(ร่าง) แผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
จังหวัดสุรินทร์
พ.ศ. 2570

สารบัญ

บทสรุปผู้บริหาร

จังหวัดสุรินทร์ตั้งอยู่ทางทิศใต้ของภาคตะวันออกเฉียงเหนืออยู่ห่างจากกรุงเทพมหานครทางรถยนต์ประมาณ 450 กิโลเมตร อยู่ในกลุ่มภาคตะวันออกเฉียงเหนือตอนล่าง 1 ซึ่งประกอบด้วย จังหวัดนครราชสีมา ชัยภูมิ บุรีรัมย์ และสุรินทร์ โดยแบ่งเขตการปกครองออกเป็น 17 อำเภอ 158 ตำบล 2128 หมู่บ้าน มีองค์การบริหารส่วนจังหวัด (อบจ.) 1 แห่ง เทศบาลเมือง 2 แห่ง เทศบาลตำบล 26 แห่ง อบต. 144 แห่ง ชุมชน 41 ชุมชน มีส่วนราชการ หน่วยงานรัฐวิสาหกิจ และหน่วยงานที่ตั้งอยู่ในพื้นที่ของจังหวัด จำนวน 327 หน่วยงาน มีวิสัยทัศน์เป็น เมืองเกษตรอินทรีย์ ศูนย์เศรษฐกิจชายแดน ท่องเที่ยววิถีชุมชน โดยจังหวัดสุรินทร์ได้ตระหนักถึงความสำคัญของการนำเทคโนโลยีดิจิทัล มาสนับสนุนการบริหารจัดการส่วนราชการให้เป็นหน่วยงานที่ทันสมัยและมีประสิทธิภาพ พร้อม “ยกระดับ จังหวัดให้เป็นองค์กรดิจิทัล”จึงได้มีการจัดทำแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จังหวัดสุรินทร์ พ.ศ. 2570 เพื่อใช้ปืนเครื่องมือในการกำหนดกรอบแนวทางในการขับเคลื่อน งานด้านเทคโนโลยีสารสนเทศและดิจิทัลของจังหวัดให้สอดคล้องกับนโยบาย แผนและยุทธศาสตร์การพัฒนาด้านเทคโนโลยีสารสนเทศและดิจิทัลตามนโยบายภาครัฐในทุกระดับ

ตามแผนปฏิบัติการดิจิทัล จังหวัดสุรินทร์ พ.ศ. 2568 - 2570 ได้กำหนดเป้าหมายไว้ชัดเจน คือ“การเป็นองค์กรดิจิทัล (Digital Parliament)” ดังนั้น สิ่งสำคัญที่ต้องคำนึงถึงคือ การรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร ซึ่งในแผนปฏิบัติการดิจิทัลจังหวัดสุรินทร์ พ.ศ. 2568 - 2570 ได้มีการกำหนดยุทธศาสตร์ที่ 2 ไว้ คือ ยุทธศาสตร์ที่ ๒ ขับเคลื่อนการปฏิบัติงานทางราชการภายใต้นโยบายและมาตรฐานดิจิทัล และนำดิจิทัลมาใช้พัฒนาการดำเนินงาน ประกอบด้วย 2 กลยุทธ์ คือ

1. ส่งเสริมการปฏิบัติงานให้เป็นไปตามมาตรฐาน/ระเบียบ/ข้อกฎหมายที่เกี่ยวข้อง
2. เพิ่มประสิทธิภาพการปฏิบัติงานสู่การเป็นองค์กรดิจิทัล พัฒนาแพลตฟอร์มดิจิทัลบริการภาครัฐ และพัฒนาเศรษฐกิจดิจิทัล (Digital Economy)

โดยมีเป้าประสงค์เชิงยุทธศาสตร์ คือ เชื่อมโยงกระบวนการทำงานระหว่างหน่วยงานภายในและภายนอก รวมทั้งความมั่นคงปลอดภัยไซเบอร์

