป็นการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของ สนข. โดยมีเป้าหมายเพื่อศึกษานโยบายมาตรฐานการดำเนินการในระดับสากล เพื่อเสนอแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ให้มีความมั่นคงปลอดภัยและเป็นไปตามมาตรฐานระดับสากล สอดคล้องกับแผนดิจิทัลของ สนข.

ดังนั้น เพื่อเป็นการยกระดับงานด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศและข้อมูลสำคัญของ สนข. ให้มีมาตรฐานและเป็นที่ยอมรับในระดับมาตรฐานสากล และเป็นการตอบสนองตามแผนปฏิบัติการดิจิทัลของ สนข. จึงได้ดำเนินการจัดทำแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. พ.ศ. ๒๕๖๔ - ๒๕๗๐ ขึ้น

๑.๒ วัตถุประสงค์

๒.๑ เพื่อให้มีแผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. พ.ศ. ๒๕๖๙ - ๒๕๗๐ และใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๒ เพื่อสร้างกระบวนการด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ที่มีประสิทธิภาพ สร้างความเชื่อมั่น ต่องานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และให้การดำเนินงานต่าง ๆ ภายในหน่วยงานเป็นไปอย่าง มีประสิทธิภาพและเสถียรภาพ

๒.๓ เพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศของ สนข. มีแผนงานโครงการด้านความมั่นคงปลอดภัย ไซเบอร์ที่สามารถติดตาม และประเมินผลการขับเคลื่อนงานด้านความมั่นคงปลอดภัยไซเบอร์

๑.๓ นิยามและคำจำกัดความที่สำคัญ

๑. **สนข.** หมายถึง สำนักงานนโยบายและแผนการขนส่งและจราจร
๒. **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ สนข.
๓. **ผู้บริหาร (Chief Executive Officer: CEO)** หมายถึง ผู้บังคับบัญชาสูงสุดของสำนักงาน ซึ่งมีบทบาท หน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย กำหนดทิศทาง รวมทั้งมอบหมายงาน ให้ผู้ปฏิบัติที่เกี่ยวข้อง กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์ใช้งานไม่ได้ ตลอดจนรับผิดชอบ ต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ
๔. **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)** หมายถึง ผู้บังคับบัญชาสูงสุดในด้านเทคโนโลยีสารสนเทศของ สนข.
๕. **ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร** หมายถึง หน่วยงานที่ดูแล และบริหารจัดการ ระบบเทคโนโลยีสารสนเทศของ สนข.
๖. **ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร** หมายถึง หัวหน้าส่วนงานที่ดูแล และบริหารจัดการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจรของ สนข.
๗. **การรักษาความมั่นคงปลอดภัยไซเบอร์** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบ เทคโนโลยีสารสนเทศและข้อมูลของ สนข.
๘. **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตาม วัตถุประสงค์หรือเป้าหมาย
๙. **ขั้นตอนการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ ต้องนำมา ปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
๑๐. **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติ ตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
๑๑. **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารจัดการ หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของ สนข. ตามสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ที่ สนข. กำหนดไว้ ดังนี้
 - ๑๑.๑ **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงของ สนข. เช่น ผอ.สนข. รอง ผอ.สนข. เป็นต้น
 - ๑๑.๒ **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ ที่ได้รับมอบหมายจาก ผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ รวมถึงระบบ สารสนเทศ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือระบบสารสนเทศต่าง ๆ เพื่อการบริหารจัดการระบบได้
 - ๑๑.๓ **ผู้ใช้งาน (User)** หมายถึง เจ้าหน้าที่และบุคลากรของ สนข. ที่มีสิทธิในการเข้าใช้งาน ระบบสารสนเทศของ สนข.

๑๒. **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่ สนข. อนุญาตให้มีสิทธิในการเข้าถึง และใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของ สนข.

๑๓. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

๑๔. **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้ สามารถเข้าใจ ได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

๑๕. **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงาน เข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑๖. **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือ การส่งข้อมูลสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กร

๑๗. **ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในสำนักงานเข้าด้วยกัน

๑๘. **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงาน ของ สนข. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างระบบสารสนเทศ ที่สำนักงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการการพัฒนา และควบคุมการติดต่อสื่อสาร

๑๙. **บัญชีผู้ใช้งาน** หมายถึง บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยี สารสนเทศของ สนข.

๑๙.๑ **พื้นที่ทำงานทั่วไป (General working area)** หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ ส่วนบุคคล และคอมพิวเตอร์พกพาเพื่อปฏิบัติงานในสำนักงาน

๑๙.๒ **พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)**

๑๙.๓ **พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or Network area)**

๑๙.๔ **พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)**

๑๙.๕ **พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)**

๒๐. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้น เกิดสูญหาย

๒๑. **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่ เกี่ยวข้องกับ ระบบเทคโนโลยีสารสนเทศ

๒๒. **สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ของสำนักงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๒๓. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

๒๔. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ทั้งนี้ รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

๒๕. **เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของการบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับ ความมั่นคงปลอดภัย

๒๖. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๒๗. **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๒๘. **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

บทที่ ๒

นโยบาย แผน กฎหมาย กฎระเบียบที่เกี่ยวข้อง และมาตรฐานความปลอดภัย

ปัจจุบันการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้นมีความสำคัญเป็นอย่างมากทั้งในประเทศและต่างประเทศ ซึ่งปัญหาภัยคุกคามทางไซเบอร์นั้นส่งผลกระทบต่อทั้งหน่วยงานภาครัฐและภาคเอกชน องค์กรต่าง ๆ ที่มีการนำระบบสารสนเทศมาประยุกต์ใช้ต้องตระหนักถึงความมั่นคงปลอดภัยเพื่อช่วยปกป้องระบบคอมพิวเตอร์ รวมไปถึงอุปกรณ์ต่าง ๆ ที่เกี่ยวข้อง และที่สำคัญยังสามารถช่วยปกป้องข้อมูลที่สำคัญได้จัดเก็บไว้ภายในระบบสารสนเทศอีกด้วย

จุดประสงค์ของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ

จุดประสงค์หลักของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ คือ ความลับ (Confidentiality) ความสมบูรณ์ (Integrity) ความพร้อมใช้ (Availability) และการห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) ของข้อมูลต่าง ๆ ภายในองค์กร โดยมีรายละเอียด ดังนี้

- ๑) การรักษาความลับ (Confidentiality) คือ การรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ ทำให้มั่นใจว่ามีเฉพาะผู้มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้
- ๒) การรักษาความสมบูรณ์ (Integrity) คือ การรับรองว่าข้อมูลที่ปกป้องนั้นต้องมีความถูกต้อง สมบูรณ์ จะไม่ถูกแก้ไข เปลี่ยนแปลง หรือทำลาย จากผู้ไม่มีสิทธิไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา
- ๓) ความพร้อมใช้ (Availability) คือ การรับรองว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมใช้งาน สามารถตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ
- ๔) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) คือ วิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้น ทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

องค์ประกอบของนโยบาย

ระบบสารสนเทศซึ่งเป็นระบบสนับสนุนการบริหารงาน การจัดการ และการปฏิบัติงานของบุคลากรไม่ว่าจะเป็นระดับบุคคล ระดับกลุ่ม หรือ ระดับองค์กร ไม่ใช่มีเพียงเครื่องคอมพิวเตอร์เท่านั้น แต่ยังรวมถึงองค์ประกอบอื่น ๆ ที่เกี่ยวข้องกับความสำเร็จของระบบอีกรวม ๕ องค์ประกอบ ดังนี้

- ๑) ฮาร์ดแวร์ (Hardware) เป็นองค์ประกอบสำคัญของระบบสารสนเทศ หมายถึง เครื่องคอมพิวเตอร์ เครื่องพิมพ์ อุปกรณ์ต่อพ่วง รวมทั้งอุปกรณ์สำหรับเชื่อมโยงเครือข่าย เช่น อุปกรณ์กระจายสัญญาณ
- ๒) ซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ (Software and Program) คือ ลำดับขั้นตอนของคำสั่งที่จะสั่งงานให้ฮาร์ดแวร์ทำงาน เพื่อประมวลผลข้อมูลให้ได้ผลลัพธ์ตามต้องการของการใช้งาน เช่น ซอฟต์แวร์ระบบปฏิบัติงาน ซอฟต์แวร์ควบคุมระบบงาน ซอฟต์แวร์สำเร็จ และซอฟต์แวร์ประยุกต์สำหรับงานต่าง ๆ ในปัจจุบันซอฟต์แวร์มีลักษณะการใช้งานที่ง่ายขึ้น โดยมีรูปแบบการติดต่อที่สื่อความหมายให้เข้าใจง่าย เช่น มีส่วนต่อประสานกราฟิกกับผู้ใช้ที่เรียกว่า Graphical User Interface (GUI) ส่วนซอฟต์แวร์สำเร็จที่มีใช้ในท้องตลาด ทำให้การใช้งานคอมพิวเตอร์ในระดับบุคคลเป็นไปอย่างกว้างขวาง และเริ่มมีลักษณะส่งเสริมการทำงานของกลุ่มมากขึ้น ส่วนงานในระดับองค์กรส่วนใหญ่จะมีการพัฒนาระบบตามความต้องการโดยการว่าจ้าง หรือโดยนักคอมพิวเตอร์ขององค์กร เป็นต้น ซอฟต์แวร์สามารถแบ่งได้ ดังนี้

๓) ข้อมูลเป็นองค์ประกอบที่สำคัญอีกประการหนึ่งของระบบสารสนเทศ อาจจะเป็นตัวชี้วัดความสำเร็จหรือความล้มเหลวของระบบได้ เนื่องจากจะต้องมีการเก็บข้อมูลจากแหล่งกำเนิด ข้อมูลจะต้องมีความถูกต้อง มีการกลั่นกรองและตรวจสอบแล้วเท่านั้นจึงจะมีประโยชน์ ข้อมูล จะเป็นต้องมีมาตรฐาน โดยเฉพาะอย่างยิ่ง เมื่อใช้งานในระดับกลุ่มหรือระดับองค์กร ข้อมูลต้องมีโครงสร้างในการจัดเก็บที่เป็นระบบระเบียบเพื่อการสืบค้นที่รวดเร็วมีประสิทธิภาพ

๔) บุคลากร ในระดับผู้บริหาร ผู้ดูแลระบบ ผู้พัฒนาระบบ นักวิเคราะห์ระบบ นักเขียนโปรแกรม และผู้ใช้บริการ เป็นองค์ประกอบสำคัญในความสำเร็จของระบบสารสนเทศบุคลากรมีความรู้ความสามารถทางคอมพิวเตอร์มากเท่าใด โอกาสที่จะใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ได้เต็มศักยภาพและคุ้มค่ายิ่งขึ้นเท่านั้น โดยเฉพาะระบบสารสนเทศในระดับบุคคลซึ่งเครื่องคอมพิวเตอร์มีขีดความสามารถมากขึ้น ทำให้ผู้ใช้งานมีโอกาสพัฒนาความสามารถของตนเอง และพัฒนาระบบงานได้เองตามความต้องการ สำหรับระบบสารสนเทศในระดับกลุ่มและองค์กรที่มีความซับซ้อนมาก อาจจะต้องใช้บุคลากรในสาขาคอมพิวเตอร์โดยตรงมาพัฒนาและดูแลระบบงาน

๕) ขั้นตอนการปฏิบัติงาน ขั้นตอนการปฏิบัติงานที่ชัดเจนของผู้ใช้หรือของบุคลากรที่เกี่ยวข้อง ก็เป็นเรื่องสำคัญอีกประการหนึ่ง เมื่อได้พัฒนาระบบงานแล้วจำเป็นต้องปฏิบัติงานตามลำดับขั้นตอน และในขณะที่ใช้งานก็จำเป็นต้องคำนึงถึงลำดับขั้นตอน การปฏิบัติของคนและความสัมพันธ์กับเครื่อง ทั้งในกรณีปกติและกรณีฉุกเฉิน เช่น ขั้นตอนการบันทึกข้อมูล ขั้นตอนการประมวลผล ขั้นตอนการปฏิบัติเมื่อเครื่องมือชำรุดหรือข้อมูลสูญหาย และขั้นตอนการทำสำเนาข้อมูลสำรองเพื่อความปลอดภัย เป็นต้น สิ่งเหล่านี้ต้องมีการซักซ้อมมีการเตรียมการ และการทำเอกสารคู่มือการใช้งานให้ชัดเจน

ในการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ให้แก่ระบบสารสนเทศ (Cyber Security) ตามที่กล่าวมาแล้วตามข้างต้น จึงได้มีการศึกษากำหนดแนวทางในการป้องกันความมั่นคงปลอดภัยทางไซเบอร์ของระบบสารสนเทศของ สนข. ขึ้นโดยได้มีการศึกษาจาก ประกาศ นโยบาย แผน กฎหมาย กฎระเบียบที่เกี่ยวข้องต่าง ๆ และมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

๒.๑ กฎหมาย กฎระเบียบ และข้อกำหนดด้านเทคโนโลยีดิจิทัล

ด้านกฎหมายที่จะสนับสนุนการพัฒนาดิจิทัลของประเทศได้มีการดำเนินการมาแล้วเป็นลำดับ แต่ยังคงอยู่ในกระบวนการออกกฎหมายอีกหลายฉบับ ซึ่งกฎหมายเหล่านี้จะเป็นการให้ความมั่นใจและกำหนดกฎกติกาการดำเนินการโดยใช้ดิจิทัลอย่างปลอดภัย ยุติธรรม และตั้งอยู่บนพื้นฐานของความเท่าเทียมกัน สรุปได้ดังนี้

๒.๑.๑ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

หมวด ๑ ธุรกรรมทางอิเล็กทรอนิกส์

๑) การรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ ในมาตรา ๗ กล่าวว่า “ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใด เพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์” ซึ่งจะเห็นได้ว่าบทบัญญัตินี้เป็นหลักการพื้นฐานที่มีให้มีการเลือกปฏิบัติระหว่างสิ่งที่จัดทำขึ้นในรูปของหนังสือ หลักฐานเป็นหนังสือ หรือต้นฉบับ (Original) กับสิ่งที่จัดทำขึ้นในรูปของข้อมูลอิเล็กทรอนิกส์

๒) การทำเป็นหนังสือ มาตรา ๘ บัญญัติไว้ว่า “ภายใต้บังคับบทบัญญัติแห่งมาตรา ๙ ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและน ากลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือมีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว” ซึ่งกล่าวได้ว่า มาตรา ๘ นั้นเป็นการบัญญัติ เพื่อขยายหลักการรับรองสถานะของข้อมูลอิเล็กทรอนิกส์ในมาตรา ๗

ในกรณีที่กฎหมายตามประมวลกฎหมายแพ่งและพาณิชย์บัญญัติให้ต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ ให้สามารถทำในรูปของข้อมูลอิเล็กทรอนิกส์ได้ แต่ทั้งนี้ต้องอยู่ภายใต้เงื่อนไขว่าข้อมูลอิเล็กทรอนิกส์นั้นต้องนำกลับมาใช้ใหม่ได้โดยที่ความหมายไม่เปลี่ยนแปลง

๓) การลงลายมือชื่อ หลักการนี้ปรากฏอยู่ในมาตรา ๙ ซึ่งสรุปได้ว่าในกรณีที่บุคคลลงลายมือชื่อในหนังสือให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้าบุคคลนั้นใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อได้ และสามารถจะแสดงได้ว่าเจ้าของลายมือชื่อนั้นรับรองข้อความในข้อมูลอิเล็กทรอนิกส์ว่าเป็นของตน โดยวิธีดังกล่าวจะต้องเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

๔) ต้นฉบับหลักการนี้ปรากฏอยู่ในมาตรา ๑๐ กล่าวโดยสรุปได้ว่า ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความหรือเอกสารที่เป็นต้นฉบับ หากได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์นั้นโดยวิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความนั้น ตั้งแต่การสร้างข้อความจนถึงข้อความที่เสร็จสมบูรณ์ และสามารถแสดงข้อความนั้นในภายหลังได้ ก็ให้ถือว่าได้มีการนำเสนอข้อความหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

๕) การรับฟังพยานหลักฐานและชี้แจงน้ำหนักพยานหลักฐานปรากฏอยู่ในมาตรา ๑๑ บทบัญญัติในมาตรานี้ เป็นการห้ามปฏิเสธการรับฟังพยานหลักฐานในกระบวนการพิจารณาด้วยเหตุที่ข้อมูลนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ แต่ทั้งนี้ในเรื่องของการรับฟังพยานหลักฐานเป็นดุลยพินิจของศาลที่จะรับฟังหรือไม่ก็ได้ กฎหมายจึงต้องกำหนดหลักเกณฑ์ในการชี้แจงน้ำหนักพยานหลักฐานไว้ โดยให้พิจารณาถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้างการเก็บรักษาหรือการสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการในการระบุตัวผู้ส่งรวมถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง

๖) การเก็บรักษาเอกสารหรือข้อความปรากฏอยู่ในมาตรา ๑๒ โดยหลักการนี้ให้ความสำคัญว่า ข้อความหรือข้อมูลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้นต้องตรงกับเนื้อหาของข้อความหรือข้อมูลของเอกสารก่อนที่จะมีการจัดเก็บให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้น

ส่วนหลักการต่าง ๆ ที่ปรากฏอยู่ในมาตรา ๑๓ ถึงมาตรา ๒๔ อันได้แก่ หลักการว่าด้วยเรื่อง การทำคำเสนอหรือคำสนองในรูปข้อมูลอิเล็กทรอนิกส์ เจ้าของข้อมูลอิเล็กทรอนิกส์ วิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ เวลาและสถานที่ซึ่งถือว่าได้มีการส่งหรือรับข้อมูลอิเล็กทรอนิกส์นั้น เป็นบทบัญญัติซึ่งคู่กรณีสามารถตกลงเปลี่ยนแปลงเป็นอย่างอื่นได้ นอกจากนั้นยังมีการบัญญัติหลักการเรื่อง วิธีการแบบปลอดภัย ไว้ในมาตรา ๒๕ ซึ่งบัญญัติขึ้นเพื่อให้กฎหมายมีความยืดหยุ่นในการปรับใช้กับเทคโนโลยีต่าง ๆ ที่มีอยู่ในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต แต่กฎหมายไม่ได้บัญญัติรายละเอียดถึงวิธีการที่จะถือว่าเป็นวิธีการที่เชื่อถือได้ จึงเป็นหน้าที่ของผู้ใช้เทคโนโลยีที่จะต้องพิจารณาว่า วิธีการใดที่จะถือว่าเป็นวิธีการที่ปลอดภัย รวมทั้งผู้ใช้อังต้องมีหน้าที่ในการพิสูจน์ด้วยว่า เพราะเหตุใดวิธีการดังกล่าวจึงเป็นวิธีการที่น่าเชื่อถือตามกฎหมาย

๒.๑.๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

สาระสำคัญของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ ในส่วนที่เกี่ยวข้อง มีดังนี้

๑) มาตรา ๓ ให้เพิ่มความต่อไปนี้เป็นวรรคสองของมาตรา ๘ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ “ในกรณีที่กฎหมายกำหนดให้ต้องมีการปิดอากรแสตมป์ หากได้มีการชำระเงินแทน หรือดำเนินการอื่นใดด้วยวิธีการทางอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่หน่วยงานของรัฐซึ่งเกี่ยวข้อง ประกาศกำหนดให้ถือว่าหนังสือหลักฐานเป็นหนังสือหรือเอกสารซึ่งมีลักษณะ

เป็นตรานั้น ได้มีการปิดอากรแสตมป์และขีดฆ่าตามกฎหมายนั้นแล้ว ในการนี้ในการกำหนดหลักเกณฑ์และวิธีการของหน่วยงานของรัฐดังกล่าว คณะกรรมการจะกำหนดกรอบและแนวทางเพื่อเป็นมาตรฐานทั่วไปไว้ด้วยก็ได้”