ดังนั้น เพื่อให้การพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ของจังหวัดสุรินทร์เป็นไปอย่างมีประสิทธิภาพ และเป็นไปตามมาตรฐานสากล รองรับการให้บริการได้อย่างเท่าเทียมและทั่วถึง จึงได้มีการจัดทำแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จังหวัดสุรินทร์ พ.ศ. 2570 เพื่อใช้เป็นกรอบแนวทางในการกำหนดทิศทางของการรักษาความมั่งคงปลอดภัยไซเบอร์ของจังหวัดฯ ต่อไป

คำนำ

ในปัจจุบัน เทคโนโลยีดิจิทัลได้ก้าวเข้ามาเป็นกลไกหลักในการขับเคลื่อนยุทธศาสตร์การพัฒนาจังหวัดสุรินทร์ในทุกมิติ ไม่ว่าจะเป็นการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data) ผ่านระบบ Surin One-Plan การวิเคราะห์ข้อมูลความยากจนชี้เป้า แพลตฟอร์มตลาดออนไลน์ Surin best แพลตฟอร์มคนหางานออนไลน์ Surin Jobs แพลตฟอร์มบริจาคโลหิตออนไลน์ Surin blood แพลตฟอร์มบริหารจัดการข้อมูลขยะมูลฝอย Surin Clean การพึ่งพาโครงสร้างพื้นฐานดิจิทัลที่เพิ่มมากขึ้นนี้ มาพร้อมกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงและมีความซับซ้อนสูงขึ้น ซึ่งอาจส่งผลกระทบโดยตรงต่อความเชื่อมั่นของประชาชน ความเป็นส่วนตัวของข้อมูลส่วนบุคคล และความมั่นคงของฐานข้อมูลราชการ

แผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จังหวัดสุรินทร์ พ.ศ. 2570 ฉบับนี้ จัดทำขึ้นเพื่อใช้เป็นกรอบแนวทางและทิศทางหลักการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ให้เป็นไปอย่างมีประสิทธิภาพและได้มาตรฐานสากล โดยมุ่งเน้นการบูรณาการความร่วมมือระหว่างส่วนราชการ องค์กรปกครองส่วนท้องถิ่น และภาคีเครือข่ายในพื้นที่ เพื่อสร้างระบบนิเวศดิจิทัลที่มีความมั่นคงปลอดภัย (Cyber Resilience) พร้อมรองรับการขยายตัวของนวัตกรรมภาครัฐ และสร้างความมั่นใจให้กับประชาชนทุกภาคส่วนว่า ข้อมูลและระบบบริการสาธารณะของจังหวัดจะได้รับการปกป้องอย่างสูงสุด

คณะทำงานหวังเป็นอย่างยิ่งว่า แผนปฏิบัติการฉบับนี้จะเป็นเครื่องมือสำคัญในการส่งเสริมให้บุคลากรทุกระดับมีความตระหนักรู้และทักษะที่จำเป็นในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อร่วมกันขับเคลื่อนจังหวัดสุรินทร์สู่การเป็นเมืองอัจฉริยะ (Smart City) ที่มีความมั่นคง ปลอดภัย และยั่งยืนบนฐานของความไว้ใจทางดิจิทัลสืบไป

บทที่ 1

บทนำ

หลักการและเหตุผล

ตามที่รัฐบาลได้มีนโยบายขับเคลื่อนเศรษฐกิจและสังคมดิจิทัล (Digital Economy and Society) มุ่งเน้นการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือสำคัญในการปรับโฉมระบบราชการสู่การเป็นรัฐบาลดิจิทัล (Digital Government) เพื่อยกระดับการให้บริการประชาชนและการบริหารงานภาครัฐให้มีความสะดวก รวดเร็ว และโปร่งใส จังหวัดสุรินทร์ได้ขานรับนโยบายดังกล่าวโดยการพัฒนาโครงสร้างพื้นฐานดิจิทัลและแพลตฟอร์มบูรณาการข้อมูลต่าง ๆ อาทิ ระบบ Surin One-Plan, แพลตฟอร์มแก้จนชี้เป้า (Surin Poverty Database) และระบบเฝ้าระวังภัยพิบัติอัจฉริยะ ซึ่งส่งผลให้การดำเนินงานของส่วนราชการภายในจังหวัดมีความเชื่อมโยงกันอย่างเป็นระบบและมีประสิทธิภาพสูงขึ้นอย่างก้าวกระโดด

การเปลี่ยนผ่านสู่ความดิจิทัลที่รวดเร็วได้ก่อให้เกิดความท้าทายใหม่ในด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ข้อมูลสถิติและฐานข้อมูลสำคัญของจังหวัดกลายเป็นเป้าหมายของการโจมตีทางไซเบอร์ที่มีความซับซ้อนและหลากหลายรูปแบบ ไม่ว่าจะเป็นการใช้มัลแวร์เรียกค่าไถ่ การเจาะระบบเพื่อขโมยข้อมูลอัตลักษณ์บุคคล หรือการจารกรรมข้อมูลทางยุทธวิธีบริเวณชายแดน ดังนั้นการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) จึงเป็นเรื่องจำเป็นที่ทุกองค์กรต้องให้ความสำคัญเป็นอันดับต้น

ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ในบริบทของแผนปฏิบัติการฉบับนี้ หมายถึง กระบวนการหรือการกระทำทั้งหมดที่จำเป็นจะต้องดำเนินการเพื่อทำให้องค์กรปราศจากความเสี่ยงและความเสียหายที่มีผลต่อความปลอดภัยของระบบสารสนเทศ และข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่ออาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่างๆ โดยการดำเนินงานภายใต้แผนฉบับนี้ ได้ยึดถือและคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูลหรือ CIA ทั้ง 3 ประการ เป็นหัวใจสำคัญ ได้แก่

1. **การรักษาความลับของข้อมูล (Confidentiality)** เพื่อสร้างความมั่นใจว่าข้อมูลส่วนบุคคลของประชาชนและข้อมูลสำคัญทางราชการจะเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
2. **การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity)** เพื่อป้องกันการถูกแก้ไขหรือบิดเบือนข้อมูลจากผู้ไม่หวังดี ทำให้ข้อมูลสถิติและสารสนเทศของจังหวัดมีความถูกต้องแม่นยำและเชื่อถือได้
3. **ความพร้อมใช้งานของข้อมูล (Availability)** เพื่อให้ระบบบริการภาครัฐและฐานข้อมูลที่สำคัญพร้อมให้บริการแก่ประชาชนและเจ้าหน้าที่ผู้เกี่ยวข้องได้ตลอดเวลา แม้ในช่วงที่เกิดสภาวะวิกฤตหรือการถูกโจมตีทางไซเบอร์

นอกจากความจำเป็นในเชิงเทคนิคแล้ว จังหวัดสุรินทร์ยังมีภาระหน้าที่ในการปฏิบัติตามกฎหมายสำคัญที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งกำหนดให้หน่วยงานภาครัฐต้องมีมาตรการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ที่ได้มาตรฐาน มีธรรมาภิบาลข้อมูล (Data Governance) และมีการประเมินความเสี่ยงอย่างต่อเนื่อง

ดังนั้น แผนปฏิบัติการความมั่นคงปลอดภัยไซเบอร์จังหวัดสุรินทร์ พ.ศ. 2569 - 2570 จึงถูกจัดทำขึ้นเพื่อมุ่งเน้นการบูรณาการกำลังพล เทคโนโลยี และกระบวนการทำงานเข้าด้วยกัน เพื่อสร้างเกราะป้องกันทางดิจิทัลที่เข้มแข็ง ส่งเสริมให้บุคลากรมีความรู้เท่าทันต่อภัยคุกคาม และเพื่อให้จังหวัดสุรินทร์สามารถขับเคลื่อนการพัฒนาเป็นเมืองอัจฉริยะ (Smart City) ได้อย่างมั่นคง ปลอดภัย และยั่งยืนบนฐานรากของความปลอดภัยสารสนเทศที่สมบูรณ์สืบไป