๒) มาตรา ๔ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ “วิธีการที่เชื่อถือได้ตาม (๒) ให้คำนึงถึงความมั่นคงและรัดกุมของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคล สภาพพร้อมใช้งานของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมายระดับความมั่นคงปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์ การปฏิบัติตามกระบวนการในการระบุตัวบุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับ วิธีการที่ใช้ในการระบุตัวบุคคลในการทำธุรกรรม วิธีการระบุตัวบุคคล ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

๓) มาตรา ๕ ให้เพิ่มความต่อไปนี้เป็นวรรคสี่ของมาตรา ๑๐ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ “ในกรณีที่มีการทำสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่งสำหรับใช้อ้างอิงข้อความของข้อมูลอิเล็กทรอนิกส์ หากสิ่งพิมพ์ออกนั้นมีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์ และมีการรับรองสิ่งพิมพ์ออกโดยหน่วยงานที่มีอำนาจตามที่คณะกรรมการประกาศกำหนดแล้วให้ถือว่าสิ่งพิมพ์ออกดังกล่าวใช้แทนต้นฉบับได้”

๔) มาตรา ๖ ให้ยกเลิกความในมาตรา ๑๑ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และให้ใช้ความต่อไปนี้เป็น “มาตรา ๑๑ ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมาย ทั้งในคดีแพ่งคดีอาญาหรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์ในการชั่งน้ำหนักพยานหลักฐานว่า ข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้นให้พิจารณาถึงความน่าเชื่อถือของลักษณะ หรือวิธีการที่ใช้สร้างเก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะ หรือวิธีการเก็บรักษาความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้อง ทั้งปวงให้น้ำความในวรรคหนึ่งมาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย”

๒.๑.๓ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

สาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ในส่วนที่เกี่ยวข้อง มีดังนี้

ภาพรวมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แบ่งเป็น การกระทำความผิดต่อระบบ การกระทำความผิดต่อข้อมูล การกระทำความผิดของผู้ให้บริการ และการกระทำความผิดของพนักงานเจ้าหน้าที่ ซึ่งมีโทษจำคุก/ปรับ/ทั้งจำทั้งปรับ ประกอบด้วย

๑) ระบบ

- เข้าถึงระบบของผู้อื่น
- เผยแพร่
- ระบุ/ขัดขวาง/รบกวน ทำให้ระบบทำงานไม่ได้

๒) ข้อมูล

- เข้าถึง ดักจับ ทำงาน/แก้ไข/ปลอมแปลง
- นำเข้า/ส่งต่อ ข้อมูลปลอม/เท็จ/ลามก/กระทบความมั่นคง
- ระบุ/ขัดขวาง/รบกวน ทำให้ระบบทำงานไม่ได้

๓) ผู้ให้บริการ

- สนับสนุน /ยินยอมให้กระทำความผิด
- ไม่เก็บรักษาข้อมูลจราจร >= ๙๐

๔) พนักงานเจ้าหน้าที่

- เผยแพร่/ส่งมอบ ข้อมูลคอมพิวเตอร์/ข้อมูลจราจร/ข้อมูลผู้ให้บริการ
- ไม่ปฏิบัติตามมาตรา ๑๘ - ๒๑ เพื่อหาผู้กระทำความผิด
- ประมาท ทำให้ผู้อื่นรู้ข้อมูล

๒.๑.๔ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

พ.ศ. ๒๕๔๙

จากการที่ประเทศไทยได้เริ่มเข้าสู่ยุคสังคมสารสนเทศ ซึ่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น จึงมีการสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตน โดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับให้หน่วยงานของรัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทำอิเล็กทรอนิกส์ ประกอบกับมาตรา ๓๕ วรรค ๑ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ บัญญัติว่า คำขอการอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาแล้ว ให้ถือว่ามิผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด จึงจำเป็นต้องตราพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โดยมีสาระสำคัญ ดังนี้

๒.๑.๔.๑ ให้หน่วยงานรัฐต้องจัดให้มีระบบเอกสารในรูปแบบอิเล็กทรอนิกส์ ในมาตรา ๓ ได้กำหนดให้การทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ หน่วยงานของรัฐจะต้องจัดให้มีระบบเอกสารที่ทำในรูปแบบอิเล็กทรอนิกส์ โดยมีลักษณะดังต่อไปนี้

๑) เอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์นั้นต้องอยู่ในรูปแบบที่เหมาะสม โดยสามารถแสดงหรืออ้างอิงเพื่อใช้ในภายหลังและยังคงความครบถ้วนของข้อความในรูปแบบของข้อมูลอิเล็กทรอนิกส์

๒) ต้องกำหนดระยะเวลาเริ่มต้นและสิ้นสุดในการยื่นเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ โดยปกติให้ยึดถือวันเวลาของการปฏิบัติงานหน่วยงานของรัฐนั้นเป็นหลัก และอาจกำหนดระยะเวลาในการดำเนินการพิจารณาของหน่วยงานของรัฐด้วยวิธีการทำอิเล็กทรอนิกส์ไว้ด้วยก็ได้เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

๓) ต้องกำหนดวิธีการที่ทำให้สามารถระบุตัวเจ้าของลายมือชื่อ ประเภท ลักษณะ หรือรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์

๔) ต้องกำหนดวิธีการแจ้งการตอบรับด้วยวิธีการทางอิเล็กทรอนิกส์หรือด้วยวิธีการอื่นใด เพื่อเป็นหลักฐานว่า ได้มีการดำเนินการด้วยวิธีการทำอิเล็กทรอนิกส์ไปยังอีกฝ่ายหนึ่งแล้ว

๒.๑.๔.๒ ให้มีระบบเอกสารในรูปแบบอิเล็กทรอนิกส์ในการพิจารณาดีทางปกครอง โดยวิธีการทางอิเล็กทรอนิกส์ของรัฐตามบทบัญญัติแห่งมาตรา ๔ นอกจากที่บัญญัติไว้ในมาตรา ๓ ในกรณีนี้ หน่วยงานของรัฐจัดทำกระบวนการพิจารณาทางปกครองโดยวิธีการทางอิเล็กทรอนิกส์ ระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ต้องมีลักษณะดังต่อไปนี้ด้วย เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

๑) มีวิธีการสื่อสารกับผู้ยื่นคำขอในกรณีที่เอกสารมีข้อบกพร่องหรือมีข้อความที่ผิดพลาด อันเห็นได้ชัดว่าเกิดจากความไม่รู้หรือความเลินเล่อของผู้ยื่นคำขอหรือการขอข้อเท็จจริงเพิ่มเติม รวมทั้งมีวิธีการแจ้งสิทธิและหน้าที่ในกระบวนการพิจารณาทางปกครองตามความจำเป็นแก่กรณีในกรณีที่กฎหมายกำหนดให้ต้องแจ้งให้คู่กรณีทราบ

๒) ในกรณีมีความจำเป็นตามลักษณะเฉพาะของธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐใด หน่วยงานของรัฐนั้นอาจกำหนดเงื่อนไขว่า คู่กรณียินยอมตกลงและยอมรับการดำเนินการพิจารณาทางปกครองของหน่วยงานของรัฐโดยวิธีการทางอิเล็กทรอนิกส์

๒.๑.๔.๓ ให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศจากบทบัญญัติในมาตรา ๕ พระราชบัญญัติการธุรกรรมอิเล็กทรอนิกส์ภาครัฐฯ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ซึ่งนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๒.๑.๔.๔ ให้หน่วยงานภาครัฐจัดทำนโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ในมาตรา ๖ ในกรณีที่มีการรวบรวมจัดเก็บใช้หรือเผยแพร่ข้อมูลหรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลด้วย

๒.๑.๔.๕ ให้หน่วยงานของรัฐจัดทำประกาศ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ และนโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ในมาตรา ๗ นโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจึงมีผลใช้บังคับได้ โดยหน่วยงานของรัฐต้องปฏิบัติตามนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และจัดให้มีการตรวจสอบการปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

๒.๑.๔.๖ ให้คณะกรรมการจัดทำตัวอย่างเบื้องต้น สำหรับการดำเนินการของหน่วยงานของรัฐให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำนโยบายและแนวปฏิบัติ หรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชบัญญัตินี้ ไว้เป็นตัวอย่างเบื้องต้นสำหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชบัญญัตินี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

๒.๑.๔.๗ การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐตามหลักเกณฑ์และวิธีการตามพระราชบัญญัตินี้ ไม่มีข้อยกเว้นในมาตรา ๙ การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐตามหลักเกณฑ์และวิธีการตามพระราชบัญญัตินี้ ไม่มีผลเป็นการยกเว้นกฎหมายหรือหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้น กำหนดไว้เพื่อการอนุญาต อนุมัติ การให้ความเห็นชอบ หรือการวินิจฉัย

๒.๑.๕ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม

ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้มีการกำหนดแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ เพื่อให้หน่วยงานภาครัฐมีการดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ และมีระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล มีสาระสำคัญ ดังนี้

๒.๑.๕.๑ หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

๒.๑.๕.๒ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงาน

๒.๑.๕.๓ ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย โดยต้องมีข้อปฏิบัติ ดังนี้

๑) มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ
๒) มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ
๓) ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบ สารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและผ่านการฝึกอบรมหลักสูตรการสร้างความรู้ความตระหนักเรื่องความมั่นคง ปลอดภัยสารสนเทศเพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๔) ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึง โดยไม่ได้รับอนุญาตการเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ ประมวลผลสารสนเทศ

๕) ให้มีการควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่าย โดยไม่ได้รับอนุญาต

๖) ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบ ปฏิบัติการโดยไม่ได้รับอนุญาต

๗) ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

๘) หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง

๙) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑๐) หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด

๑๑) หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคง ปลอดภัย ด้านสารสนเทศที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่าข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า

๒.๑.๖ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำ หรือแปลงเอกสารและข้อความให้อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

ตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม พ.ศ. ๒๕๕๑ มีสาระสำคัญเพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการทำธุรกรรมหรือสัญญา ให้มีผลเช่นเดียวกับการทำสัญญาตามหลักเกณฑ์ที่กฎหมายปัจจุบัน (ประมวลกฎหมายแพ่งและพาณิชย์) กำหนดไว้ได้แก่การทำเป็นหนังสือ หลักฐานเป็นหนังสือ การลงลายมือชื่อ กล่าวคือ ถ้ามีการทำสัญญาระหว่างบุคคล ที่ใช้ข้อมูลอิเล็กทรอนิกส์หรือลายมือชื่ออิเล็กทรอนิกส์ตามความหมายของกฎหมายแล้ว กฎหมายนี้ถือว่า การทำสัญญานั้นได้ทำตามหลักเกณฑ์ข้างต้นของกฎหมายแพ่งและพาณิชย์แล้ว เป็นผลทำให้สัญญานั้น

มีผลสมบูรณ์ หรือใช้บังคับได้ตามกฎหมาย ทั้งนี้เป็นไปตามเงื่อนไขที่กฎหมายธุรกรรมทางอิเล็กทรอนิกส์กำหนด นอกจากนี้ ในมาตรา ๑๒/๑ วรรค ๒ กำหนดให้การจัดทำ แปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กำหนด ดังนั้น คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศ เรื่อง “หลักเกณฑ์และวิธีการในการจัดทำ หรือแปลงเอกสาร และข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓” โดยมีวัตถุประสงค์เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือและมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรม โดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิมโดยมีสาระสำคัญ ดังนี้

๒.๑.๖.๑ ให้มีการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ให้มีกระบวนการในการจัดทำหรือแปลงเอกสารและข้อความอย่างน้อย ดังนี้

๑) กระบวนการจัดทำหรือแปลงเอกสารและข้อความให้เป็นข้อมูลอิเล็กทรอนิกส์ ด้วยวิธีการทางอิเล็กทรอนิกส์

๒) กระบวนการตรวจสอบและรับรองว่าข้อมูลอิเล็กทรอนิกส์ที่จัดทำหรือแปลง นั้นมีความหมายเหมือนกับเอกสารและข้อความเดิม

๓) กระบวนการบันทึกหลักฐานการดำเนินการจัดทำหรือแปลงเอกสาร และข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

๔) กระบวนการบันทึกเมตาดาตาในรูปแบบอิเล็กทรอนิกส์ที่เป็นข้อความบรรยาย สาระสำคัญของเอกสารและข้อความซึ่งต้องครอบคลุมให้สามารถสืบค้นเอกสารและข้อความนั้นได้ถูกต้อง

๒.๑.๖.๒ การจัดทำหรือแปลงเอกสารและข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ ให้มีผู้รับผิดชอบดำเนินการในการจัดทำหรือแปลงในเรื่องของวิธีการดังกล่าว อย่างน้อยดังต่อไปนี้

๑) จัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

๒) ตรวจสอบและรับรองความถูกต้องและครบถ้วนของข้อมูลอิเล็กทรอนิกส์ ที่ได้จากการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ว่า ข้อมูลอิเล็กทรอนิกส์ มีความหมาย หรือรูปแบบเหมือนกับเอกสารและข้อความเดิม

๓) ตรวจสอบกระบวนการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูป ของข้อมูลอิเล็กทรอนิกส์ให้เป็นไปตามที่กำหนดไว้

๔) ตรวจสอบและรับรองความถูกต้องและครบถ้วนของเมตาดาตา

๒.๑.๖.๓ การจัดทำหรือแปลงเอกสารและข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ ให้มีการกำหนดมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นวิธีการที่เชื่อถือได้ อย่างน้อยต้องครอบคลุมหัวข้อต่อไปนี้

๑) การระบุตัวตน (Identification)

๒) การยืนยันตัวตน (Authentication)

๓) อนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization)

๔) ความรับผิดชอบต่อผลของการกระทำ (Accountability)

๒.๑.๖.๔ การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้น ให้ข้อมูลอิเล็กทรอนิกส์มีความละเอียดและความชัดเจนของเอกสารและข้อความเดิม ให้ผู้จัดทำหรือแปลง มีหน้าที่รักษาและดำรงสภาพของระบบการจัดทำหรือแปลงเอกสารไว้ให้สมบูรณ์ เพื่อให้มีการกำกับดูแล หรือการตรวจสอบได้ตลอดเวลา จากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ หรือหน่วยงานอื่นที่คณะกรรมการ ธุรกรรมทางอิเล็กทรอนิกส์มอบหมายหรือหน่วยงานที่กำหนดไว้เป็นอย่างอื่น

๒.๒ นโยบายและแผนที่เกี่ยวข้อง

นโยบายและแผนที่เกี่ยวข้อง ซึ่งได้ทำการศึกษาประกอบ อย่างน้อยได้แก่

๒.๒.๑ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้มีการกำหนดแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ เพื่อให้หน่วยงานภาครัฐมีการดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ และมีระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล มีสาระสำคัญ ดังนี้

๒.๒.๑.๑ หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

๒.๒.๑.๒ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงาน

๒.๒.๑.๓ ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย โดยต้องมีข้อปฏิบัติ ดังนี้

๑) มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ
๒) มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ
๓) ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบ สารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและผ่านการฝึกอบรมหลักสูตรการสร้างตระหนักรู้เรื่องความมั่นคง ปลอดภัยสารสนเทศเพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๔) ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึง โดยไม่ได้รับอนุญาตการเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ ประมวลผลสารสนเทศ

๕) ให้มีการควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่าย โดยไม่ได้รับอนุญาต

๖) ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบ ปฏิบัติการโดยไม่ได้รับอนุญาต

๗) ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

๘) หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง

๙) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑๐) หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด

๑๑) หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่าข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า

๒.๒.๒ แผนปฏิบัติการดิจิทัลของ สนข. พ.ศ. ๒๕๖๖ - ๒๕๗๐

สนข. ได้จัดทำแผนปฏิบัติการดิจิทัลของ สนข. พ.ศ. ๒๕๖๖ - ๒๕๗๐ สอดคล้องกับ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และแผนพัฒนาารัฐบาล ดิจิทัลของประเทศไทย พ.ศ. ๒๕๖๖ - ๒๕๗๐ รวมทั้งนโยบาย ยุทธศาสตร์ และแผนระดับต่าง ๆ ที่เกี่ยวข้อง และมีระยะเวลาดำเนินงานที่สอดคล้องกับแผนพัฒนาารัฐบาลดิจิทัลของประเทศไทย โดยมีจุดประสงค์เพื่อใช้เป็นกรอบ แนวทางในการดำเนินงานด้านดิจิทัลของ สนข. ในระยะ ๕ ปีดังกล่าว และเพื่อรองรับการพัฒนา สนข. สู่ระบบ

ราชการ ๔.๐ ที่มุ่งพัฒนางานในมิติระบบราชการที่เปิดกว้างและเชื่อมโยงกัน ยึดประชาชนเป็นศูนย์กลาง มีขีดสมรรถนะสูงและทันสมัย ประกอบด้วยยุทธศาสตร์ จำนวน ๕ ข้อ ๑๓ กลยุทธ์ ดังนี้

ยุทธศาสตร์ที่ ๑ พัฒนาข้อมูล ระบบข้อมูล และฐานข้อมูล เพื่อยกระดับเป็นศูนย์ข้อมูล ด้านการขนส่งและจราจรที่มีคุณภาพตามมาตรฐานธรรมาภิบาลข้อมูลภาครัฐ (Database & Data Center)

- กลยุทธ์ที่ ๑ ปรับปรุงฐานข้อมูล และจัดทำข้อมูลตามหลักธรรมาภิบาล ข้อมูล เพื่อการเปิดเผย เชื่อมโยง และแลกเปลี่ยนข้อมูล (Data)

- กลยุทธ์ที่ ๒ ดำเนินการบริหารจัดการข้อมูลตามหลักธรรมาภิบาล ข้อมูลภาครัฐ (Data Governance)

- กลยุทธ์ที่ ๓ ดำเนินการด้านข้อมูลส่วนบุคคลให้เป็นไปตามแนวทางการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)

- กลยุทธ์ที่ ๔ กำหนดแนวปฏิบัติ/ คู่มือการดำเนินการเกี่ยวกับข้อมูล ส่วนบุคคลของ สนข.

ยุทธศาสตร์ที่ ๒ จัดทำรายงานการวิเคราะห์และคาดการณ์สภาพการขนส่งและจราจร โดยใช้เทคโนโลยีการวิเคราะห์ข้อมูล (Data Analytics) เพื่อการจัดทำนโยบายและแผนพัฒนาระบบคมนาคม ไปสู่ Digital Transport (Data Analytics for Plan & Policy)

- กลยุทธ์ที่ ๕ นำข้อมูลไปใช้วิเคราะห์เชิงนโยบาย เพื่อสนับสนุน การตัดสินใจกำหนดนโยบายและจัดทำแผนพัฒนาระบบคมนาคม (Data Analysis)

- กลยุทธ์ที่ ๖ ใช้เทคโนโลยีและนวัตกรรมการขนส่งพัฒนาระบบคมนาคม ให้เป็น Digital Transport (Plan & Policy)

ยุทธศาสตร์ที่ ๓ สื่อสารและประชาสัมพันธ์เพื่อสร้างมูลค่าเพิ่มของข้อมูลสารสนเทศ นโยบายและแผนด้านการขนส่งและจราจร (Communication & Service)

- กลยุทธ์ที่ ๗ เปิดเผยข้อมูลแก่สาธารณะและพัฒนาการบริการข้อมูล ผ่านช่องทางดิจิทัลเพื่อให้ทุกภาคส่วนเข้าถึงและมีส่วนร่วมในการเสนอแนะและตัดสินใจเชิงนโยบาย (Information & Participation)

ยุทธศาสตร์ที่ ๔ พัฒนาศักยภาพบุคลากร ให้มีความพร้อมเพื่อเพิ่มประสิทธิภาพ ในการปฏิบัติงาน (Digital Skill & Knowledge)

- กลยุทธ์ที่ ๘ กำหนดกรอบการพัฒนาทักษะและความรู้ด้านดิจิทัล ตามมาตรฐานสมรรถนะดิจิทัล รวมทั้งฝึกอบรมและวัดผล (HR Planning & Training)

ยุทธศาสตร์ที่ ๕ พัฒนาระบบการบริหารจัดการมุ่งสู่องค์กรดิจิทัล (Digital Management)

- กลยุทธ์ที่ ๙ ส่งเสริมวัฒนธรรมการใช้เทคโนโลยีดิจิทัลแก่บุคลากร (Digital Culture)

- กลยุทธ์ที่ ๑๐ ปรับเปลี่ยนกระบวนการทำงานให้เป็นดิจิทัลโดยใช้ระบบ บริหารจัดการรูปแบบดิจิทัล (Re-Process)

- กลยุทธ์ที่ ๑๑ สร้างความเชื่อมั่นต่อระบบการปฏิบัติงานและการให้ บริการว่าปลอดภัยจากภัยคุกคามทางไซเบอร์ (Infrastructure & Security)

- กลยุทธ์ที่ ๑๒ กำหนดแนวปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

- กลยุทธ์ที่ ๑๓ จัดหา พัฒนา ปรับปรุงโครงสร้างพื้นฐานด้านดิจิทัล ของ สนข. ให้มีความทันสมัยรองรับการดำเนินงานในรูปแบบดิจิทัลที่มีความมั่นคงปลอดภัย

ทั้งนี้ ในการจัดทำแผนการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ สนข. พ.ศ. ๒๕๖๙ - ๒๕๗๐ มุ่งเน้นเรื่องของการบริหารจัดการและเพิ่มประสิทธิภาพการป้องกันและรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้แก่ระบบสารสนเทศและข้อมูลของ สนข. ให้มีความปลอดภัย มีการดำเนินการทั้งในด้านการรักษาความลับของข้อมูล (Confidentiality) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) อีกทั้งต้องเป็นไปตามมาตรฐานสากล ดังนั้น จึงสอดคล้องในแนวคิดการยกระดับ สนข. ให้เป็นองค์กรดิจิทัล ซึ่งเป็นไปตามยุทธศาสตร์ที่ ๕ กลยุทธ์ที่ ๑๑ - ๑๓ ตามที่กล่าวข้างต้น

๒.๒.๓ แผนพัฒนาระดับความพร้อมรัฐบาลดิจิทัลของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ - ๒๕๗๐

สนข. ได้จัดทำแผนพัฒนาระดับความพร้อมรัฐบาลดิจิทัลของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ - ๒๕๗๐ เพื่อใช้เป็นกรอบแนวทางติดตามผลการดำเนินงานด้านดิจิทัลของ สนข. การดำเนินโครงการ/กิจกรรม ที่เกี่ยวกับการใช้เทคโนโลยีดิจิทัลสำหรับการพัฒนาระบบการบริหารงานภาครัฐภายใน สนข. และเพื่อการวัดระดับความพร้อมรัฐบาลดิจิทัลของ สนข. โดยมีเป้าหมายสำคัญ คือ “ในปี พ.ศ. ๒๕๗๐ มีคะแนนผลการสำรวจระดับความพร้อมการพัฒนารัฐบาลดิจิทัลในภาพรวมให้อยู่ในอันดับที่ไม่ต่ำกว่าอันดับที่ ๔๐ โดยแต่ละปีมีคะแนนระดับความพร้อมของตัวชี้วัด (Pillar) เพิ่มขึ้นตัวชี้วัดละ ๑ ระดับ” เพื่อการขับเคลื่อน สนข. ให้เป็นองค์กรดิจิทัลต่อไป ซึ่งภายในแผนประกอบด้วยโครงการและกิจกรรมต่าง ๆ รวมถึงการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ด้วย

ในการยกระดับ สนข. ให้เป็นองค์กรดิจิทัล ใช้กรอบตามแบบจำลองวุฒิภาวะรัฐบาลดิจิทัล (Digital Government Maturity Model) ของสำนักงานข้าราชการพลเรือน (สำนักงาน ก.พ.) โดยแนวคิดการยกระดับ สนข. ให้เป็นองค์กรดิจิทัล โดยมีตัวชี้วัดหลัก (Pillar) ดังนี้

Pillar ๑ แผนนโยบายและหลักปฏิบัติ (Policies & Practices)

Pillar ๒ กระบวนการพัฒนาด้วยข้อมูล (Data-driven Practices)

Pillar ๓ ศักยภาพเจ้าหน้าที่ภาครัฐด้านดิจิทัล (Digital Capabilities)

Pillar ๔ บริการภาครัฐ (Public Services)

Pillar ๕ การบริหารจัดการรูปแบบดิจิทัล (Smart Back Office)

Pillar ๖ โครงสร้างพื้นฐานความมั่นคงปลอดภัยและมีประสิทธิภาพ (Secure and Efficient Infrastructure)

Pillar ๗ เทคโนโลยีดิจิทัลและการนำไปใช้ (Digital Technological Practices)
ภายใต้แนวทางการดำเนินงานยุทธศาสตร์ ๕ ด้าน ต่อไปนี้

ยุทธศาสตร์ที่ ๑ พัฒนาข้อมูล ระบบข้อมูล และฐานข้อมูล เพื่อยกระดับเป็นศูนย์ข้อมูลด้านการขนส่งและจราจรที่มีคุณภาพตามมาตรฐานธรรมาภิบาลข้อมูลภาครัฐ (Database & Data Center)

ยุทธศาสตร์ที่ ๒ จัดทำรายงานการวิเคราะห์และคาดการณ์สภาพการขนส่งและจราจร โดยใช้เทคโนโลยีการวิเคราะห์ข้อมูล (Data Analytics) เพื่อการจัดทำนโยบายและแผนพัฒนาระบบคมนาคมไปสู่ Digital Transport (Data Analytics for Plan & Policy)

ยุทธศาสตร์ที่ ๓ สื่อสารและประชาสัมพันธ์เพื่อสร้างมูลค่าเพิ่มของข้อมูลสารสนเทศ นโยบายและแผนด้านการขนส่งและจราจร (Communication & Service)

ยุทธศาสตร์ที่ ๔ พัฒนาศักยภาพบุคลากรให้มีความพร้อมเพื่อเพิ่มประสิทธิภาพในการปฏิบัติงาน (Digital Skill & Knowledge)

ยุทธศาสตร์ที่ ๕ พัฒนาระบบการบริหารจัดการมุ่งสู่องค์กรดิจิทัล (Digital Management)

๒.๒.๔ แผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

สนข. ได้มีการประกาศแผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สนข. เพื่อใช้เป็นแนวทางและแนวปฏิบัติให้การใช้งานระบบเทคโนโลยีสารสนเทศ สนข. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อ สนข. แบ่งออกเป็น ๗ หมวด ได้แก่

หมวดที่ ๑ การควบคุมและการเข้าถึงการใช้งานระบบสารสนเทศ

หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและการสำรองข้อมูล

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่และสภาพแวดล้อม

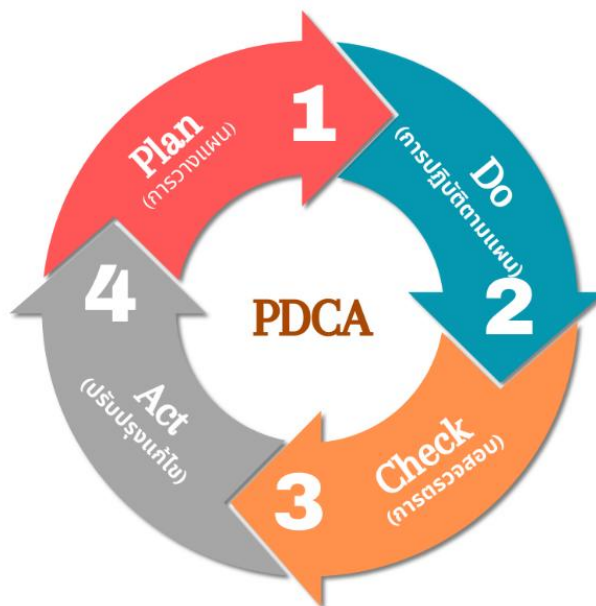
หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศ

หมวดที่ ๗ หน้าที่และความรับผิดชอบ

๒.๓ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

การนำมาตรฐานการรักษาความมั่นคงปลอดภัยมาประยุกต์ใช้กับระบบสารสนเทศในองค์กร เริ่มเป็นที่แพร่หลายมากขึ้น มาตรฐาน ISO/IEC 27001 ก็เป็นมาตรฐานหนึ่งที่ได้รับนิยมนิยามในปัจจุบัน และได้รับการยอมรับจากหลายประเทศในการนำไปใช้บริหารจัดการระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานที่พัฒนามาจากมาตรฐานในตระกูล ISO/IEC 27000 ซึ่งเกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security Management System: ISMS) ได้ผ่านการปรับปรุงและเผยแพร่เมื่อเดือนตุลาคม ๒๕๕๘ โดย International Organization for Standardization (ISO) และ International Electrotechnical Commission (IEC) มีจุดประสงค์เพื่อให้องค์กรสามารถบริหารจัดการทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างมีระบบและเหมาะสมต่อการดำเนินภารกิจขององค์กร เริ่มแรกองค์กรต้องทำการวิเคราะห์ความเสี่ยงของระบบจากภัยคุกคามและจุดอ่อนต่าง ๆ โดยการประเมินความเสี่ยง และการจัดการกับความเสี่ยง เช่น ลด โอนย้าย หรือยอมรับความเสี่ยง (Risk Assessment and Treatment) เพื่อรักษาระบบสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม และพอเพียง ขณะเดียวกันมาตรฐานนี้ยังกำหนดให้องค์กรต้อง ควบคุมดูแลระบบรักษาความมั่นคงปลอดภัย และกลไกในการพัฒนาอย่างต่อเนื่องอีกด้วย นอกจากนี้ มาตรฐาน ISO/IEC 27001 ยังประกอบไปด้วยวงจรบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act (การวางแผน-การปฏิบัติ-การตรวจสอบ-การปรับปรุง) ดังแสดงในภาพที่ ๒-๑



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

๒.๓.๑ กระบวนการการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ
(อ้างอิงข้อกำหนดตามมาตรฐาน ISO/IEC 27001)

๒.๓.๑.๑ รายละเอียดของระบบบริหารจัดการความปลอดภัยสำหรับสารสนเทศ

๑) ข้อกำหนดทั่วไป

องค์กรจะต้องกำหนดลงมือปฏิบัติดำเนินการ เฝ้าระวัง ทบทวน บำรุงรักษา และปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ได้กำหนดไว้เป็นสายลักษณะอักษร ภายในรอบกิจกรรม การดำเนินการตามภารกิจต่าง ๆ รวมทั้งความเสี่ยงที่เกี่ยวข้อง แนวทางที่ใช้ในมาตรฐานนี้จะนำกระบวนการ ดำเนินงานที่มีคุณภาพตามวงจร Plan-Do-Check-Act มา ประยุกต์ใช้จากภาพที่ ๒-๑ แสดงให้เห็นถึงแบบจำลอง ขั้นตอนการทำงานของระบบ ISMS ที่ตรงตามความต้องการของกลุ่มองค์กร รวมถึงระบบการปฏิบัติงานต่าง ๆ ที่เกิดขึ้นทำให้ระบบรักษาความมั่นคงปลอดภัยข้อมูลตรงตามความต้องการและความคาดหวังได้ ซึ่งแต่ละขั้นตอน ประกอบด้วยรายละเอียดโดยย่อ ดังนี้

- Plan คือ การวางแผนการกำหนดนโยบายความมั่นคงและจัดทำระบบ บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) องค์กรควรกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยและกำหนดนโยบายความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะขององค์กร สถานที่ตั้ง ทรัพยากร และเทคโนโลยี นอกจากนี้ ยังต้องกำหนดวิธีการประเมิน ความเสี่ยงที่เป็นรูปธรรมขององค์กร ระบบความเสี่ยง วิเคราะห์และ ประเมินความเสี่ยง ระบบและประเมินทางเลือก ในการจัดการกับความเสี่ยงการดำเนินการที่เป็นไปได้ เลือกวัตถุประสงค์และมาตรการทางด้านความปลอดภัย เพื่อจัดการกับความเสี่ยง

- Do คือ การลงมือปฏิบัติหรือดำเนินการตามระบบ ISMS องค์กรควรจัดทำ แผนการจัดการความเสี่ยง ลงมือปฏิบัติตามแผนการจัดการความเสี่ยงและตามมาตรฐานที่เลือกไว้

- Check คือ การตรวจสอบและทบทวนผลการดำเนินการตามระบบ ISMS องค์กรควรลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่น ๆ สำหรับการเฝ้าระวังและทบทวนดำเนินการทบทวน ความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ วัดความสัมฤทธิ์ผลของมาตรการ ทางด้านความมั่นคงปลอดภัย ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้กับระดับความเสี่ยง ที่เหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ ดำเนินการตรวจสอบและทบทวนระบบบริหารจัดการความมั่นคง

ปลอดภัย ปรับปรุงแผนทางด้านการความปลอดภัยโดยนำผลของการเฝ้าระวังและทบทวนกิจกรรมต่าง ๆ มาพิจารณาร่วมด้วย บันทึกผลการดำเนินการซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

- Act คือ การแก้ไข บำรุงรักษา และปรับปรุงคุณภาพของระบบ ISMS เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบและมีการพัฒนาขึ้นอย่างต่อเนื่อง (Continuous Improvement) องค์กรควรปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้ รวมถึง การใช้มาตรการเชิงแก้ไข ป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านการมั่นคงปลอดภัยขององค์กรเองและองค์กรอื่น แจ้งการปรับปรุงและดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้อง และตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้น บรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

๒) ข้อกำหนดทางด้านการจัดทำเอกสาร

(๑) ความต้องการทั่วไป เอกสารที่จำเป็นต้องจัดทำจะรวมถึงบันทึกแสดง การตัดสินใจของผู้บริหาร เช่น นโยบายความมั่นคงปลอดภัย ขอบเขตของระบบบริหารจัดการความมั่นคง ปลอดภัย วิธีการประเมินความเสี่ยง เป็นต้น

(๒) การบริหารจัดการเอกสาร ซึ่งเอกสารตามข้อกำหนดของระบบ บริหาร จัดการความมั่นคงปลอดภัยจะต้องได้รับการป้องกันและควบคุม ขั้นตอนการปฏิบัติที่เกี่ยวข้องกับการจัดการเอกสาร เช่น อนุมัติการใช้งานเอกสารก่อนที่จะเผยแพร่ ทบทวน ปรับปรุงและอนุมัติเอกสารตามความจำเป็น ระบุ การเปลี่ยนแปลงและสถานะภาพของเอกสารปัจจุบัน เป็นต้น

(๓) การบริหารจัดการบันทึกข้อมูลหรือฟอร์มต่าง ๆ องค์กรจะต้องมี การกำหนด จัดทำ และบำรุงรักษา บันทึกข้อมูลหรือฟอร์มต่าง ๆ เพื่อใช้เป็นหลักฐานแสดงความสอดคล้องกับ ข้อกำหนดและการดำเนินการที่มีประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๓.๑.๒ หน้าที่ความรับผิดชอบของผู้บริหาร

๑) การให้ความสำคัญในการบริหารจัดการ โดยผู้บริหารจะต้องแสดงถึงการให้ ความสำคัญต่อการกำหนดการลงมือปฏิบัติ การดำเนินการเฝ้าระวัง การทบทวน การบำรุงรักษาและการปรับปรุง ระบบบริหารจัดการความมั่นคงปลอดภัย

๒) การบริหารจัดการทรัพยากรที่จำเป็น และการอบรมการสร้างตระหนัก และการเพิ่มขีดความสามารถ เพื่อให้บุคลากรทั้งหมดที่ได้รับมอบหมายหน้าที่สามารถปฏิบัติงานได้ตามที่ กำหนดไว้ในนโยบายความมั่นคงปลอดภัย

๒.๓.๑.๓ องค์กรควรดำเนินการตรวจสอบภายในระบบบริหารจัดการความมั่นคง ปลอดภัย ตามรอบระยะเวลาที่กำหนดไว้เพื่อตรวจสอบว่า วัตถุประสงค์ มาตรการ กระบวนการ และขั้นตอน ปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัยมีความสอดคล้องกับข้อกำหนดในมาตรฐานฉบับนี้ และกฎหมาย ระเบียบ ข้อบังคับต่าง ๆ รวมถึงสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย และได้รับการลงมือปฏิบัติ และบำรุงรักษาอย่างสัมฤทธิ์ผลและเป็นไปตามที่คาดหวังไว้ นอกจากนี้ องค์กรจะต้อง วางแผนตรวจสอบภายในโดยพิจารณาถึงสถานะภาพและความสำคัญของกระบวนการและส่วนต่าง ๆ ที่จะได้รับการตรวจสอบและผลการตรวจสอบในครั้งที่ผ่านมา รวมถึงองค์กรจะต้องระบุหน้าที่ความรับผิดชอบ และข้อกำหนดต่าง ๆ ในการวางแผนและดำเนินการตรวจสอบจัดทำรายงานผลการตรวจสอบและบันทึกข้อมูล ของการตรวจสอบนั้น

๒.๓.๑.๔ ผู้บริหารจะต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบ ระยะเวลาที่กำหนดไว้ (เช่น ปีละ ๑ ครั้ง) เพื่อให้มีการดำเนินการที่เหมาะสม พอเพียงและสัมฤทธิ์ผล การทบทวนจะต้องรวมถึงการปรับปรุงหรือเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งรวมถึง

นโยบายความมั่นคงปลอดภัย และวัตถุประสงค์ทางด้านความปลอดภัย ผลของการทบทวนจะต้องได้รับการบันทึกไว้เป็นลายลักษณ์อักษรและบันทึกข้อมูลที่เกี่ยวข้องกับการทบทวนไว้

๒.๓.๒ มาตรการการจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

๒.๓.๒.๑ นโยบายความมั่นคงปลอดภัย (Security Policy) ประกอบด้วยนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ ซึ่งมีวัตถุประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง โดยผู้บริหารองค์กรจะต้องมีการจัดทำนโยบายที่เป็นลายลักษณ์อักษร รวมถึงการทบทวนนโยบายตามระยะเวลาที่กำหนด หรือมีเปลี่ยนแปลงที่สำคัญขององค์กร

๒.๓.๒.๒ โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Internal Organization) โดยได้กล่าวถึง บทบาทของผู้บริหารองค์กรและหัวหน้างานสารสนเทศในด้านต่าง ๆ ดังต่อไปนี้

๑) โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กรเพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

๒) โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับหน่วยงานภายนอก เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผล สารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับหน่วยงานภายนอก

๒.๓.๒.๓ การบริหารจัดการทรัพย์สินขององค์กร (Asset Management) โดยได้กล่าวถึง บทบาทของหัวหน้างานสารสนเทศและหัวหน้างานพัสดุในด้านต่าง ๆ ดังต่อไปนี้

๑) หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจขึ้นได้

๒) การจัดหมวดหมู่สารสนเทศ เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

๒.๓.๒.๔ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security) กล่าวถึงบทบาทของผู้บริหารด้านสารสนเทศ หัวหน้างานสารสนเทศ หัวหน้างานบุคคล และหัวหน้างานที่เกี่ยวข้องในด้านต่าง ๆ ดังต่อไปนี้

๑) การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ที่ผิดวัตถุประสงค์

๒) การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบ และทำความเข้าใจกับนโยบายเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

๓) การสิ้นสุดและการเปลี่ยนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

๒.๓.๒.๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) โดยได้กล่าวถึง บทบาทของหัวหน้างานสารสนเทศและหัวหน้างานอาคารในด้านต่าง ๆ ดังต่อไปนี้

๑) บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหายและการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

๒) ความมั่นคงปลอดภัยของอุปกรณ์ เพื่อป้องกันการสูญหาย การเกิดความเสี่ยง การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และทำให้กิจกรรมการดำเนินงานต่าง ๆ ขององค์กรเกิดการติดขัด หรือหยุดชะงัก

๒.๓.๒.๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations Management) โดยได้กล่าวถึง บทบาทของผู้บริหารองค์กร ผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ ผู้ที่เป็นเจ้าของกระบวนการ ทำงานและเจ้าหน้าที่สารสนเทศในด้านต่าง ๆ ดังต่อไปนี้