วัตถุประสงค์

1. เพื่อสร้างระบบนิเวศดิจิทัลที่มีความมั่นคงปลอดภัยและยืดหยุ่น (Cyber Resilience) มุ่งเน้นการพัฒนาระบบป้องกันและรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานภาครัฐภายในจังหวัด ให้มีความพร้อมตามมาตรฐานสากลและหลักการ CIA (Confidentiality, Integrity, Availability) เพื่อปกป้องฐานข้อมูลสำคัญและระบบบริการประชาชนให้สามารถทำงานได้อย่างต่อเนื่องและมั่นคง

2. เพื่อยกระดับธรรมาภิบาลข้อมูลและการปฏิบัติตามกฎหมาย มุ่งเน้นการจัดทำแนวทางและมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เพื่อสร้างความเชื่อมั่นให้กับประชาชนในการเข้าถึงและใช้บริการข้อมูลดิจิทัลของจังหวัด

3. เพื่อเสริมสร้างความตระหนักรู้และสมรรถนะด้านไซเบอร์ให้กับบุคลากร มุ่งเน้นการพัฒนาทักษะและความเข้าใจ (Cyber Literacy) ให้กับเจ้าหน้าที่รัฐในทุกระดับ เพื่อให้มีความรู้เท่าทันต่อรูปแบบภัยคุกคามสมัยใหม่ สามารถป้องกันความผิดพลาดจากปัจจัยบุคคล (Human Error) และเป็นกำลังสำคัญในการขับเคลื่อนจังหวัดสู่การเป็นเมืองอัจฉริยะ (Smart City) ที่ปลอดภัย

เพื่อให้แผนปฏิบัติการฯ มีความชัดเจนและเป็นไปตามมาตรฐานสากล ส่วน "นิยามและคำจำกัดความที่สำคัญ" ควรครอบคลุมทั้งคำศัพท์ทางเทคนิคและคำศัพท์เฉพาะที่เกี่ยวข้องกับบริบทของจังหวัด ดังนี้

นิยามและคำจำกัดความที่สำคัญ

เพื่อให้เกิดความเข้าใจที่ตรงกันในการนำแผนปฏิบัติการฉบับนี้ไปสู่การปฏิบัติ จึงกำหนดนิยามและคำจำกัดความที่สำคัญไว้ดังนี้

- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารงานของจังหวัดสุรินทร์
- **ผู้บริหาร (Chief Executive Officer : CEO)** หมายถึง ผู้บังคับบัญชาสูงสุดของจังหวัดสุรินทร์ ซึ่งมีบทบาท หน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย กำหนดทิศทางรวมทั้งมอบหมายงานให้ผู้ปฏิบัติที่เกี่ยวข้อง กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์ใช้งานไม่ได้ ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใดๆ

• **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)** หมายถึง ผู้บังคับบัญชาสูงสุดในด้านเทคโนโลยีสารสนเทศของจังหวัดสุรินทร์

• **ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)** มาตรการและการดำเนินการทั้งหมดที่ออกแบบมาเพื่อปกป้องระบบคอมพิวเตอร์ เครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึงที่ไม่ได้รับอนุญาต การโจมตี การทำให้เสียหาย หรือการจารกรรม เพื่อให้ระบบสารสนเทศทำงานได้อย่างต่อเนื่องและปลอดภัย

• **ภัยคุกคามทางไซเบอร์ (Cyber Threat)** การกระทำหรือเหตุการณ์ที่มีเจตนาร้ายหรือเหตุอันไม่พึงประสงค์ ที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศ ข้อมูล หรือโครงสร้างพื้นฐานดิจิทัล รวมถึงการใช้มัลแวร์ (Malware) การหลอกลวงออนไลน์ (Phishing) และการโจมตีเพื่อปฏิเสธการให้บริการ (DDoS)

• **ระบบสารสนเทศที่สำคัญ (Critical Information System)** ระบบคอมพิวเตอร์หรือฐานข้อมูลที่มีความสำคัญต่อภารกิจหลักของหน่วยงานราชการในจังหวัดสุรินทร์ ซึ่งหากถูกแทรกแซงหรือหยุดชะงักจะส่งผลกระทบต่อความมั่นคง การบริการประชาชน หรือความสงบเรียบร้อย เช่น ระบบ Surin One-Plan และฐานข้อมูลสถิติที่สำคัญ

• **ธรรมาภิบาลข้อมูล (Data Governance)** กรอบการบริหารจัดการข้อมูลให้มีคุณภาพ ถูกต้อง ปลอดภัย และเป็นไปตามกฎหมาย เพื่อให้การใช้ข้อมูลเป็นไปอย่างมีประสิทธิภาพและโปร่งใส

• **การรักษาความลับ (Confidentiality)** การรับประกันว่าข้อมูลจะถูกเข้าถึงและเปิดเผยเฉพาะผู้ที่มีสิทธิได้รับอนุญาตเท่านั้น เพื่อป้องกันการรั่วไหลของข้อมูลอ่อนไหวหรือข้อมูลส่วนบุคคล (PDPA)

• **การรักษาความคงสภาพ (Integrity)** การรับประกันว่าข้อมูลและระบบจะไม่ถูกแก้ไข เปลี่ยนแปลง หรือบิดเบือนโดยไม่ได้รับอนุญาต เพื่อให้ข้อมูลมีความถูกต้องสมบูรณ์และเชื่อถือได้

• **ความพร้อมใช้งาน (Availability)** ความสามารถของระบบและข้อมูลที่จะถูกเรียกใช้งานได้ทันทีเมื่อมีความต้องการ โดยเฉพาะในช่วงสถานการณ์วิกฤตหรือสถานการณ์ภัยพิบัติ

• **การตอบสนองต่อเหตุการณ์ (Incident Response)** กระบวนการตรวจจับ วิเคราะห์ และดำเนินการแก้ไขเมื่อเกิดเหตุการณ์คุกคามทางไซเบอร์ เพื่อจำกัดความเสียหายและทำให้ระบบกลับมาทำงานเป็นปกติโดยเร็วที่สุด

• **ความเป็นส่วนตัวของข้อมูล (Data Privacy)** สิทธิและมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนจากการถูกจัดเก็บ ประมวลผล หรือเผยแพร่โดยปราศจากฐานอำนาจทางกฎหมายหรือการยินยอม

• **ขั้นตอนการปฏิบัติ** (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ อย่างชัดเจน ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

• **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่แนะนำให้ปฏิบัติตามเพื่อให้บรรลุเป้าหมายได้ง่ายสะดวกขึ้น

• **บัญชีผู้ใช้งาน** หมายถึง บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของจังหวัดฯ

• **รหัสผ่าน หมายถึง** ตัวอักษร อักขระ ตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

• **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหารจัดการหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของจังหวัดฯ ตามสิทธิและหน้าที่ ขึ้นอยู่กับบทบาท (Role) ที่จังหวัดฯ กำหนดไว้ ดังนี้

(1) ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของจังหวัดฯ เช่น ผู้ว่าราชการจังหวัด รองผู้ว่าราชการจังหวัด เป็นต้น

(2) ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ซึ่งได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์ เพื่อการบริหารจัดการระบบได้

(3) ผู้ใช้งาน (User) หมายถึง เจ้าหน้าที่และบุคลากรของจังหวัดฯ ที่มีสิทธิในการเข้าใช้งานระบบสารสนเทศของจังหวัดฯ

บทที่ 2
นโยบาย แผน กฎหมาย กฎระเบียบที่เกี่ยวข้อง และมาตรฐานความปลอดภัย

ความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้นมีความสำคัญเป็นอย่างมาก เนื่องจากปัญหาภัยคุกคามทางไซเบอร์นั้น ส่งผลกระทบต่อทั้งหน่วยงานภาครัฐ ภาคเอกชน องค์กรทุกภาคส่วนที่มีการนำระบบสารสนเทศมาประยุกต์ใช้ ต้องตระหนักถึงความมั่นคงปลอดภัย เพื่อช่วยปกป้องระบบคอมพิวเตอร์ รวมไปถึงอุปกรณ์ต่างๆ ที่เกี่ยวข้อง และที่สำคัญยังสามารถช่วยปกป้องข้อมูลสำคัญที่ได้จัดเก็บไว้ภายในระบบสารสนเทศอีกด้วย