๑) การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

๒) การบริหารจัดการการให้บริการของหน่วยงานภายนอก เพื่อจัดทำและรักษา ระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอก ให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

๓) การวางแผนและการตรวจรับทรัพยากรสารสนเทศ เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

๔) การป้องกันโปรแกรมที่ไม่ประสงค์ดี เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

๕) การสำรองข้อมูล เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของระบบสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

๖) การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

๗) การจัดการสื่อที่ใช้ในการบันทึกข้อมูล เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลง แก้ไข การลบหรือทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงัก

๘) การแลกเปลี่ยนสารสนเทศ เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศ และซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

๙) การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และการใช้งาน

๑๐) การเฝ้าระวังทางด้านความมั่นคงปลอดภัย เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

๒.๓.๒.๗ การควบคุมการเข้าถึง (Access control) โดยได้กล่าวถึง บทบาทของผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ ผู้ดูแลระบบและเจ้าหน้าที่ในด้านต่าง ๆ ดังต่อไปนี้

๑) ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ เพื่อควบคุมการเข้าถึงสารสนเทศ

๒) การบริหารจัดการการเข้าถึงของผู้ใช้ เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๓) การควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต

๔) การควบคุมการเข้าถึงระบบปฏิบัติการที่ไม่ได้รับอนุญาต

๕) การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศที่ไม่ได้รับอนุญาต

๖) การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอก เพื่อสร้างความมั่นคงปลอดภัยให้กับอุปกรณ์และการปฏิบัติงานที่เกี่ยวข้อง

๒.๓.๒.๘ การจัดการพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance) โดยได้กล่าวถึง บทบาทของหัวหน้างานสารสนเทศ ผู้พัฒนาระบบ และผู้เป็นเจ้าของระบบในด้านต่าง ๆ ดังต่อไปนี้

๑) ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ เพื่อให้การจัดการและพัฒนาระบบสารสนเทศได้พิจารณาถึง ประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

๒) การประมวลผลสารสนเทศในแอปพลิเคชัน เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศที่ผิดวัตถุประสงค์

๓) มาตรการการเข้ารหัสข้อมูล เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการทางการเข้ารหัสข้อมูล

๔) การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

๕) การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

๖) การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

๒.๓.๒.๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management) โดยได้กล่าวถึง บทบาทของหัวหน้างานสารสนเทศ หัวหน้างานนิติกร ผู้ดูแลระบบและเจ้าหน้าที่ในด้านต่าง ๆ ดังต่อไปนี้

๑) การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

๒) การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

๒.๓.๒.๑๐ การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management) โดยได้กล่าวถึง บทบาทของผู้บริหารสารสนเทศ และหัวหน้างานสารสนเทศ ที่เกี่ยวกับหัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร เพื่อป้องกันการติดขัดหรือ การหยุดชะงักของกิจกรรมต่าง ๆ เพื่อป้องกันกระบวนการทำงานที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๒.๓.๒.๑๑ การปฏิบัติตามข้อกำหนด (Compliance) โดยได้กล่าวถึง บทบาทของหัวหน้างานสารสนเทศและหัวหน้างานนิติกรในด้านต่าง ๆ ดังต่อไปนี้

๑) การปฏิบัติตามข้อกำหนดทางกฎหมาย เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ

๒) การปฏิบัติตามนโยบายมาตรฐานความปลอดภัยและข้อกำหนดทางเทคนิค เพื่อให้ระบบเป็นตามนโยบายและมาตรฐานความมั่นคงปลอดภัยตามที่องค์กรกำหนดไว้

๓) การตรวจประเมินระบบสารสนเทศ เพื่อตรวจประเมินระบบสารสนเทศให้ได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทำงานน้อยที่สุด

บทที่ ๓

สถานภาพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.

การสำรวจและวิเคราะห์สถานภาพด้านการระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบเทคโนโลยีสารสนเทศของ สนข. ในปัจจุบัน มีรายละเอียดในด้านต่าง ๆ ประกอบด้วย

๑. สถานภาพด้านเทคโนโลยีสารสนเทศ
๒. สถานภาพด้านมาตรการระบบรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๑ สถานภาพด้านเทคโนโลยีสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร (ศทท.) เป็นหน่วยงานภายใน สนข. มีหน้าที่รับผิดชอบในการจัดทำนโยบายและพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของ สนข. การบริการจัดการด้านข้อมูลขนส่งและจราจร การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ การให้บริการระบบคอมพิวเตอร์ อุปกรณ์ต่อพ่วง และระบบเครือข่าย เพื่อรองรับการปฏิบัติงานของเจ้าหน้าที่ สนข. ทุกระดับให้ได้รับความสะดวก รวดเร็ว รวมถึงการพัฒนาระบบงานอิเล็กทรอนิกส์ที่ช่วยอำนวยความสะดวก และเพิ่มประสิทธิภาพในการปฏิบัติงาน อีกทั้งยังได้ติดตามผลการทำงานอย่างต่อเนื่องเพื่อพัฒนาระบบงานสารสนเทศให้มีประสิทธิภาพมากยิ่งขึ้น โดยจากการสำรวจสถานภาพด้านเทคโนโลยีสารสนเทศของ สนข. ในปัจจุบัน สามารถสรุปรายละเอียดได้ ดังนี้

๓.๑.๑ ฮาร์ดแวร์และซอฟต์แวร์ด้านความปลอดภัย ที่ติดตั้งอยู่ ณ ปัจจุบัน ดังนี้

ตารางที่ ๓-๑ แสดงฮาร์ดแวร์ และซอฟต์แวร์ด้านความปลอดภัยของ สนข.

ลำดับ	รายการ/อุปกรณ์	ยี่ห้อ/รุ่น	สถานที่ติดตั้ง	จำนวน
๑	อุปกรณ์ป้องกันระบบเครือข่าย (Firewall)	ยี่ห้อ Fortinet รุ่น Fortigate 600F	ห้อง Server ศทท.	๑ ชุด
๒	อุปกรณ์ป้องกันระบบเครือข่าย (Firewall)	ยี่ห้อ Paloalto รุ่น PA-๕๕๐	ห้อง Server ศทท.	๑ ชุด
๓	ซอฟต์แวร์ระบบป้องกันไวรัสแบบ Client & Server	Kaspersky Security Center (Client & Server)	ห้อง Server ศทท. และ เครื่อง Client	๑ ระบบ
๔	ซอฟต์แวร์ระบบรักษาความปลอดภัยไซเบอร์	Cortex XDR	เครื่อง Client	๑ ระบบ
๕	โปรแกรมสำรองข้อมูล Arcserve	Arcserve UDP	ห้อง Server ศทท.	๑ ระบบ

๓.๑.๒ ระบบเครือข่ายอินเทอร์เน็ต

สนข. มีการเชื่อมโยงสัญญาณเครือข่ายอินเทอร์เน็ต เพื่อให้บริการสัญญาณอินเทอร์เน็ตภายใน สนข. จำนวน ๕ โครงข่าย ดังนี้

๑) สัญญาณเครือข่ายจาก บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ความเร็ว ๑,๐๐๐ Mbps เพื่อให้บริการบนโครงข่ายสายสัญญาณ (LAN) เชื่อมต่อกับระบบอินเทอร์เน็ต

๒) สัญญาณเครือข่ายจากโครงข่าย MOTNET สำนักงานปลัดกระทรวงคมนาคม ความเร็ว ๑๖ Mbps เพื่อเชื่อมโยงระบบสารสนเทศของ สนข.

๓) สัญญาณเครือข่ายจากบริการสื่อสารพร้อมอุปกรณ์เชื่อมต่อโครงสร้างพื้นฐานเครือข่าย Digital Government Link (DG-Link) ความเร็ว ๓๐๐/๓๐๐ Mbps จากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เพื่อเชื่อมโยงข้อมูลภาครัฐและระบบบริหารสำนักงานอัตโนมัติ (e-Office) ของ สนข. และระบบแอปพลิเคชัน นำทาง (NAMTANG)

๔) สัญญาณเครือข่ายจาก บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน) ความเร็ว ๑,๐๐๐ Mbps เพื่อให้บริการบนโครงข่ายสายสัญญาณ (LAN) เชื่อมต่อกับระบบอินเทอร์เน็ต

๕) สัญญาณเครือข่ายแบบ Leaseline จากบริษัท ซิมโฟนี คอมมูนิเคชั่น จำกัด (มหาชน) ความเร็ว ๑/๑ Gbps เพื่อให้บริการบนโครงข่ายสายสัญญาณ (LAN) เชื่อมต่อกับระบบอินเทอร์เน็ต

๓.๑.๓ ระบบเครือข่ายไร้สาย (WiFi)

สนข. มีการติดตั้งอุปกรณ์กระจายสัญญาณ (Access Point) จำนวน ๓๒ ตัว ครอบคลุมพื้นที่การใช้งานภายในอาคาร สนข. ดังนี้

ตัวที่	ชื่ออุปกรณ์กระจายสัญญาณ	สถานที่ติดตั้ง	ชั้น
๑	FL1_AP01_HR	หน้าห้องกลุ่มบริหารทรัพยากรบุคคล	๑
๒	FL1_AP02_CBA	ห้องสำนักบริหารกลาง	๑
๓	FL1_AP17_Finance	ห้องกลุ่มบริหารงานคลัง	๑
๔	FL1_AP21_Meeting 101	ห้องประชุม ๑๐๑	๑
๕	FL1_AP22_CBA	ห้อง สบก.	๑
๖	FL1_AP23_CBA	ห้อง สบก.	๑
๗	FL2_AP03_TMD	กองจัดระบบการจราจรทางบก	๒
๘	FL2_AP04_Meeting 201	ห้องประชุม ๒๐๑	๒
๙	FL2_AP05_PNB	สำนักแผนงาน	๒
๑๐	FL2_AP08_PNB	สำนักแผนงาน	๒
๑๑	FL2_AP16_Training	ห้อง Computer Training	๒
๑๒	FL2_AP24_Meeting 201	ห้องประชุม ๒๐๑	๒
๑๓	FL2_AP25_Meeting 202	ห้องประชุม ๒๐๒	๒
๑๔	FL2_AP26_TMD	กองจัดระบบการจราจรทางบก	๒
๑๕	FL3_AP06_CEO	ห้องผู้บริหาร	๓
๑๖	FL3_AP07_RPB	สำนักส่งเสริมระบบการขนส่งและจราจรในภูมิภาค	๓
๑๗	FL3_AP14_SPB	สำนักแผนความปลอดภัย	๓
๑๘	FL3_AP15_SPB	สำนักแผนความปลอดภัย	๓
๑๙	FL3_AP18_CEO	ห้องผู้บริหาร	๓
๒๐	FL3_AP27_Meeting CEO	ห้องรับรอง ๒	๓
๒๑	FL4_AP09_BSD	กองพัฒนาระบบการขนส่งและจราจร	๔
๒๒	FL4_AP11_Meeting 401	ห้องประชุม ๔๐๑	๔
๒๓	FL4_AP13_Library	ห้องสมุด	๔
๒๔	FL4_AP19_TTIC	ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร	๔

ตัวที่	ชื่ออุปกรณ์กระจายสัญญาณ	สถานที่ติดตั้ง	ชั้น
๒๕	FL4_AP20_TTIC	ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร	๔
๒๖	FL4_AP28_Meeting 401	ห้องประชุม ๔๐๑	๔
๒๗	FL4_AP29_BSD	กองพัฒนาระบบการขนส่งและจราจร	๔
๒๘	FL5_AP10_Meeting 501	ห้องประชุม ๕๐๑	๕
๒๙	FL5_AP12_OCT	สำนักงานโครงการบริหารจัดการระบบตัวร่วม	๕
๓๐	FL5_AP30_OCT	สำนักงานโครงการบริหารจัดการระบบตัวร่วม	๕
๓๑	FL5_AP31_Meeting Youngyut	ห้องประชุมยงยุทธฯ	๕
๓๒	FL5_AP32_Meeting Youngyut	ห้องประชุมยงยุทธฯ	๕

๓.๑.๔ บุคลากรด้านเทคโนโลยีสารสนเทศ

ในการมอบหมายบุคลากรให้ปฏิบัติหน้าที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของ สนข. ได้มอบหมายให้กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร ซึ่งเป็นกลุ่มงานที่ดูแลรับผิดชอบงานด้านระบบคอมพิวเตอร์และระบบเครือข่าย และงานด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศและข้อมูลสารสนเทศด้วย ซึ่งกลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย มีกรอบอัตรากำลัง ดังนี้

- ๑) หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย ตำแหน่ง นักวิชาการคอมพิวเตอร์ ระดับชำนาญการพิเศษ จำนวน ๑ อัตรา
- ๒) ตำแหน่ง นักวิชาการคอมพิวเตอร์ ระดับปฏิบัติการ/ชำนาญการ จำนวน ๖ อัตรา

๓.๒ สถานภาพด้านมาตรการระบบรักษาความมั่นคงปลอดภัยไซเบอร์

สถานภาพด้านมาตรการระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. สามารถสรุปรายละเอียดได้ ดังนี้

๓.๒.๑ สถานภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.

๑) ระบบรักษาความมั่นคงปลอดภัย Internet Security สำหรับการใช้งานระบบอินเทอร์เน็ต จะใช้เส้นทางออกอินเทอร์เน็ต จำนวน ๔ เส้นทาง โดยกำหนดเส้นทางหลัก ได้แก่ อินเทอร์เน็ตความเร็วสูง ความเร็ว ๑/๑ Gbps และ ๑๐๐๐/๑๐๐๐ Mbps และอินเทอร์เน็ตเส้นทางสำรอง ได้แก่ เครือข่าย DG-Link ความเร็ว ๓๐๐/๓๐๐ Mbps และ MOTNET ความเร็ว ๑๖/๑๖ Mbps และ ซึ่งจะมีการรักษาความปลอดภัย สำหรับผู้ใช้งานระบบ Internet ประกอบด้วย

- Next Generation-Firewall
- การพิสูจน์ตัวตนผ่านระบบ Domain Name (Authentication)
- ระบบคัดกรองและปิดกั้นเว็บไซต์ (Web filter)
- ระบบป้องกันการบุกรุก (Intrusion Prevention System : IPS)
- ระบบตรวจสอบและเฝ้าระวัง (Monitoring)

๒) ระบบพิสูจน์ตัวตน (Authentication)

ระบบพิสูจน์ตัวตน สำหรับเข้าสู่ระบบอินเทอร์เน็ตและระบบงานอิเล็กทรอนิกส์ต่าง ๆ ของ สนข. ให้สามารถใช้งานได้อย่างสะดวก รวดเร็ว และปลอดภัย ด้วยรหัสผู้ใช้งานชุดเดียวสามารถเข้าสู่ระบบสารสนเทศ จำนวน ๘ ระบบงาน ได้แก่ ระบบเครือข่ายสายสัญญาณ ระบบเครือข่ายไร้สาย ระบบเชื่อมต่อเครือข่ายอินเทอร์เน็ตจากภายนอก ระบบบริหารจัดการข้อมูลส่วนบุคคลเพื่อการบูรณาการ ระบบบริหารจัดการสำนักงานอัตโนมัติ สนข. ระบบตรวจสอบพัสดุครุภัณฑ์ สนข. ระบบรายงานการดำเนินงานภายใน สนข. (TRS) และระบบการเรียนการสอนออนไลน์

๓) การกำหนดและใช้งาน Internet Protocol Address (IP Address) ภายใน สนข.

สำหรับระบบเครือข่ายภายใน สนข. ได้มีการกำหนดหมายเลข IP Address เป็นลักษณะ Vlan (Virtual Local Area Network) เพื่อเข้าถึงระบบเครือข่ายภายใน และเป็นการรักษาความมั่นคงปลอดภัยในการใช้งานระบบคอมพิวเตอร์และเครือข่ายของ สนข.

๔) การป้องกันการบุกรุกโจมตีระบบคอมพิวเตอร์และเครือข่าย (Firewall)

มีการกำหนดให้เปิดช่องทาง (Port) ในการเข้าถึงข้อมูลของแต่ละโครงข่ายเท่าที่จำเป็น เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่ปลอดภัย เช่น การเข้าถึงระบบสารสนเทศภายใน สนข. ที่ให้บริการประเภท Web Application แก่บุคคลภายนอก โดยจะเปิด Port เฉพาะประเภท HTTP และ HTTPS รวมถึงมีการปิดกั้นการเข้าถึงเว็บไซต์ประเภทที่มีความเสี่ยงต่อภัยคุกคามทางไซเบอร์ เช่น ประเภทเกมส์ ประเภทสื่อลามกอนาจาร ประเภทพนัน และเว็บไซต์ที่มีเนื้อหาไม่เหมาะสม เป็นต้น

๕) ระบบรักษาความมั่นคงปลอดภัยสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server Security) โดยจะมีระบบรักษาความมั่นคงปลอดภัยเครื่องคอมพิวเตอร์แม่ข่าย ประกอบด้วย

- การรักษาความปลอดภัยด้วยระบบสแกนลายนิ้วมือห้องศูนย์ข้อมูล สนข.
- Antivirus Client & Server สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและลูกข่าย
- Web App Firewall
- การตั้งค่า Firewall ของเครื่องคอมพิวเตอร์แม่ข่าย และการอัปเดตแพตช์ (Patch)

ด้านความปลอดภัยต่าง ๆ อย่างสม่ำเสมอ

๓) แผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ โดย สนข. ได้มีการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฯ เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศ สนข. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยไซเบอร์ต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อ สนข.