จุดประสงค์ของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ

จุดประสงค์หลักของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ คือ ความลับ (Confidentiality) ความสมบูรณ์ (Integrity)ความพร้อมใช้ (Availability) และการห้ามปฏิเสธความรับผิดชอบ (Non–repudiation) ของข้อมูลต่างๆ ภายในองค์กร โดยมีรายละเอียด ดังนี้

1) การรักษาความลับ (Confidentiality) คือ การรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ ทำให้มั่นใจว่ามีเฉพาะผู้มีสิทธิหรือได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้

2) การรักษาความสมบูรณ์ (Integrity) คือ การรับรองว่าข้อมูลที่ปกป้องนั้นต้องมีความถูกต้องสมบูรณ์ จะไม่ถูกแก้ไข เปลี่ยนแปลง หรือทำลาย จากผู้ไม่มีสิทธิไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา

3) ความพร้อมใช้ (Availability) คือ การรับรองว่าข้อมูลและบริการการสื่อสารต่างๆ พร้อมใช้งาน สามารถตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิเข้าถึงระบบได้เมื่อต้องการ

4)การห้ามปฏิเสธความรับผิดชอบ (Non–repudiation) คือ วิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่า ได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธ ได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

1. นโยบายความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Policy)

นโยบายคือเข็มทิศหลักที่ใช้ในการปฏิบัติงาน เพื่อให้ทุกหน่วยงานในจังหวัดสุรินทร์มีแนวปฏิบัติเป็นไปในทิศทางเดียวกัน ดังนี้

นโยบายการป้องกันเชิงรุก (Proactive Defense Policy) กำหนดให้หน่วยงานราชการต้องให้ความสำคัญกับการป้องกันก่อนเกิดเหตุ โดยมีการตรวจสอบช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) อย่างน้อยปีละ 1 ครั้ง

นโยบายการรักษาความปลอดภัยข้อมูลประชาชน มุ่งเน้นการปกป้องข้อมูลส่วนบุคคลในโครงการหลักของจังหวัด เช่น ฐานข้อมูลแก้จนชี้เป้า และ Surin One-Plan โดยต้องมีการเข้าถึงข้อมูลตามลำดับสิทธิ์ (Principle of Least Privilege)

นโยบายการตอบสนองต่อเหตุการณ์วิกฤต กำหนดให้มีช่องทางการรายงานเหตุภัยคุกคามไซเบอร์ที่ชัดเจนและมีคณะทำงานตอบโต้เหตุการณ์ฉุกเฉิน (Cyber Incident Response Team: CIRT) ประจำจังหวัด

นโยบายการสร้างความตระหนักรู้ เจ้าหน้าที่รัฐทุกคนต้องผ่านการอบรมพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อลดความเสี่ยงจากการถูกหลอกลวงออนไลน์ (Phishing) และปัจจัยเสี่ยงจากบุคคล (Human Error)

2. กฎหมาย กฎระเบียบ และข้อกำหนดด้านเทคโนโลยีดิจิทัล

กฎหมายต่างๆ ที่จะสนับสนุนการพัฒนาดิจิทัลของประเทศ ได้มีการดำเนินการมาแล้วเป็นลำดับ กฎหมายเหล่านี้จะเป็นการให้ความมั่นใจและกำหนด กฎ กติกา การดำเนินการใช้ดิจิทัลอย่างปลอดภัย ยุติธรรม และตั้งอยู่บนพื้นฐานของความเท่าเทียมกัน โดยสรุปได้ดังนี้

1) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

หมวด 1 ธุรกรรมทางอิเล็กทรอนิกส์

(1) การรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ ในมาตรา 7 กล่าวว่า “ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใด เพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์” ซึ่งจะเห็นได้ว่าบทบัญญัตินี้เป็นหลักการพื้นฐานที่มิให้มีการเลือกปฏิบัติระหว่างสิ่งที่จัดทำขึ้นในรูปของหนังสือ หลักฐานเป็นหนังสือ หรือต้นฉบับ (Original) กับสิ่งที่จัดทำขึ้นในรูปของ ข้อมูลอิเล็กทรอนิกส์

(2) การทำเป็นหนังสือ มาตรา 8 บัญญัติไว้ว่า “ภายใต้บังคับบทบัญญัติแห่งมาตรา 9 ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือมีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว” ซึ่งกล่าวได้ว่า มาตรา 8 เป็นการบัญญัติเพื่อขยายหลักการรับรองสถานะของข้อมูลอิเล็กทรอนิกส์ในมาตรา 7

(3) การลงลายมือชื่อ หลักการนี้ปรากฏอยู่ในมาตรา 9 ซึ่งสรุปได้ว่าในกรณีที่บุคคลลงลายมือชื่อในหนังสือให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้าบุคคลนั้นใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อได้ และสามารถจะแสดงได้ว่า เจ้าของลายมือชื่อนั้น รับรองข้อความในข้อมูล อิเล็กทรอนิกส์ ว่าเป็นของตน โดยวิธีดังกล่าว จะต้องเป็นวิธีการที่เชื่อถือได้ โดยเหมาะสมกับวัตถุประสงค์ของการสร้าง หรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

4) ต้นฉบับหลักการนี้ปรากฏอยู่ในมาตรา 10 กล่าวโดยสรุปได้ว่า ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความหรือเอกสารที่เป็นต้นฉบับ หากได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์นั้นโดยวิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความนั้น ตั้งแต่การ สร้างข้อความจนถึงข้อความที่เสร็จสมบูรณ์ และสามารถแสดงข้อความนั้นในภายหลังได้ ก็ให้ถือว่าได้มีการนำเสนอข้อความหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

5) การรับฟังพยานหลักฐานและชั่งน้ำหนักพยานหลักฐานปรากฏอยู่ในมาตรา 11 บทบัญญัติในมาตรานี้ เป็นการห้ามปฏิเสธการรับฟังพยานหลักฐานในกระบวนพิจารณาด้วยเหตุที่ข้อมูลนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ แต่ทั้งนี้ในเรื่องของการรับฟัง พยานหลักฐาน เป็นดุลยพินิจของศาลที่จะรับฟังหรือไม่ก็ได้ กฎหมายจึงต้องกำหนดหลักเกณฑ์ในการชั่งน้ำหนักพยานหลักฐานไว้ โดยให้พิจารณาถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้างการเก็บรักษาหรือการสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการในการระบุตัวผู้ส่งรวมถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง

6) การเก็บรักษาเอกสารหรือข้อความปรากฏอยู่ในมาตรา 12 โดยหลักการนี้ให้ความสำคัญว่า ข้อความหรือข้อมูลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้นต้องตรงกับเนื้อหาของข้อความหรือข้อมูลของเอกสารก่อนที่จะมีการจัดเก็บให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้น

ด้านหลักการต่างๆ ที่ปรากฏอยู่ในมาตรา 13 ถึงมาตรา 24 อันได้แก่ หลักการว่าด้วยเรื่อง การทำคำเสนอหรือคำสนองในรูปข้อมูลอิเล็กทรอนิกส์ เจ้าของข้อมูลอิเล็กทรอนิกส์ วิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ เวลาและสถานที่ซึ่งถือว่าได้มีการส่งหรือรับข้อมูลอิเล็กทรอนิกส์นั้น เป็นบทบัญญัติซึ่งคู่กรณีสามารถตกลงเปลี่ยนแปลงเป็นอย่างอื่นได้ นอกจากนั้นยังมีการบัญญัติหลักการเรื่อง วิธีการแบบปลอดภัย ไว้ในมาตรา 25 ซึ่งบัญญัติขึ้นเพื่อให้กฎหมายมีความยืดหยุ่นในการปรับใช้กับเทคโนโลยีต่างๆ ที่มีอยู่ในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต แต่กฎหมายไม่ได้บัญญัติรายละเอียดถึงวิธีการที่จะถือว่าเป็นวิธีการที่เชื่อถือได้ จึงเป็นหน้าที่ของผู้ใช้เทคโนโลยีที่จะต้องพิจารณาว่า วิธีการใดที่จะถือว่าเป็นวิธีการที่ปลอดภัย รวมทั้งผู้ใช้ยังต้องมีหน้าที่ในการพิสูจน์ด้วยว่าเพราะเหตุใดวิธีการดังกล่าวจึงเป็นวิธีการที่น่าเชื่อถือตามกฎหมาย

2) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551

สาระสำคัญของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 เฉพาะในส่วนที่เกี่ยวข้อง มีดังนี้

(1) มาตรา 3 ให้เพิ่มความต่อไปนี้เป็นวรรคสองของมาตรา 8 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 “ในกรณีที่กฎหมายกำหนดให้ต้องมีการปิดอากรแสตมป์หากได้มีการชำระเงินแทนหรือดำเนินการอื่นใดด้วยวิธีการทำงอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่หน่วยงานของรัฐซึ่งเกี่ยวข้อง ประกาศกำหนดให้ถือว่าหนังสือหลักฐานเป็นหนังสือหรือเอกสารซึ่งมีลักษณะเป็นตราสารนั้น ได้มีการปิดอากรแสตมป์และขีดฆ่าตามกฎหมายนั้นแล้ว ในการนี้ในการกำหนดหลักเกณฑ์และวิธีการของหน่วยงานของรัฐดังกล่าว คณะกรรมการจะกำหนดกรอบและแนวทางเพื่อเป็นมาตรฐานทั่วไปไว้ด้วยก็ได้”

(2) มาตรา 4 ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา 9 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 “วิธีการที่เชื่อถือได้ตาม (2) ให้คำนึงถึงความมั่นคงและรัดกุม ของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคล สภาพพร้อมใช้งานของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์ เกี่ยวกับลายมือชื่อ ที่กำหนดไว้ในกฎหมาย ระดับความมั่นคงปลอดภัย ของการใช้ลายมือชื่ออิเล็กทรอนิกส์ การปฏิบัติ ตามกระบวนการในการระบุตัวบุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับ วิธีการที่ใช้ในการระบุ ตัวบุคคลในการทำธุรกรรม วิธีการระบุตัวบุคคล

ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

(3) มาตรา 5 ให้เพิ่มความต่อไปนี้เป็นวรรคสี่ของมาตรา 10 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 กรณีที่มีการทำสิ่งพิมพ์ ออกของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่ง สำหรับใช้อ้างอิงข้อความ ของข้อมูลอิเล็กทรอนิกส์ หากสิ่งพิมพ์ออกนั้น มีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์และมีการรับรองสิ่งพิมพ์ ซึ่งถูกออกโดยหน่วยงานที่มีอำนาจ หน้าที่ตามที่คณะกรรมการประกาศกำหนดแล้ว ให้ถือว่าสิ่งพิมพ์ออกดังกล่าวใช้แทนต้นฉบับได้”

(4) มาตรา 6 ให้ยกเลิกความในมาตรา 11 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และให้ใช้ความต่อไปนี้แทน “มาตรา 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมาย ทั้งในคดีแพ่งคดีอาญาหรือคดีอื่นใด เพียงเพราะเหตุว่า เป็นข้อมูลอิเล็กทรอนิกส์ ในการชั่งน้ำหนัก พยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์ จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึง ความน่าเชื่อถือ ของลักษณะหรือวิธีการที่ใช้สร้างเก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะ หรือวิธีการเก็บรักษาความครบถ้วนและไม่มีการเปลี่ยนแปลง ของข้อความลักษณะ หรือวิธีการที่ใช้ ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้อง ทั