๓.๒.๒ สถานภาพที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

หลักการปฏิบัติพื้นฐานของการรักษาความมั่นคงปลอดภัย ประกอบด้วย ๓ ด้าน เรียกว่า “CIA Triad” ประกอบด้วย ความมั่นคงปลอดภัย (Security) เป็นการปกป้องทรัพย์สิน (Asset) ให้พ้นจากภัยคุกคาม (Threat) หลักการของความมั่นคงปลอดภัยที่จะได้กล่าวต่อไปนี้จะสามารถใช้ได้กับทรัพย์สินทุกประเภท ไม่ว่าจะเป็นทรัพย์สินที่จับต้องได้หรือไม่ก็ตาม เช่น คอมพิวเตอร์ เงินทอง เครื่องประดับต่าง ๆ องค์กรความรู้ สิทธิบัตร ข้อมูลลูกค้า ความลับทางการค้า และข้อมูลอื่น ๆ หลักการของความมั่นคงปลอดภัย การปกป้องทรัพย์สินขององค์กรนั้น ตั้งอยู่บนหลักความมั่นคงปลอดภัย ๓ ขา (Security Triads) อันประกอบด้วย CIA ดังนี้



ภาพที่ ๓-๒ หลักการ CIA

ความลับ หรือ Confidentiality : เป็นการปกป้องข้อมูลไม่ให้รั่วไหลไปสู่ภายนอกองค์กร หรือบุคคลที่ต้องการเข้าถึงข้อมูลขององค์กร เนื่องจากข้อมูลข่าวสารที่หลุดออกไปจะส่งผลกระทบต่อองค์กรเป็นอย่างมาก จึงต้องมีการดำเนินการต่าง ๆ เพื่อปกป้องข้อมูลขององค์กร และรักษาความลับของข้อมูล เช่น การเข้ารหัส (Encryption) เทคโนโลยีที่มีการเชื่อมต่อกับเครือข่ายภายนอก (Virtual Private Network) มาตรฐานการรักษาความปลอดภัยของข้อมูลที่รับส่งผ่านอินเทอร์เน็ต (Secure Socket Layer) การเข้ารหัส และถอดรหัสข้อมูลด้วยกุญแจส่วนตัว (Public Key Infrastructure) เป็นต้น

ความถูกต้อง หรือ Integrity : เป็นการป้องกันการปลอมแปลงข้อมูลไม่ให้ถูกแก้ไข โดยที่ไม่ได้รับอนุญาต หรือไม่ถูกเปลี่ยนแปลงโดยแฮกเกอร์หรือผู้บุกรุก โดยเฉพาะข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร หรือมีผลต่อองค์กร หากข้อมูลถูกเปลี่ยนแปลงแก้ไขไปแล้วจะส่งผลกระทบต่อองค์กรอย่างมาก จึงต้องมีการตรวจสอบความถูกต้อง (Checker) ของข้อมูลอยู่เสมอ

สภาพพร้อมใช้งาน หรือ Availability : เป็นการทำให้มีความพร้อมในการใช้งานระบบคอมพิวเตอร์ได้ตลอดเวลา หรือเมื่อเกิดปัญหาระบบล่มแล้ว การไม่มีระบบสำรองไว้ใช้งานหรือการรอนจนกว่าจะสามารถกู้ระบบได้จะทำให้เกิด “downtime” เป็นอย่างมาก ซึ่งเป็นต้นเหตุทำให้การดำเนินงานขององค์กรติดขัด ไม่สามารถดำเนินงานได้อย่างต่อเนื่อง จึงควรมีแผนการป้องกัน ตัวอย่างเช่น แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Planning) แผนกู้คืนระบบเทคโนโลยีสารสนเทศและดิจิทัล (Disaster Recovery Planning) เป็นต้น

หลักการของความมั่นคงปลอดภัยทั้ง ๓ มิติ นั้น เป็นสิ่งที่จำเป็นและไม่สามารถแยกขาดจากกันได้นอกจากนี้ยังมีประเภทของความมั่นคงปลอดภัย ดังนี้

๑) ความปลอดภัยทางกายภาพ (Physical Security) ได้แก่ ความปลอดภัยด้านอาคารสถานที่ การตรวจสอบคนที่ต้องผ่านเข้าออกอาคารสถานที่ เป็นต้น

๒) ความปลอดภัยทางงานอำนวยการ (Administrative Security) ได้แก่ นโยบาย มาตรฐาน คำสั่ง กระบวนการ ข้อเสนอแนะ เป็นต้น ตัวอย่างการสร้างความปลอดภัยทางงานอำนวยการ ได้แก่ การแบ่งอำนาจ ความรับผิดชอบ การหมุนเวียนงาน การบังคับให้ลาพักผ่อน การตรวจสอบภูมิหลังก่อนการจ้างงาน

๓) ความปลอดภัยทางเทคนิค ได้แก่ การนำเทคโนโลยีมาช่วยสร้างความปลอดภัย ตัวอย่างของการสร้างความมั่นคงปลอดภัยทางเทคนิค ได้แก่ ระบบ Access Control List ระบบ Firewall ระบบ Intrusion Detection System (IDS) เป็นต้น

บทที่ ๔
การวิเคราะห์สภาพแวดล้อม
การรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.

การวิเคราะห์สภาพแวดล้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประกอบด้วย ๒ ส่วน คือ

๑. ความต้องการด้านเทคโนโลยีสารสนเทศ

๒. การวิเคราะห์สถานภาพแวดล้อมด้วยการทำ SWOT Analysis และภาพรวมของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.

๔.๑ ความต้องการด้านเทคโนโลยีสารสนเทศ

จากการสำรวจและวิเคราะห์สถานภาพปัจจุบันทางด้านเทคโนโลยีสารสนเทศของ พบว่า สนข. ได้มีการกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไว้เป็นส่วน ๆ อย่างชัดเจน ซึ่งส่วนมากจะเป็นแนวทางในการปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยให้แก่ระบบสารสนเทศของ สนข. ประกอบกับ สนข. มีการดำเนินโครงการด้านไอซีทีต่าง ๆ ในรูปแบบของการจัดหาและติดตั้งอุปกรณ์ด้าน ICT โดยมีเจ้าหน้าที่ด้านเทคโนโลยีเป็นผู้ดูแลเท่าที่จำเป็นมาใช้ซึ่งยังไม่เต็มรูปแบบ และยังไม่ได้นำเทคโนโลยีสำหรับการบริหารจัดการด้าน ICT Security มาใช้งานมากนัก แต่ทั้งนี้ก็ถือได้สามารถดำเนินการป้องกันภัยทางไซเบอร์ได้เป็นอย่างดีในระดับหนึ่ง

ดังนั้น ในการพัฒนางานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. จึงต้องคำนึงถึงเทคโนโลยีสำหรับการบริหารจัดการและรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ทั้งด้านฮาร์ดแวร์ และระบบซอฟต์แวร์ พร้อมทั้งแนวทางการปฏิบัติที่เป็นมาตรฐานในการสร้างระบบความมั่นคงปลอดภัย ซึ่งจำเป็นต้องคำนึงถึงองค์ประกอบต่าง ๆ ดังนี้

๔.๑.๑ การออกแบบสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ของระบบรักษาความปลอดภัยแบบบูรณาการของระบบสารสนเทศ (IT Security Detailed Design)

ระบบสารสนเทศของ สนข. นั้น จำเป็นต้องมีการออกแบบระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) ที่ติดตั้งระดับของผู้ใช้งาน (End Point) ไปจนถึงระดับแอปพลิเคชันของ สนข. โดยมีหลักการออกแบบ ดังนี้

๔.๑.๑.๑ สถาปัตยกรรมด้านความปลอดภัย (Security Architecture Principles)

ระบบสื่อสารเครือข่ายเป็นโครงสร้างพื้นฐานของระบบงานสารสนเทศทั้งหมดของ สนข. ซึ่งเป็นอาคารขนาด ๕ ชั้น รองรับการทำงานของหลายหน่วยงาน มีการรับส่งข้อมูลของระบบงานสารสนเทศด้านต่าง ๆ หลายระบบงานมีการใช้งานระบบสื่อสารทั้งรูปแบบภาพ เสียงและข้อมูล ดังนั้นระบบเครือข่ายของ สนข. จำเป็นต้องมีประสิทธิภาพและเสถียรภาพ มีความปลอดภัยสูง ดูแลรักษาได้ง่าย และมีความยืดหยุ่นในการปรับเปลี่ยนสามารถรองรับการขยายเพิ่มเติมได้ในอนาคต รวมถึงต้องมีระบบรักษาความปลอดภัยครอบคลุมในทุกด้าน โดยมีเป้าหมายพื้นฐานในการออกแบบรักษาความมั่นคงปลอดภัยด้วยการยึดหลักการของ CIA เพื่อให้ระบบสารสนเทศได้รับความมั่นคงปลอดภัย ดังต่อไปนี้

๑) การรักษาความลับ (Confidentiality) การรักษาความลับเป็นการปกป้องการเข้าถึงและเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต ข้อมูลที่เป็นความลับจะยังคงไว้ซึ่งความพร้อมใช้ (Availability) และความแท้จริงของข้อมูล (Integrity)

๒) ความแท้จริงของข้อมูล (Integrity) เป็นการป้องกันไม่ให้ข้อมูลถูกแก้ไขจากผู้ที่ไม่ได้รับสิทธิ์ เพื่อให้ข้อมูลดังกล่าวมีความถูกต้องและพร้อมใช้อยู่ตลอดเวลา

๓) ความพร้อมใช้อยู่เสมอ (Availability) ระบบสารสนเทศที่ได้รับการป้องกันด้านความปลอดภัยจะมีคุณสมบัติพร้อมใช้อยู่ตลอดเวลาโดยทั่วไปความปลอดภัย (Security)

การบริหารจัดการระบบรักษาความปลอดภัยครบถ้วนสมบูรณ์ และเป็นระบบตรวจสอบและป้องกันการบุกรุกและป้องกันการโจรกรรมข้อมูลจากระบบงาน และระบบฐานข้อมูล ซึ่งระบบจะครอบคลุมการตรวจสอบและป้องกันการบุกรุกในรูปแบบต่าง ๆ ดังนี้

Security Framework ของฮาร์ดแวร์และซอฟต์แวร์

ภาพรวมของระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของ สนข. จะครอบคลุมการตรวจสอบและการป้องกันการบุกรุกในรูปแบบต่าง ๆ แบ่งย่อยออกเป็น ๖ กิจกรรมงานหลักด้านความมั่นคงปลอดภัยตามหลัก NIST Security Framework ได้แก่

๑) การกำกับดูแล (Govern) การกำกับดูแลและบริหาร กำหนดนโยบาย บทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์

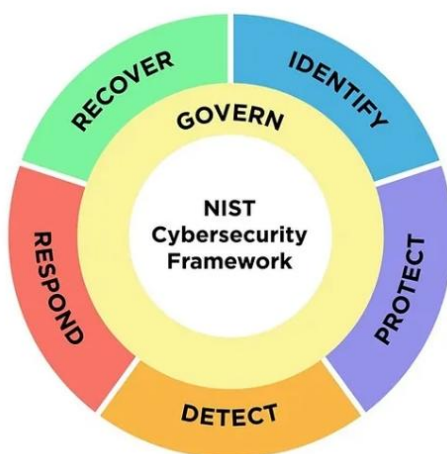
๒) การระบุ (Identify) เป็นขั้นตอนการบริหารจัดการทรัพย์สิน และกิจกรรมงานสำคัญ ด้วยการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยที่มีต่อระบบ ทรัพย์สิน และข้อมูล เพื่อกำหนดกลยุทธ์ในการบริหารความเสี่ยง

๓) การป้องกัน (Protect) จะเน้นการป้องกัน เพื่อจำกัดระดับผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัย มาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการ รวมไปถึงการตรวจสอบหาช่องโหว่ที่อาจพบในระบบและดำเนินการแก้ไข

๔) การตรวจจับ (Detect) เป็นการเฝ้าระวังแบบเรียลไทม์จะมีการตรวจสอบวิเคราะห์ภัยคุกคามด้วยเทคนิคขั้นสูง ด้วยการรวบรวมข้อมูลและศึกษาพฤติกรรมที่เกิดขึ้น เพื่อตรวจหาภัยคุกคามที่อาจเกิดขึ้น

๕) การตอบสนอง (Respond) เป็นการตอบสนองต่อภัยคุกคาม ตามขั้นตอนที่กำหนดไว้ โดยจะมีการสืบสวนทางข้อมูลดิจิทัล Packet Capture (PCAP) เพื่อการวิเคราะห์หาต้นเหตุของภัยคุกคามที่เกิดขึ้น

๖) การคืนสภาพหรือการกู้คืน (Recover) เป็นการจัดทำและดำเนินกิจกรรมตามแผนงาน เพื่อรองรับการดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนระบบที่สามารถให้บริการตามที่กำหนด ทั้ง Transaction Log และ Backup



ภาพที่ ๔-๑ กรอบแนวทางระบบรักษาความปลอดภัย
ตามมาตรฐาน NIST Cybersecurity Framework ๒.๐

ในการออกแบบ Security Matrix ให้ครอบคลุม ๓ กิจกรรมหลักตามแนวทางของ NIST Cybersecurity Framework เพื่อป้องกันการบุกรุกและภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ แบ่งได้ ดังนี้

๑) การกำกับดูแล (Govern)

ในระดับอุปกรณ์ (Device Layer) มีการจัดทำนโยบายและแนวปฏิบัติการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ

ในระดับระบบสารสนเทศ (Application Layer) มีการกำหนดนโยบายการพัฒนาระบบแอปพลิเคชัน และนโยบายการจัดการใช้งานแอปพลิเคชัน

ในระดับเครือข่าย (Network Layer) มีการกำหนดนโยบายการจัดการและการใช้งานระบบเครือข่าย

ในระดับข้อมูล (Data Layer) มีการกำหนดนโยบายการจัดการข้อมูล

ในระดับผู้ใช้งาน (User Layer) มีการกำหนดนโยบายเกี่ยวกับผู้ใช้งาน เช่น นโยบายการใช้งาน ข้อตกลงการใช้งาน นโยบายการฝึกอบรมและนโยบายการสร้างตระหนักรู้

๒) การระบุ (Identify)

ในระดับอุปกรณ์ (Device Layer) มีการจัดทำบัญชีรายชื่อครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ พร้อมมีระบบตรวจสอบพัสดุครุภัณฑ์ สนข. เพื่อบริหารจัดการบัญชีครุภัณฑ์ของ สนข.

ในระดับระบบสารสนเทศ (Application Layer) มีการจัดหาอุปกรณ์เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น Firewall Web-App Firewall และ Anti-Virus เป็นต้น

ในระดับเครือข่าย (Network Layer) มีการกำหนดมาตรการป้องกันต่าง ๆ ในการเข้าถึงและใช้งานระบบต่าง ๆ ภายใน สนข.

ในระดับข้อมูล (Data Layer) การมาตรการป้องกันการเข้าถึงและใช้งานข้อมูล และระบบงานสารสนเทศของ สนข.

ในระดับผู้ใช้งาน (User Layer) จะเป็นการสร้างความความรู้และตระหนักรู้เพื่อให้เข้าใจถึงภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงการวิธีการป้องกันภัยทางไซเบอร์ในรูปแบบต่าง ๆ

๓) การป้องกัน (Protect)

มีการทำ Identity and Access Management เพื่อแยกแยะกลุ่มผู้ใช้งานและสิทธิ์การใช้งานระบบสารสนเทศของ สนข.

ในระดับอุปกรณ์ (Device Layer) จะมีการติดตั้ง Endpoint Anti-Virus และ Intrusion Prevention System (IPS) เพื่อป้องกันภัยคุกคาม

ในระดับระบบสารสนเทศ (Application Layer) จะมีติดตั้ง Web Application Firewall (WAF) เพื่อตรวจจับและป้องกันภัยคุกคามแอปพลิเคชัน (Application)

ในระดับเครือข่าย (Network Layer) จะใช้เทคโนโลยี Next-Generation Firewall (NG-FW) ในการป้องกันระบบเครือข่าย

ในระดับข้อมูล (Data Layer) จะมีการดำเนินการด้าน Personal Data Protection Act (PDPA) เพื่อรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และการสำรองข้อมูลของระบบสารสนเทศ

ในระดับผู้ใช้งาน (User Layer) จะเป็นการสร้างความความรู้และตระหนักรู้ให้เข้าใจถึงภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงการวิธีการป้องกันภัยทางไซเบอร์ในรูปแบบต่าง ๆ

๔) การตรวจจับ (Detect) และการตอบสนอง (Response)

ในระดับอุปกรณ์ (Device Layer) จะมีการติดตั้งป้องกันไวรัส (Anti-Virus) เพื่อป้องกันการโจมตีจากไวรัส และพวก Malware

ในระดับเครือข่าย (Network Layer) มีการติดตั้งอุปกรณ์ป้องกันการโจมตีจากภัยคุกคามทางไซเบอร์ เพื่อป้องกันระบบเครื่องคอมพิวเตอร์แม่ข่าย-ลูกข่าย และระบบเครือข่ายภายใน สนข.

ในระดับข้อมูล (Data Layer) ใช้การบริหารจัดการสิทธิ์ในการเข้าถึงระบบงานสารสนเทศ และข้อมูล

ในระดับผู้ใช้งาน (User Layer) จะเป็นการสร้างความความรู้และตระหนักรู้เพื่อให้เข้าใจถึงภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ให้สามารถเฝ้าระวังเพื่อลดความเสี่ยงของการเกิดภัยทางไซเบอร์ และให้สามารถแก้ไขปัญหาเบื้องต้นได้

๕) การคืนสภาพหรือการกู้คืน (Recover)

ในระดับระบบสารสนเทศ (Application Layer) ที่มีการเก็บ Transaction Log และในระดับข้อมูล (Data Layer) จะทำการ Backup ข้อมูลอย่างสม่ำเสมอ เพื่อกู้คืนข้อมูลในกรณีที่ข้อมูลหรือระบบได้รับความเสียหาย

๔.๑.๑.๒ การให้บริการระบบสารสนเทศผ่านการรักษาความมั่นคงปลอดภัย แบ่งออกเป็น ๒ ส่วน คือ

๑) การให้บริการระบบเทคโนโลยีสารสนเทศภายใน (Intranet) ให้เจ้าหน้าที่ของ สนข. เข้าใช้งานระบบจากเครือข่ายภายในเครือข่ายของ สนข.

๒) การให้บริการระบบเทคโนโลยีสารสนเทศภายนอก (Internet) ให้เจ้าหน้าที่และผู้ใช้งานทั่วไปเข้าใช้งานระบบสารสนเทศของ สนข. จากเครือข่ายอินเทอร์เน็ต

การออกแบบระบบรักษาความมั่นคงปลอดภัยสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและข้อมูลหลัก (Server and Data Center Zone) จะกำหนดให้อยู่ในโซนแม่ข่าย (DMZ Zone) และมีการป้องกันการถูกโจมตีด้วย Web Application Firewall และอุปกรณ์ DNS ที่ช่วยในการป้องกันการโจมตีข้อมูล ในขณะที่โซนเครื่องคอมพิวเตอร์ลูกข่ายจะได้รับการป้องกันการถูกโจมตี ทั้งจาก Firewall และ Anti-Virus และมีการอัปเดต Patch ความปลอดภัยอย่างสม่ำเสมอ ในส่วนของระบบงานสารสนเทศ และชุดข้อมูลใน Database จะมีการสำรองข้อมูลอย่างสม่ำเสมอ

ดังนั้น ในภาพรวมของระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ สนข. จะสามารถแบ่งออกตามลักษณะของการให้บริการต่าง ๆ ดังนี้

๑) ระบบรักษาความมั่นคงปลอดภัยสำหรับระบบเครือข่ายภายในเป็นส่วนของการรักษาความมั่นคงปลอดภัยสำหรับช่องทางการเข้าถึงระบบงานสารสนเทศภายในเครือข่ายของ สนข.

๒) ระบบรักษาความมั่นคงปลอดภัยสำหรับการเข้าถึงระบบอินเทอร์เน็ตของ สนข. เป็นส่วนที่รักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบอินเทอร์เน็ต จากเครือข่ายคอมพิวเตอร์ทั้งหมดของ สนข. ทั้งแบบมีสาย (Wired) และแบบไร้สาย (Wireless)

๔.๑.๒ การออกแบบสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ของระบบรักษาความมั่นคงปลอดภัยระบบเครือข่ายในส่วนของอินเทอร์เน็ตโซน (Internet Zone)

ระบบเครือข่ายของ สนข. จำเป็นต้องมีการรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพ และมีความน่าเชื่อถือ ดังนั้น จึงมีการติดตั้งอุปกรณ์การรักษาความมั่นคงปลอดภัย ดังนี้

๑) อุปกรณ์ Next Generation Firewall (NG-Firewall) ทำหน้าที่ป้องกันและควบคุมการใช้งานอินเทอร์เน็ตในระดับแอปพลิเคชัน สามารถกำหนดการเข้า-ออกของจราจรทางคอมพิวเตอร์ตามนโยบายของ สนข. และการป้องกันการโจมตี เช่น HTTP Flood Attacks, DNS Flood Attacks และ SSL Flood Attacks รวมถึงการบริหารจัดการช่องทางเชื่อมต่ออินเทอร์เน็ตตามนโยบายของ สนข. และการรักษาความปลอดภัยด้วยวิธีการแปลงหมายเลข IP Address ด้วยวิธีการทำ Network Address Translation (NAT)

๒) อุปกรณ์ Wireless Controller ทำหน้าที่บริหารจัดการการเชื่อมต่ออุปกรณ์กับระบบเครือข่ายอินเทอร์เน็ตผ่านอุปกรณ์กระจายสัญญาณเครือข่ายแบบไร้สาย (Wireless)

๓) อุปกรณ์ Web Application Firewall (WAF) เป็นอุปกรณ์ป้องกันการโจมตีระดับเน็ตเวิร์ค และแอปพลิเคชันที่ทำหน้าที่ตรวจจับและป้องกันภัยคุกคามแอปพลิเคชัน (Application) ซึ่งตรวจจับและป้องกันการบุกรุกเครือข่ายแบบ Real-Time รวมทั้งสามารถกำหนดการใช้งานของแอปพลิเคชันต่าง ๆ ของ สนข. ได้

๔.๑.๓ การออกแบบสถาปัตยกรรมฮาร์ดแวร์ และซอฟต์แวร์ของระบบรักษาความปลอดภัยในส่วน DMZ Zone

แอปพลิเคชันและเซอร์วิส (Application and Service) ที่ให้บริการทั้งผู้ใช้งานภายในและผู้ใช้งานภายนอกของ สนข. ได้ทำการแยกออกจากส่วนของระบบเครือข่าย เพื่อป้องกันภัยจากการบุกรุกและการโจมตีจากอินเทอร์เน็ต แต่ยังให้บริการแอปพลิเคชันและเซอร์วิสได้ โดยมีดังนี้

๑) อุปกรณ์ Web Application Firewall (WAF) เป็นอุปกรณ์ป้องกันการโจมตี ทำหน้าที่ตรวจจับและป้องกันภัยคุกคามแอปพลิเคชัน (Application) ของ สนข. จากผู้ใช้งานภายในและผู้ใช้งานภายนอกโดยการกำหนดนโยบาย (Policy) การเข้าถึงระบบงานต่าง ๆ

๒) ระบบป้องกันไวรัส (Anti-Virus) ทำหน้าที่ป้องกันการบุกรุกจากภัยประเภทไวรัสและซอร์สโค้ด (Source Code) ที่ไม่ประสงค์ดี เช่น สามารถป้องกันสแปม (Spam) จัดการปัญหาสแปมจากแหล่งที่มาต่าง ๆ (Reputation) ป้องกัน Virus ประเภทมัลแวร์ (Malware) และสปายแวร์ (Spyware) เป็นต้น

๓) อุปกรณ์บริหารจัดการ DNS/DHCP สำหรับติดตั้งในโซน DMZ เป็นอุปกรณ์ที่ทำหน้าที่กำหนดการให้บริการ IP Address (DHCP) และ DNS ภายในกับเครื่องลูกข่ายในระบบ โดยการทำ DNS Query และทำ Real-Time update (ในส่วนของ DNS)

๔.๑.๔ การออกแบบสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ของระบบรักษา ความปลอดภัยระบบเครือข่ายในส่วนโซนภายใน (Internal Zone)

ระบบเครือข่ายในส่วนโซนภายในนี้จะเป็ระบบเครือข่ายภายในของ สนข. จะมีการแบ่งผู้ใช้งานกระจายอยู่ตามชั้นต่าง ๆ ภายในอาคาร สนข. จำนวน ๕ ชั้น แบ่งเป็น Vlan จำนวน ๔ Vlan โดยแบ่งการใช้งานผ่านเครือข่ายแบบมีสาย (Wire LAN) จำนวน ๓ Vlan และเครือข่ายแบบไร้สาย (Wireless LAN) จำนวน ๑ Vlan ดังนั้น การรักษาความปลอดภัยเครือข่าย จึงกำหนดให้มีความครอบคลุมทั้งในส่วนองเครือข่ายแบบมีสายและแบบไร้สาย เพื่อความปลอดภัยสูงสุด

๔.๑.๕ การออกแบบสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ระบบพิสูจน์ตัวตนและกำหนดสิทธิ์ในการเข้าถึงระบบเครือข่ายของ สนข.

สนข. มีระบบพิสูจน์ตัวตนของผู้เข้าใช้งานระบบเครือข่ายภายใน และระบบสารสนเทศสำหรับบุคคลของ สนข. ซึ่งเป็นการตรวจสอบ ระบุตัวตน และกำหนดสิทธิ์ในการใช้งานระบบต่าง ๆ ภายใน สนข. ซึ่งกำหนดให้ผู้ใช้งานจะต้องมีการดำเนินการพิสูจน์ตัวตนทั้งระบบเครือข่ายแบบมีสาย (Wire LAN) และแบบไร้สาย (Wireless LAN)

๔.๑.๖ การออกแบบสถาปัตยกรรมฮาร์ดแวร์และซอฟต์แวร์ระบบรักษาความปลอดภัยของระบบเครื่องแม่ข่ายในส่วนของ Data Center

๑) อุปกรณ์ป้องกันการบุกรุกและโจมตีระบบเครือข่าย (Firewall) เป็นอุปกรณ์ป้องกันการบุกรุกและการโจมตีระบบ ทำหน้าที่ตรวจจับและคัดกรองข้อมูลจราจรทางคอมพิวเตอร์ที่จะเข้ามาสู่ระบบเครื่องแม่ข่าย เพื่อป้องกันการถูกโจมตีจากภัยทางไซเบอร์ต่าง ๆ ที่จะเข้าถึงระบบงานและข้อมูลสำคัญของ สนข. และยังกำหนดนโยบาย (Policy) การเชื่อมต่อข้อมูลกับภายนอกอีกด้วย

๒) ระบบป้องกันไวรัส (Anti-Virus) สำหรับเครื่องแม่ข่าย ทำหน้าที่ป้องกันภัยคุกคามในระดับเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual machines) โดยรองรับการ integrates กับ Endpoint เพื่อป้องกันการโจมตีที่ซับซ้อน อาทิ ไวรัสมัลแวร์ (Malware) สปายแวร์ (Spyware) และโทรจัน (Trojans) เป็นต้น

๓) การสำรองข้อมูลเครื่องแม่ข่าย (Data Center Backup) โดยมีการทำการสำรองข้อมูลให้ระบบสารสนเทศต่าง ๆ ของ สนข. เป็นประจำทั้งระบบเครื่องแม่ข่าย และระบบเครื่องแม่ข่ายเสมือน โดยมีการทำการสำรองข้อมูล ๓ รูปแบบ ได้แก่ แบบ Incremental แบบ Full Backup และ การสำรองข้อมูล Backup ที่อุปกรณ์จัดเก็บข้อมูลภายนอก (Storage)

๔.๑.๗ การออกแบบการบริหารข้อมูลส่วนบุคคล (Identity Management)

๑) การบริหารข้อมูลส่วนบุคคล หรือ Identity Management หมายถึง ระบบที่สามารถใช้บริหารรายชื่อผู้ใช้งานรวมถึงรายละเอียดในการใช้งานระบบงานสารสนเทศ (User Information and User Profiles) แต่ระบบได้ ในขณะที่ Single Sign-on หมายถึง กระบวนการที่จะบริหารจัดการเรื่องของการที่ผ่านซึ่งปกติผู้ใช้งานจะมีรหัสผ่านมากกว่าหนึ่งรหัสเพื่อเข้าใช้งานระบบสารสนเทศต่าง ๆ อาทิ รหัสสำหรับระบบเครือข่ายภายในหรือเข้าสู่ระบบอินเทอร์เน็ต รหัสสำหรับการใช้งานวินโดวส์ รหัสสำหรับเข้ารับระบบสารสนเทศหรือระบบฐานข้อมูล รวมถึงปัญหาเรื่องของการลืมรหัสผ่าน การเปลี่ยนรหัสตามเวลาที่กำหนด

การบริหารจัดการการเข้าถึงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ แอปพลิเคชันต่าง ๆ และระบบฐานข้อมูลของผู้ใช้งาน จึงเป็นสิ่งจำเป็น ด้วยระบบบริหารแบบศูนย์กลาง Identity Management ผู้ดูแลระบบจะสามารถสร้าง แก้ไข และลบข้อมูลรายชื่อผู้ใช้งานทั้งบน Active Directory และ LDAP ที่ออกแบบไว้ โดยระบบ Identity Management จะมีฟังก์ชันการทำงานหลัก อาทิ User Provisioning, Password Management และ User Profile Management

๔.๒ การวิเคราะห์สถานภาพแวดล้อมด้วยการทำ SWOT Analysis และภาพรวมของระบบรักษาความมั่นคงปลอดภัยไซเบอร์

การวิเคราะห์สถานภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. เพื่อค้นหาโอกาสภัยคุกคาม จุดแข็ง จุดอ่อนหรือข้อด้อย และสิ่งที่เป็นปัญหาสำคัญในการดำเนินงานทางด้านระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. โดยวางกรอบแนวคิดในการวิเคราะห์สภาพแวดล้อม (SWOT Analysis) เพื่อวิเคราะห์สภาพแวดล้อมด้านระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ซึ่งได้มีการแยกการวิเคราะห์สภาพแวดล้อมที่เป็นผลจากปัจจัยจากภายนอกและปัจจัยจากภายใน ซึ่งสามารถแสดงได้ดังภาพที่ ๔-๒

	เชิงบวก	เชิงลบ
สภาพแวดล้อมภายใน	S จุดแข็ง (Strengths)	W จุดอ่อน (Weaknesses)
สภาพแวดล้อมภายนอก	O โอกาส (Opportunities)	T ภัยคุกคาม / อุปสรรค (Threats)

ภาพที่ ๔-๒ การวิเคราะห์สภาพแวดล้อมด้านความมั่นคงปลอดภัยไซเบอร์ ด้วย SWOT

การดำเนินการวิเคราะห์สภาพแวดล้อมด้วยการทำ SWOT Analysis ได้นำผลการวิเคราะห์จากแผนปฏิบัติการดิจิทัล สนข. พ.ศ. ๒๕๖๖ - ๒๕๗๐ และจากประสบการณ์การของเจ้าหน้าที่ผู้ดูแลระบบงานด้านระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศของ สนข.

๔.๒.๑ ผลการวิเคราะห์ SWOT Analysis ระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.

การวิเคราะห์สภาพแวดล้อมซึ่งมีผลจากปัจจัยภายใน ประกอบด้วย การวิเคราะห์ปัจจัยภายในเพื่อกำหนดเป็นจุดแข็ง (Strengths) และการวิเคราะห์ปัจจัยภายในเพื่อกำหนดเป็นจุดอ่อน (Weaknesses) ดังนี้

ตารางที่ ๔-๑ ผลการวิเคราะห์ปัจจัยภายในเพื่อกำหนดเป็นจุดแข็ง (Strengths)

รหัส	จุดแข็ง (Strengths)
S1	ผู้นำและผู้บริหารระดับสูงของ สนข. มีวิสัยทัศน์ และให้ความสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์
S2	สนข. มีนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจนตามแผนปฏิบัติการดิจิทัล สนข. พ.ศ. ๒๕๖๖ - ๒๕๗๐ ตามยุทธศาสตร์ที่ ๕ กลยุทธ์ที่ ๑๑ - ๑๓
S3	สนข. มีผู้บริหารด้านเทคโนโลยีสารสนเทศ และคณะกรรมการเทคโนโลยีดิจิทัล ในการขับเคลื่อนงานด้านเทคโนโลยีของ สนข. และสามารถเข้ามากำกับดูแล ให้ข้อเสนอแนะงานด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ได้
S4	มีการจัดทำแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ สนข. และทบทวนมาอย่างต่อเนื่อง
S5	สนข. มีการดำเนินงานและพัฒนางานด้านความมั่นคงปลอดภัยด้านไซเบอร์ ทั้งในส่วนของ ฮาร์ดแวร์ ซอฟต์แวร์ นโยบายและแนวทางปฏิบัติมาอย่างต่อเนื่อง
S6	มีโครงสร้างพื้นฐานด้านดิจิทัลที่เพียงพอต่อการใช้งาน และมีความยืดหยุ่น
S7	บุคลากรด้าน ICT มีความพร้อมในการพัฒนางานด้านความมั่นคงปลอดภัยไซเบอร์ มีการเรียนรู้ และเฝ้าระวังภัยทางไซเบอร์อย่างต่อเนื่อง

รหัส	จุดแข็ง (Strengths)
S8	บุคลากรของ สนข. มีทักษะการใช้ระบบคอมพิวเตอร์ และเทคโนโลยีในปฏิบัติงาน
S9	บุคลากรของ สนข. สามารถปรับตัวกับเทคโนโลยีใหม่ และพร้อมเรียนรู้และพัฒนา

ตารางที่ ๔-๒ ผลการวิเคราะห์ปัจจัยภายในเพื่อกำหนดเป็นจุดอ่อน (Weaknesses)

รหัส	จุดอ่อน (Weaknesses)
W1	กลยุทธ์การพัฒนาดิจิทัลของ สนข. ที่ผ่านมามีครอบคลุมทุกยุทธศาสตร์ของแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย
W2	มีการประชาสัมพันธ์และการสร้างการตระหนักรู้ในเรื่องความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรของ สนข. ไม่มากเท่าที่ควร
W3	สถานที่และพื้นที่ในส่วนของการบริหารและปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ มีโครงสร้าง และพื้นที่จำกัด ซึ่งยังไม่ได้มาตรฐาน ในการจัดวางอุปกรณ์ของระบบรักษาความมั่นคงปลอดภัยด้าน ICT
W4	ระบบรักษาความมั่นคงปลอดภัยด้าน ICT ของ สนข. ยังมีไม่เต็มประสิทธิภาพเพียงพอ
W5	ยังไม่มีการจัดทำแนวทางและมาตรการการรับมือภัยคุกคามทางไซเบอร์อย่างเป็นลายลักษณ์
W6	ยังไม่มีมาตรการหรือแนวทางที่ชัดเจนในการดำเนินการเกี่ยวกับระบบติดตาม ฝ้าระวัง และเตือนภัย (Warning System)
W7	บุคลากรด้าน ICT ของ สนข. ที่มีความรู้ ทักษะ และความเชี่ยวชาญเฉพาะทางด้านความมั่นคงปลอดภัย (Digital Skill) ยังมีจำนวนไม่เพียงพอ
W8	บุคลากรของ สนข. บางส่วนยังขาดความรู้ ความเข้าใจ ในการรักษาความมั่นคงปลอดภัยไซเบอร์

การวิเคราะห์สภาพแวดล้อมซึ่งมีผลจากปัจจัยภายนอก ประกอบด้วย การวิเคราะห์ปัจจัยภายนอกเพื่อกำหนดเป็นโอกาส (Opportunities) และการวิเคราะห์ปัจจัยภายนอกเพื่อกำหนดเป็นอุปสรรค (Threats) ดังนี้

ตารางที่ ๔-๓ ผลการวิเคราะห์ปัจจัยภายนอกเพื่อกำหนดเป็นโอกาส (Opportunities)

รหัส	ปัจจัยสภาพแวดล้อมภายนอกที่เป็นโอกาส (Opportunities)
O1	การปรับ สนข. สู่การเป็นองค์กรดิจิทัล ทำให้ต้องมีการออกแบบและพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
O2	การเข้าสู่ยุคสังคมออนไลน์ ทำให้ประชาชนให้ความสนใจข้อมูลข่าวสารต่าง ๆ จากสื่อสังคมออนไลน์ ทำให้ สนข. มีช่องทางในการสื่อสารกับประชาชนมากขึ้น
O3	มีหน่วยงานกลางที่รับผิดชอบขับเคลื่อนงานด้านความมั่นคงปลอดภัยไซเบอร์ ทำหน้าที่ส่งเสริมกำกับ และสนับสนุนงานด้านความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงานภาครัฐ
O4	มีหน่วยงานภายนอกที่สามารถให้การสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัย เช่น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) เป็นต้น
O5	รัฐบาลให้ความสำคัญในการกำหนดทิศทางการพัฒนารัฐบาลดิจิทัล เพื่อบูรณาการข้อมูลประชาชนให้เป็นภาพเดียวกัน และหน่วยงานในภาครัฐให้ความสำคัญกับการบูรณาการฐานข้อมูล ประสานเชื่อมโยงกระบวนการงานสารสนเทศร่วมกัน

รหัส	ปัจจัยสภาพแวดล้อมภายนอกที่เป็นโอกาส (Opportunities)
O6	การพัฒนาของเทคโนโลยีที่หลากหลายและทันสมัย ส่งผลให้ สนข. มีทางเลือกในการพัฒนางานด้านความมั่นคงปลอดภัยไซเบอร์

ตารางที่ ๔-๔ ผลการวิเคราะห์ปัจจัยภายนอกเพื่อกำหนดเป็นอุปสรรค (Threats)

รหัส	ปัจจัยสภาพแวดล้อมที่กำหนดภายนอกที่เป็นอุปสรรค
T1	ข้อจำกัดในการได้รับจัดสรรงบประมาณเกี่ยวกับแผนงาน/โครงการด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.
T2	การเปลี่ยนแปลงของเทคโนโลยีด้าน ICT ที่รวดเร็ว และมีความหลากหลายของการใช้ ICT ที่เพิ่มขึ้น ก่อให้เกิดความเสี่ยงที่มาจากภัยทางไซเบอร์
T3	อุปกรณ์และเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีการพัฒนาตลอดเวลา และมีราคาสูง ส่งผลต่อการขอรับการจัดสรรงบประมาณในการลงทุน
T4	ภัยทางไซเบอร์มีการพัฒนารูปแบบ กระบวนการ และความรุนแรงในการโจมตีอย่างต่อเนื่อง
T5	ระบบความมั่นคงปลอดภัยทางด้าน ICT ของหน่วยงานภาครัฐส่วนใหญ่ยังขาดการบูรณาการร่วมกัน

๔.๒.๒ การวิเคราะห์ด้วย TOWS Matrix

จากการวิเคราะห์สภาพแวดล้อมด้วยการทำ SWOT Analysis ทำให้ทราบถึงปัจจัยสภาพแวดล้อมภายนอก ซึ่งได้แก่ โอกาสและอุปสรรค และปัจจัยสภาพแวดล้อมภายใน ซึ่งได้แก่ จุดแข็งและจุดอ่อน ที่ส่งผลต่อกระบวนนโยบายการพัฒนาและการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของ สนข. ซึ่งสามารถนำสิ่งที่ได้จากการวิเคราะห์มากำหนดเป็นแผนงาน เพื่อนำไปสู่การกำหนดโครงการต่าง ๆ โดยการวิเคราะห์ด้วยเครื่องมือ TOWS Matrix สามารถแสดงได้ดังในภาพที่ ๔-๓



ภาพที่ ๔-๔ การวิเคราะห์สภาพแวดล้อมโดยใช้เครื่องมือ TOWS Matrix

TOWS Matrix เป็นเครื่องมือในการกำหนดกลยุทธ์ โดยวิธีการจับคู่กันระหว่างปัจจัยสภาพแวดล้อมภายนอกกับปัจจัยสภาพแวดล้อมภายใน คำว่า “TOWS” เป็นตัวย่อที่มาจากแต่ละปัจจัย ได้แก่

อุปสรรค (Threats) โอกาส (Opportunities) จุดอ่อนหรือข้อด้อย (Weaknesses) และ จุดแข็ง (Strengths) ซึ่งการจับคู่กันนี้ จะได้ผลเป็นกลยุทธ์ทั้งหมด ๔ รูปแบบ ได้แก่

๑) กลยุทธ์ SO การจับคู่กันระหว่างจุดแข็งกับโอกาส (SO) เพื่อนำจุดแข็งที่มีอยู่ร่วมกับโอกาสที่ปรากฏมากำหนดแผนงานโครงการที่จะพัฒนา

๒) กลยุทธ์ ST การจับคู่กันระหว่างจุดแข็งกับความเสี่ยง (ST) เพื่อนำจุดแข็งที่มีอยู่มากำหนดเป็นกลยุทธ์ในการขับเคลื่อนแผน เพื่อป้องกันหรือหลีกเลี่ยงอุปสรรคที่จะเกิดขึ้นจากภายนอก

๓) กลยุทธ์ WO การจับคู่กันระหว่างจุดอ่อนกับโอกาส (WO) เพื่อนำโอกาสที่ปรากฏอยู่มากำหนดเป็นกลยุทธ์ในการขับเคลื่อนแผนเพื่อกำจัดหรือลดจุดอ่อนที่มี

๔) กลยุทธ์ WT การจับคู่กันระหว่างจุดอ่อนกับอุปสรรค (WT) เป็นการกำหนดกลยุทธ์ในการขับเคลื่อนแผน เพื่อกำจัดหรือลดจุดอ่อนที่มี และป้องกันหรือหลีกเลี่ยงภัยคุกคามที่เกิดจากภายนอกด้วยในขณะเดียวกัน

ตารางที่ ๔-๕ กลยุทธ์ที่ได้จากการวิเคราะห์ TOWS Matrix

ปัจจัย	จุดแข็ง (Strengths-S)	จุดอ่อน (Weaknesses-W)
โอกาส (Opportunities-O)	กลยุทธ์เชิงรุก SO <ul style="list-style-type: none"> - การทบทวนนโยบายและแผนงานของหน่วยงาน เพื่อสร้างนิเวศที่เอื้อต่องานด้านความมั่นคงปลอดภัยไซเบอร์ (S1, S2, S3, S4 กับ O1, O2) - การเฝ้าระวังภัยไซเบอร์และการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (S5, S6, S7 กับ O3, O4) - การพัฒนาระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้ได้มาตรฐานสากล (S4, S5, S6, S7 กับ O3, O4, O5, O6) - การพัฒนาบุคลากร ICT ให้มีความรู้ทักษะ และความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์ และมีความเป็นมืออาชีพ (S1, S3, S4, S8, S9 กับ O1, O2, O6) 	กลยุทธ์เชิงแก้ไข WO <ul style="list-style-type: none"> - การปรับปรุงซอฟต์แวร์และเฟิร์มแวร์ให้ทันสมัยและปลอดภัย (W4 กับ O1, O6) - การปรับปรุงแนวทาง มาตรการ และแนวปฏิบัติ เพื่อเพิ่มศักยภาพงานความมั่นคงปลอดภัยไซเบอร์ (W1, W5, W6 กับ O1, O3, O4, O6) - การสร้างความตระหนักรู้ด้านภัยทางไซเบอร์แก่บุคลากรของ สนข. (W2, W8 กับ O1, O3, O5)
อุปสรรค (Threats-T)	กลยุทธ์เชิงป้องกัน ST <ul style="list-style-type: none"> - การพัฒนาศักยภาพงานป้องกันและรับมือภัยคุกคามทางไซเบอร์ (S4, S5, S6, S7 กับ T1, T2, T3, T4, T5) - การบริหารความต่อเนื่องของงานด้าน ICT (S4, S5 กับ T1, T2, T3, T4) - การสร้างความร่วมมือในงานด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานอื่น (S6 กับ T5) 	กลยุทธ์เชิงรับ WT <ul style="list-style-type: none"> - การพัฒนาบุคลากรด้าน ICT ให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี (W3, W4, W7 กับ T2, T4) - การบริหารความเสี่ยงและการกำหนดมาตรการและแนวทาง การรับมือภัยคุกคามทางไซเบอร์ (W1, W5, W6 กับ T1, T2, T3, T4, T5)

ปัจจัย	จุดแข็ง (Strengths-S)	จุดอ่อน (Weaknesses-W)
		- การแก้ปัญหาด้านภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (W3, W4, W5, W6 W7, กับ T1, T2, T4, T5)

จากการวิเคราะห์ TOWS Matrix สามารถนำมาเชื่อมโยงเพื่อหาความสัมพันธ์และจัดกลุ่มเข้าด้วยกัน เพื่อกำหนดเป็นแผนงาน ได้ดังนี้

ตารางที่ ๔-๖ การเชื่อมโยงกลยุทธ์ที่ได้จาก TOWS Matrix ไปสู่การกำหนดแผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ สนข. พ.ศ. ๒๕๖๙ - ๒๕๗๐)

ที่	ประเด็น	กลยุทธ์	แผนงาน/โครงการ/กิจกรรม
๑	การทบทวนนโยบายและแผนงานของหน่วยงาน เพื่อสร้างนิเวศที่เอื้อต่องานด้านความมั่นคงปลอดภัยไซเบอร์ (S1, S2, S3, S4 กับ O1, O2)	กลยุทธ์เชิงรุก (SO)	๑. จัดทำแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สนข. ๒. จัดทำและทบทวน ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๓. จัดทำและทบทวน แผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของ สนข. ๔. จัดทำและทบทวน แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Plan) ๕. จัดทำและทบทวน แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ๖. จัดทำและทบทวน แผนบริหารความต่อเนื่องด้านระบบสารสนเทศ Business Continuity Plan (BCP) ๗. จัดทำและทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สนข. ๘. การดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของ สนข.
๒	การเฝ้าระวังภัยไซเบอร์และการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (S5, S6, S7 กับ O3, O4)	กลยุทธ์เชิงรุก (SO)	๑. การดำเนินการติดตามและเฝ้าระวังภัยคุกคามทางไซเบอร์ ๒. การดำเนินการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ของหน่วยงานตามกฎหมาย

ที่	ประเด็น	กลยุทธ์	แผนงาน/โครงการ/กิจกรรม
			๓. การกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ
๓	การพัฒนาระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้ได้มาตรฐานสากล (S4, S5, S6, S7 กับ O3, O4, O5, O6)	กลยุทธ์เชิงรุก (SO)	๑. จัดทำโครงสร้างพื้นฐานและอุปกรณ์ดิจิทัลทั้งด้านฮาร์ดแวร์ (Hardware) ด้านซอฟต์แวร์ (Software) และด้านเซิร์ฟเวอร์ และเน็ตเวิร์ค (Network) ให้เหมาะสมและเพียงพอต่อการปฏิบัติงาน ๒. จัดทำสถาปัตยกรรมองค์กร (Enterprise Architecture) ของ สนข. ๓. โครงการพัฒนาระบบเว็บท่า สนข. ๔. โครงการจัดจ้างผู้เชี่ยวชาญเพื่อพัฒนาและปรับปรุงระบบสารสนเทศ ให้ผ่านการรับรองมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ISO/IEC 27001:2013
๔	การพัฒนาบุคลากร ICT ให้มีความรู้ทักษะ และความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์ และมีความเป็นมืออาชีพ (S1, S3, S4, S8, S9 กับ O1, O2, O6)	กลยุทธ์เชิงรุก (SO)	๑. การพัฒนาทักษะ และยกระดับความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ ของบุคลากร ICT สนข.
๕	การพัฒนาศักยภาพงานป้องกันและรับมือภัยคุกคามทางไซเบอร์ (S4, S5, S6, S7 กับ T1, T2, T3, T4, T4)	กลยุทธ์เชิงป้องกัน (ST)	๑. โครงการบำรุงรักษาระบบคอมพิวเตอร์และเครือข่าย ๒. โครงการบำรุงรักษาระบบเว็บท่า สนข. ๓. โครงการจัดจ้างผู้เชี่ยวชาญเพื่อพัฒนาและปรับปรุงระบบสารสนเทศ ให้ผ่านการรับรองมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ISO/IEC 27001:2013
๖	การบริหารความต่อเนื่องของงานด้าน ICT (S4, S5 กับ T1, T2, T3, T4)	กลยุทธ์เชิงป้องกัน (ST)	๑. จัดทำและทบทวน แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Plan) ๒. จัดทำและทบทวน แผนแก้ไขปัญหจากสถานการณ์ความไม่แน่นอน และภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

ที่	ประเด็น	กลยุทธ์	แผนงาน/โครงการ/กิจกรรม
			<p>๓. จัดทำและทบทวน แผนบริหารความต่อเนื่องด้านระบบสารสนเทศ Business Continuity Plan (BCP)</p> <p>๔. จัดทำและทบทวน แผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของ สนข.</p> <p>๕. จัดทำและทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สนข.</p>
๗	การสร้างความร่วมมือในงานด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานอื่น (S6 กับ T5)	กลยุทธ์เชิงป้องกัน (ST)	๑. การดำเนินงานให้สอดคล้องและเป็นไปตามหน่วยงานกลางที่รับผิดชอบขับเคลื่อนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ ของประเทศ
๘	การปรับปรุงซอฟต์แวร์และเฟิร์มแวร์ให้ทันสมัยและปลอดภัย (W4 กับ O1, O6)	กลยุทธ์เชิงแก้ไข (WO)	<p>๑. โครงการบำรุงรักษาระบบคอมพิวเตอร์และเครือข่าย</p> <p>๒. โครงการบำรุงรักษาระบบเว็บท่า สนข.</p> <p>๓. การดำเนินการติดตามและเฝ้าระวังภัยคุกคามทางไซเบอร์</p>
๙	การปรับปรุงแนวทาง มาตรการ และแนวปฏิบัติ เพื่อเพิ่มศักยภาพงานด้านความมั่นคงปลอดภัยไซเบอร์ (W1, W5, W6 กับ O1, O3, O4, O6)	กลยุทธ์เชิงแก้ไข (WO)	๑. จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สนข.
๑๐	การสร้างความรู้ความตระหนักรู้ด้านภัยทางไซเบอร์แก่บุคลากรของ สนข. (W2, W8 กับ O1, O3, O5)	กลยุทธ์เชิงแก้ไข (WO)	<p>๑. ฝึกอบรมและการสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของบุคลากร สนข.</p> <p>๒. การจัดทำ และเผยแพร่สื่อประชาสัมพันธ์ หรือสื่ออินโฟกราฟิกเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์</p>
๑๑	การพัฒนาบุคลากรด้าน ICT ให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี (W3, W4, W7 กับ T2, T4)	กลยุทธ์เชิงรับ (WT)	พัฒนาทักษะ และยกระดับความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ ของบุคลากร ICT สนข.
๑๒	การบริหารความเสี่ยงและการกำหนดมาตรการและแนวทางการรับมือภัยคุกคามทางไซเบอร์ (W1, W5, W6 กับ T1, T2, T3, T4, T5)	กลยุทธ์เชิงรับ (WT)	<p>๑. จัดทำและทบทวน แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Plan)</p> <p>๒. จัดทำและทบทวน แผนแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)</p>

ที่	ประเด็น	กลยุทธ์	แผนงาน/โครงการ/กิจกรรม
			๓. จัดทำและทบทวน แผนบริหาร ความต่อเนื่องด้านระบบสารสนเทศ Business Continuity Plan (BCP) ๔. จัดทำและทบทวน แผนรับมือภัย คุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของ สนข. ๕. จัดทำและทบทวนแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของ สนข.
๑๓	การแก้ปัญหาด้านภัยคุกคาม ทางไซเบอร์ที่เกิดขึ้น (W3, W4, W5, W6 W4, กับ T1, T2, T4, T5)	กลยุทธ์เชิงรับ (WT)	๑. โครงการบำรุงรักษาระบบคอมพิวเตอร์ และเครือข่าย ๒. การดำเนินการติดตามและเฝ้าระวัง ภัยคุกคามทางไซเบอร์

จากการวิเคราะห์ TOWS Matrix ทำให้สามารถสรุปประเด็นและกลยุทธ์ในการพัฒนางานด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งสามารถนำไปกำหนดเป็นแผนงาน/โครงการ เพื่อนำไปสู่การขับเคลื่อนและเพิ่มศักยภาพให้ได้ครอบคลุมตามประเด็นดังกล่าวข้างต้นด้วย

บทที่ ๕

แผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.

จากการวิเคราะห์ในบทที่ ๔ นั้น ทำให้ทราบถึงความต้องการและแนวทางในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. และสามารถนำมาเป็นกรอบนโยบายและทิศทางในการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามวิสัยทัศน์และพันธกิจที่กำหนดไว้ การดำเนินงานของแผนงานโครงการ และกิจกรรมต่าง ๆ ตามแผน ตลอดจนมีการพัฒนากลไกและระบบในการติดตามผลการดำเนินงานอย่างเป็นระบบ เพื่อให้เกิดผลในทางปฏิบัติได้อย่างเป็นรูปธรรม และสามารถขับเคลื่อนให้สามารถบรรลุเป้าหมายความสำเร็จได้มีปัจจัยในการดำเนินงานในประเด็น ดังต่อไปนี้

๕.๑ มาตรการส่งเสริมงานด้านความมั่นคงปลอดภัยไซเบอร์

สนข. ได้มีการจัดทำมาตรการส่งเสริมงานด้านความมั่นคงปลอดภัยไซเบอร์ โดยได้กำหนดเป็นแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการวางแผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤต ด้านสารสนเทศ (Business Continuity Plan : BCP) เพื่อให้มีแนวปฏิบัติและความต่อเนื่องของการใช้งานของระบบสารสนเทศของ สนข. จึงจำเป็นต้องมีการดำเนินการดังนี้

๕.๑.๑ จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สนข.

ด้วยปัญหายุ่งยากความทางไซเบอร์ที่มีความรุนแรงเพิ่มมากขึ้น ซึ่งอาจส่งผลกระทบต่อการทำงานของระบบสารสนเทศของ สนข. ทำให้การดำเนินงานต่าง ๆ ที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศ เกิดผลกระทบและปัญหาต่อการปฏิบัติงานของเจ้าหน้าที่ ทำให้ขาดความเชื่อมั่นต่อการทำงานด้วยระบบอิเล็กทรอนิกส์ในทุกรูปแบบ ดังนั้น เพื่อให้ สนข. มีความมั่นคงปลอดภัยและสร้างความเชื่อถือ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล จึงต้องกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ สนข. ขึ้นเพื่อใช้เป็นแนวทางในการดำเนินงานและกิจกรรมการรักษาความมั่นคงปลอดภัยให้แก่ระบบสารสนเทศของ สนข.

๕.๑.๒ จัดทำแผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤตด้านสารสนเทศ Business Continuity Plan (BCP) ของ สนข.

BCP คือ เอกสารคำแนะนำและวิธีการที่ช่วยให้การบริการด้านเทคโนโลยีสารสนเทศขององค์กรสามารถตอบสนองต่อการเกิดอุบัติเหตุ ภัยพิบัติ ภาวะฉุกเฉินและ/หรือภัยคุกคามได้โดยไม่ต้องหยุดหรืออุปสรรคในการดำเนินงานที่สำคัญ ดังนั้น จำเป็นจะต้องมีแผนการกู้คืนระบบหรือแผนการกู้คืนทรัพยากรบุคคลและกระบวนการทำงาน เพื่อให้สามารถดำเนินงานต่อไปได้ ในการดำเนินการวางแผนต่อเนื่อง BCP จะช่วยให้การบริการที่สำคัญ ๆ ด้านเทคโนโลยีสารสนเทศ สามารถใช้งานได้อย่างต่อเนื่อง จึงจำเป็นต้องมีการจัดทำแผนบริหารความพร้อมต่อเนื่องด้านระบบสารสนเทศของ สนข. ขึ้นเพื่อรองรับต่อระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ รวมถึงความมั่นคงปลอดภัยทางไซเบอร์ เพื่อใช้เป็นแนวทางให้ สนข. สามารถดำเนินการได้อย่างต่อเนื่อง

๕.๑.๓ สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Awareness)

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Awareness) คือ การให้บุคลากรขององค์กร รวมถึงการบริหารจัดการบุคคลหรือกลุ่มบุคคลให้ได้รับข้อมูล โครงการ ความมั่นคงปลอดภัยทางไซเบอร์ และสร้างแผนการกระจายข้อมูลสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ไปยังบุคลากรในองค์กร เพื่อสร้างเข้าใจว่าบุคลากรขององค์กรนั้น คือส่วนหนึ่งที่สำคัญต่อการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้บุคลากรต้องทราบถึงรูปแบบของภัยคุกคามต่าง ๆ และต้องสามารถตอบสนองกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้ตามนโยบายและแนวทางขององค์กรที่ประกาศไว้ได้อย่างเหมาะสม จึงมีความจำเป็นต้องสร้างความตระหนักให้กับบุคลากรในองค์กร เพราะการสร้างให้บุคลากรในองค์กรมีบทบาทที่ให้องค์กรเกิดความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยทำให้บุคลากรมีความรู้เท่าทันต่อภัยคุกคามที่เกิดขึ้น และต้องทำให้เกิดความรู้สึกในเชิงบวก ด้านความมั่นคงปลอดภัย และการสร้างให้บุคลากรมีความตระหนักรู้ภัยเกี่ยวกับภัยทางไซเบอร์ รวมไปถึงการมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยให้ระบบสารสนเทศได้อย่างแท้จริง

๕.๒ เป้าหมายการดำเนินงาน

ตามแผนปฏิบัติการดิจิทัลสำนักงานนโยบายและแผนการขนส่งและจราจร พ.ศ. ๒๕๖๖ - ๒๕๗๐ ได้มีการกำหนดยุทธศาสตร์ที่ ๕ พัฒนาระบบบริหารจัดการมุ่งสู่องค์กรดิจิทัล (Digital Management) เป้าประสงค์ คือ เชื่อมโยงกระบวนการทำงานระหว่างหน่วยงานภายในและภายนอก รวมทั้งความมั่นคงปลอดภัยทางไซเบอร์ มีกลยุทธ์ที่เกี่ยวข้อง ได้แก่

- กลยุทธ์ที่ ๑๑ สร้างความเชื่อมั่นต่อ ระบบการปฏิบัติงานและการให้บริการว่าปลอดภัยจากภัยคุกคามทางไซเบอร์ (Infrastructure & Security)
- กลยุทธ์ที่ ๑๒ กำหนดแนวปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
- กลยุทธ์ที่ ๑๓ จัดทำ พัฒนา ปรับปรุง โครงสร้างพื้นฐานด้านดิจิทัลของ สนข. ให้มีความทันสมัยรองรับการดำเนินงานในรูปแบบดิจิทัลที่มีความมั่นคงปลอดภัย

ดังนั้น เพื่อให้เป็นไปตามเป้าประสงค์ ประกอบกับการวิเคราะห์ระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. จึงได้กำหนดเป้าหมายการขับเคลื่อนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ในปีงบประมาณ พ.ศ. ๒๕๖๘ - ๒๕๗๐ ดังนี้

ตารางที่ ๕-๑ เป้าหมายการดำเนินงานเพื่อขับเคลื่อนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ในปีงบประมาณ พ.ศ. ๒๕๖๘ - ๒๕๗๐

ปีงบประมาณ	เป้าหมายการดำเนินงาน
ปีงบประมาณ พ.ศ. ๒๕๖๘ (ดำเนินการแล้ว)	๑. ทบทวนและประกาศนโยบาย ระเบียบ ข้อบังคับ แนวปฏิบัติ มาตรการการดำเนินงานต่าง ๆ ที่สอดคล้องกับการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ๒. มีนโยบายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของ สนข. ๓. จัดทำอุปกรณ์และระบบความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพอย่างต่อเนื่อง ๔. อบรมบุคลากรของ สนข. ให้มีความรู้ความเข้าใจ และตระหนักรู้ถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ ๕. พัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ให้บุคลากร ICT ของหน่วยงาน

ปีงบประมาณ	เป้าหมายการดำเนินงาน
ปีงบประมาณ พ.ศ. ๒๕๖๙	๑. มีการประเมินด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ๒. ทบทวนและประกาศนโยบาย ระเบียบ ข้อบังคับ แนวปฏิบัติ มาตรการการดำเนินงานต่าง ๆ ที่สอดคล้องกับการดำเนินงาน ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างต่อเนื่อง ๓. อบรมบุคลากรของ สนข. ให้มีความรู้ความเข้าใจ และตระหนักรู้ ถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างต่อเนื่อง ๔. จัดหาอุปกรณ์และเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ที่มีประสิทธิภาพ อย่างต่อเนื่อง ๕. มีโครงสร้างสถาปัตยกรรมด้านระบบสารสนเทศของหน่วยงาน (Enterprise Architecture) ของ สนข.
ปีงบประมาณ พ.ศ. ๒๕๗๐	๑. จัดหาอุปกรณ์และเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ที่มีประสิทธิภาพ อย่างต่อเนื่อง ๒. พัฒนาระบบเว็บท่า สนข. ที่มีความมั่นคงปลอดภัยทางไซเบอร์ และมีประสิทธิภาพ ๓. ได้รับการประเมินด้านความมั่นคงปลอดภัยโดยหน่วยงานภายใน หรือภายนอก ตามมาตรฐานสากล

จากเป้าหมายการขับเคลื่อนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ในปีงบประมาณ พ.ศ. ๒๕๖๘ - ๒๕๗๐ ได้นำมากำหนดเป็นแผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัย ไซเบอร์ของ สนข. พ.ศ. ๒๕๖๙ - ๒๕๗๐ โดยมีแผนงาน โครงการ และกิจกรรม ดังนี้

๕.๓ แผนงาน/โครงการ/กิจกรรม ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ - ๒๕๗๐

ตารางที่ ๕-๒ แผนงาน/โครงการ/กิจกรรม ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ - ๒๕๗๐

แผนงาน/โครงการ/กิจกรรม	ผลผลิต	เป้าหมายตามแผนปฏิบัติการ (ปีงบประมาณ)		งบประมาณรวม (บาท)	ผู้รับผิดชอบ
		พ.ศ. ๒๕๖๙	พ.ศ. ๒๕๗๐		
๑. จัดทำสถาปัตยกรรมองค์กร (Enterprise Architecture) ของ สนข.	- มีสถาปัตยกรรมองค์กร (Enterprise Architecture) ของ สนข.	✓ (๑ ฉบับ)	-	-	ศทท.
๒. จัดทำและทบทวนแผนการซักซ้อม และรับมือภัยความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์ สนข.	เพื่อให้ สนข. มีความพร้อมในการรับมือและแก้ไข สถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยี สารสนเทศที่หยุดชะงักไม่สามารถให้บริการได้และ มีการทบทวนและซักซ้อมแผนฯ เป็นประจำ อย่างต่อเนื่อง	✓ (๑ ฉบับ)	✓ (๑ ฉบับ)	-	ศทท.
๓. พัฒนาทักษะ และยกระดับความรู้ ความสามารถด้านความมั่นคงปลอดภัย ไซเบอร์ของบุคลากร ICT สนข.	- บุคลากร ICT สนข. ได้รับการฝึกอบรมเพื่อพัฒนา ทักษะ และยกระดับความรู้ ความสามารถ ด้านความมั่นคงปลอดภัยไซเบอร์ ในรูปแบบ On-site หรือ On-line	✓ (๑ หลักสูตร) (อยู่ระหว่างดำเนินการ)	✓ (๑ หลักสูตร)	-	ศทท.
๔. ฝึกอบรมและการสร้างความตระหนักรู้ เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ของบุคลากร สนข. ในระดับผู้ปฏิบัติงาน	- บุคลากรของ สนข. ในระดับผู้ปฏิบัติงาน มีความรู้ ความเข้าใจ และตระหนักรู้ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - มีกระบวนการติดตามผลการตระหนักรู้ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	✓ (๑ หลักสูตร) (อยู่ระหว่างดำเนินการ)	✓ (๑ หลักสูตร)	-	ศทท.
๕. จัดทำและเผยแพร่สื่อประชาสัมพันธ์ หรือสื่ออินโฟกราฟิกด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์	- มีการเผยแพร่สื่อประชาสัมพันธ์หรือสื่ออินโฟกราฟิก ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ผ่านสื่อ ช่องทางต่าง ๆ	✓ (๓ ชิ้นงาน) (อยู่ระหว่างดำเนินการ)	✓ (๓ ชิ้นงาน)	-	ศทท.

แผนงาน/โครงการ/กิจกรรม	ผลผลิต	เป้าหมายตามแผนปฏิบัติการ (ปีงบประมาณ)		งบประมาณรวม (บาท)	ผู้รับผิดชอบ
		พ.ศ. ๒๕๖๙	พ.ศ. ๒๕๗๐		
๖. จัดทำและทบทวนแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช.	- มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช. - มีการทบทวนแนวปฏิบัติฯ อย่างต่อเนื่อง	✓ (๑ ฉบับ) (อยู่ระหว่างจัดทำ)	✓ (๑ ฉบับ)	-	ศทท.
๗. จัดทำและทบทวนแผนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	- มีแผนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - มีการทบทวนแผนฯ อย่างต่อเนื่อง	✓ (๑ ฉบับ)	✓ (๑ ฉบับ)	-	ศทท.
๘. จัดทำและทบทวน แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Plan) ของ สนช.	- มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Plan) ของ สนช. - มีการทบทวนแผนฯ อย่างต่อเนื่อง	✓ (๑ ฉบับ)	✓ (๑ ฉบับ)	-	ศทท.
๙. จัดทำและทบทวนแผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Audit Plan : CSAP) ของ สนช.	- มีแผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ - มีการทบทวนแผนฯ อย่างต่อเนื่อง	✓ (๑ ฉบับ)	✓ (๑ ฉบับ)	-	ศทท.
๑๐. จัดทำและทบทวนแผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของ สนช.	- มีแผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของ สนช. - มีการทบทวนแผนฯ อย่างต่อเนื่อง	✓ (๑ ฉบับ)	✓ (๑ ฉบับ)	-	ศทท.
๑๑. จัดทำและทบทวนแนวปฏิบัติการบริหารจัดการและสื่อสารในภาวะวิกฤตด้านไซเบอร์ (Crisis Communication Management Plan) ของ สนช.	- มีแนวปฏิบัติการบริหารจัดการและสื่อสารในภาวะวิกฤตด้านไซเบอร์ - มีการทบทวนแนวปฏิบัติฯ อย่างต่อเนื่อง	✓ (๑ ฉบับ)	✓ (๑ ฉบับ)	-	ศทท.
๑๒. จัดทำและทบทวนแผนแก้ไขสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของ สนช.	- มีแผนแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ - มีการทบทวนแผนฯ อย่างต่อเนื่อง	✓ (๑ ฉบับ)	✓ (๑ ฉบับ)	-	ศทท.

แผนงาน/โครงการ/กิจกรรม	ผลผลิต	เป้าหมายตามแผนปฏิบัติการ (ปีงบประมาณ)		งบประมาณรวม (บาท)	ผู้รับผิดชอบ
		พ.ศ. ๒๕๖๙	พ.ศ. ๒๕๗๐		
๑๓. จัดทำและทบทวนการบริหาร ความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) และแผนความต่อเนื่องทางธุรกิจ ด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP)	- มีแผนบริหารความต่อเนื่องด้านระบบสารสนเทศ Business Continuity Plan (BCP) สนข. - มีการทบทวนแผนฯ อย่างต่อเนื่อง	✓ (๑ ฉบับ)	✓ (๑ ฉบับ)	-	ศทท.
๑๔. การดำเนินงานด้านการคุ้มครองข้อมูล ส่วนบุคคล (PDPA) ของ สนข.	- มีการทบทวนการดำเนินงานตามประกาศ การคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของ สนข.	✓ (๑ ฉบับ)	✓ (๑ ฉบับ)	-	ศทท.
๑๕. จัดทำโครงสร้างพื้นฐานและอุปกรณ์ ดิจิทัลทั้งด้านฮาร์ดแวร์ (Hardware) ด้านซอฟต์แวร์ (Software) และ ด้านเซิร์ฟเวอร์ (Server) และเน็ตเวิร์ค (Network) ให้เหมาะสมและเพียงพอ ต่อการปฏิบัติงาน	- มีครุภัณฑ์สำหรับพัฒนาโครงสร้างพื้นฐาน และอุปกรณ์ดิจิทัล ทั้งด้านฮาร์ดแวร์ (Hardware) ด้านซอฟต์แวร์ (Software) ด้านเซิร์ฟเวอร์ (Server) และเน็ตเวิร์ค (Network)	✓ (๒ โครงการ) (๑๙.๓ ล้านบาท)	✓ (๑ โครงการ) (๔.๙ ล้านบาท)	๔๑.๕ ล้านบาท	ศทท.
๑๖. โครงการบำรุงรักษาระบบคอมพิวเตอร์ และเครือข่าย	- ระบบสามารถทำงานได้อย่างเป็นปกติ - รายงานผลการบำรุงรักษาระบบคอมพิวเตอร์ และเครือข่าย	✓ (๑ โครงการ) (๒.๐๓ ล้านบาท)	✓ (๑ โครงการ) (๒.๐๓ ล้านบาท)	๖.๑ ล้านบาท	ศทท.
๑๗. โครงการบำรุงรักษาระบบเว็บท่า สนข.	- ระบบสามารถทำงานได้อย่างเป็นปกติ - รายงานผลการบำรุงรักษาระบบเว็บท่า สนข.	✓ (๑ โครงการ) (๐.๔ ล้านบาท)	✓ (๑ ระบบ) (๐.๔ ล้านบาท)	๑.๒ ล้านบาท	ศทท.

แผนงาน/โครงการ/กิจกรรม	ผลผลิต	เป้าหมายตามแผนปฏิบัติการ (ปีงบประมาณ)		งบประมาณรวม (บาท)	ผู้รับผิดชอบ
		พ.ศ. ๒๕๖๙	พ.ศ. ๒๕๗๐		
๑๘. การสร้างความร่วมมือในงานด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานอื่น	- มีการดำเนินงานร่วมงานด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานอื่น	✓ (๑ เรื่อง)	✓ (๑ เรื่อง)	-	ศทท.
๑๙. การกำหนดและทบทวนมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ	- มีรายงานมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศ	✓ (๑ ฉบับ)	✓ (๑ ฉบับ)	-	ศทท.
๒๐. การติดตามและเฝ้าระวังภัยคุกคามทางไซเบอร์	- มีการติดตามและเฝ้าระวังภัยคุกคามทางไซเบอร์เป็นประจำ	✓ (๑ งาน)	✓ (๑ งาน)	-	ศทท.
๒๑. โครงการพัฒนาระบบเว็บทำ สนข.	- มีระบบเว็บทำ สนข. ที่ทันสมัย ทำงานได้อย่างมีประสิทธิภาพ และมีความมั่นคงปลอดภัย	-	✓ (๔.๕ ล้าน) (๑ ระบบ)	๔.๕ ล้าน	ศทท.
๒๒. โครงการจัดซื้อและติดตั้งเครื่องกำเนิดไฟฟ้าสำรองฉุกเฉิน (Generator) สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)	- ระบบไฟฟ้าสำรองฉุกเฉิน (Generator) สำหรับศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ของ สนข.	-	✓ (๓.๑ ล้าน) (๑ งาน)	๓.๑ ล้าน	ศทท.
๒๓. โครงการปรับปรุงประสิทธิภาพระบบการรักษาความมั่นคงปลอดภัยภายในศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)	- มีระบบดับเพลิงอัตโนมัติด้วยสารสะอาดภายในห้อง Data Center - มีระบบเฝ้าระวังและระบบบริหารจัดการศูนย์ข้อมูลและรักษาความปลอดภัยภายในห้อง Data Center	-	✓ (๖ ล้าน) (๑ ฉบับ)	๖ ล้าน	ศทท.
คิดเป็นงบประมาณรวมทั้งสิ้น (บาท)				๖๒.๖ ล้าน	

๕.๔ การติดตามประเมินผลการดำเนินงานตามแผนงาน

เพื่อให้การขับเคลื่อนแผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร พ.ศ. ๒๕๖๙ - ๒๕๗๐ เกิดประสิทธิภาพตามเป้าหมายที่กำหนด จำเป็นต้องมีกระบวนการติดตาม ตรวจสอบ และประเมินผลการดำเนินงานโครงการอย่างต่อเนื่อง เพื่อนำไปสู่การบริหารจัดการภาครัฐที่มุ่งผลสัมฤทธิ์ของการปฏิบัติงานเป็นหลัก โดยให้ทุกฝ่ายได้มีส่วนร่วมในการผลักดันโครงการ และมีความเข้าใจไปในทิศทางเดียวกัน เพื่อเพิ่มความโปร่งใสในการดำเนินงาน ตลอดจนการพัฒนากระบวนการและกลไกการติดตามประเมินผลที่มีประสิทธิภาพ สามารถติดตามความก้าวหน้า และประเมินผลการดำเนินงานอย่างสม่ำเสมอ โดยให้ความสำคัญกับการลดต้นทุนค่าใช้จ่ายและเพิ่มประสิทธิภาพ โดยใช้จ่ายงบประมาณอย่างคุ้มค่าและเหมาะสม ซึ่งมีแนวทางการกำหนดระบบการติดตาม ดังนี้

๑) การติดตามความก้าวหน้าในขณะดำเนินการและประเมินผลการขับเคลื่อนแผนงาน โครงการ ทั้งในระดับผลลัพธ์ ผลลัพธ์ และผลกระทบ เพื่อประเมินผลแผนที่ได้รับจากการดำเนินการ ทั้งนี้ต้องให้ความสำคัญกับการกำหนดเกณฑ์ของตัวชี้วัดเพื่อสะท้อนผลการดำเนินงานได้อย่างมีประสิทธิภาพ

๒) การติดตาม และประเมินผลเมื่อสิ้นสุดการดำเนินงานตามแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานนโยบายและแผนการขนส่งและจราจร พ.ศ. ๒๕๖๙ - ๒๕๗๐

๓) การนำเสนอผลการติดตามประเมินผล ควรนำเสนอผลการประเมินให้ทุกฝ่ายที่เกี่ยวข้อง ให้ได้รับทราบผลการประเมิน เพื่อเป็นข้อมูลนำไปประกอบการปรับปรุง หรือการพัฒนาต่อยอดการดำเนินงานให้มีประสิทธิภาพครอบคลุม สามารถแก้ไขปัญหาได้อย่างมีประสิทธิภาพ

บทที่ ๖

บทสรุปและข้อเสนอแนะ

๖.๑ บทสรุป

แผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ สนข. พ.ศ. ๒๕๖๙ - ๒๕๗๐ จะเป็นแผนเพื่อขับเคลื่อนงานด้านความมั่นคงปลอดภัยด้านไซเบอร์ของ สนข. ซึ่งภายในแผนได้มีการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์เพื่อเพิ่มประสิทธิภาพในการดำเนินงานด้านความมั่นคงปลอดภัยของ สนข. ประกอบกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามมาตรฐานสากล ดังนั้น แผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สนข. พ.ศ. ๒๕๖๙ - ๒๕๗๐ จะทำให้ สนข. เกิดความเชื่อมั่นต่อปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Management System) มีกระบวนการตั้งแต่ การสร้าง การนำมาใช้งาน การดำเนินการ การตรวจสอบติดตามและประเมินผล รวมไปถึงการบำรุงรักษา ดังนั้น การพัฒนาความมั่นคงปลอดภัยด้านไซเบอร์ ต้องคำนึงถึงโครงสร้างตามแนวนโยบายขององค์กร การวางแผน ความรับผิดชอบ การจัดกระบวนการ ขั้นตอนปฏิบัติ และทรัพยากรขององค์กรด้วย ซึ่งวัตถุประสงค์หลักของการรักษาความมั่นคงปลอดภัยไซเบอร์ คือการกำหนดมาตรการและแนวทางที่ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ ที่จะเข้าถึงระบบสารสนเทศของ สนข. และอาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศและข้อมูลซึ่งเป็นเครื่องมือที่สำคัญในการปฏิบัติราชการของ สนข. รวมถึงเพื่อสร้างความตระหนักรู้ให้แก่เจ้าหน้าที่และบุคลากรของ สนข. ในทุกระดับ ให้ได้รับรู้และเข้าใจถึงความจำเป็นในการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมปฏิบัติตามได้อย่างถูกต้องเพื่อหลีกเลี่ยงความเสี่ยงหรือลดความรุนแรงของผลเสียหายที่อาจเกิดขึ้นได้

๖.๒ ปัจจัยความสำเร็จ

การขับเคลื่อนแผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. พ.ศ. ๒๕๖๙ - ๒๕๗๐ ไปสู่การความสำเร็จได้นั้น ขึ้นอยู่กับปัจจัยในหลาย ๆ ด้าน ดังนี้

๖.๒.๑ บทบาทของผู้บริหาร

บทบาทของผู้บริหารนั้นจะต้องเป็นผู้กำหนดนโยบายและกำกับดูแลงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของ สนข. เพื่อให้การดำเนินงานขององค์กรบรรลุจุดมุ่งหมาย โดยอาศัยหน้าที่ทางการบริหารที่สำคัญ คือ การวางแผน (Planning) การจัดการองค์กร (Organizing) การเป็นผู้นำ (Leading) และการควบคุม (Controlling) ซึ่งบทบาทการบริหารจัดการของผู้บริหารยังมีเป้าหมายสำคัญอยู่ที่การพัฒนาบุคลากรให้มีความรู้ ความเชี่ยวชาญในงานที่รับผิดชอบเพื่อให้สามารถขับเคลื่อนการปฏิบัติงานตามบทบาทและจุดมุ่งหมายขององค์กรให้มีคุณภาพ โดยการใช้ทรัพยากรให้เกิดประโยชน์กับองค์กรมากที่สุด เพื่อนำไปสู่ความสำเร็จ ตามเป้าหมาย และบรรลุตามวัตถุประสงค์

๖.๒.๒ การสนับสนุนด้านงบประมาณ

งบประมาณเป็นปัจจัยหลักในการดำเนินงาน และมีส่วนสำคัญอย่างมากที่จะทำให้การขับเคลื่อนแผนงานโครงการต่าง ๆ สามารถดำเนินงานได้สำเร็จซึ่งต้องมีการจัดสรรงบประมาณที่เหมาะสมและเพียงพอ โดยคำนึงถึงการใช้งบประมาณอย่างคุ้มค่าและมีประสิทธิภาพ รวมทั้งเกิดการพัฒนาอย่างยั่งยืน ซึ่งต้องพิจารณาถึงประโยชน์ที่หน่วยงานจะได้รับจากการดำเนินโครงการทั้งทางด้านประสิทธิภาพ ประสิทธิผล เนื่องจากหากมีปัจจัยเอื้ออำนวยที่พร้อมและเพียงพอก็จะส่งผลให้เกิดความมั่นคงและมีประสิทธิผลสูงสุด

๖.๒.๓ บุคลากร

บุคลากรด้าน ICT จะต้องได้รับการสนับสนุนให้มีความรู้ความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์ และต้องมีส่วนร่วมในการขับเคลื่อนแผนงาน โครงการและกิจกรรมต่าง ๆ เพื่อมุ่งไปสู่การรักษาความเป็นมาตรฐานความมั่นคงปลอดภัยไซเบอร์ในระดับสากล รวมถึงต้องมีการเสริมสร้างองค์ความรู้และความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่เจ้าหน้าที่และบุคลากรของ สนข. ให้มีความรู้ความเข้าใจ และสามารถตระหนักถึงภัยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จะเกิดขึ้น และสามารถนำไปดำเนินการเพื่อปกป้องระบบงานสารสนเทศไปจนถึงข้อมูลสำคัญของตนเองและขององค์กรได้

๖.๓ ข้อเสนอแนะ

สนข. ควรมีการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

- ๑) ควรมีการทบทวนแผน นโยบาย แนวปฏิบัติ รวมไปถึงมาตรการต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์เป็นประจำทุกปี
- ๒) ควรมีการส่งเสริมบุคลากร ICT ของหน่วยงานให้มีความรู้ ทักษะ และความเชี่ยวชาญเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์
- ๓) ควรมีการส่งเสริมให้เจ้าหน้าที่และบุคลากรของ สนข. ในทุกระดับ มีความรู้และการตระหนักถึงการรักษาความมั่นคงปลอดภัยไซเบอร์
- ๔) ควรมีการดำเนินการที่สอดคล้องกับหน่วยงานหลักที่รับผิดชอบด้านความมั่นคงปลอดภัยด้านไซเบอร์ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) รวมไปถึงให้เป็นไปตามมาตรฐานสากลที่เกี่ยวข้องด้วย

เอกสารอ้างอิง

๑. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ (แก้ไขเพิ่มเติม ฉบับที่ ๒ พ.ศ. ๒๕๕๑)
๒. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙
๓. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
๔. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖
๕. คู่มือการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามข้อกำหนดภายใต้ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
๖. แผนปฏิบัติการดิจิทัลของ สนข. พ.ศ. ๒๕๖๖ - ๒๕๗๐
๗. แผนพัฒนาความพร้อมรัฐบาลดิจิทัลของ สนข. พ.ศ. ๒๕๖๗ - ๒๕๗๐

ผู้จัดทำร่าง

นายทรงเกียรติ ตะเภาทอง
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

ที่ปรึกษา

๑. นางสาวจิรัชก ห้วยหงษ์ทอง
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๒. นายณฤทธิ์ มัยรัตน์
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๓. นายพิสิษฐ์ ป้อมทอง
นักวิชาการคอมพิวเตอร์ชำนาญการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๔. นายชัยวัฒน์ ธรรมาสถิตนุกุล
นักวิชาการคอมพิวเตอร์ชำนาญการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร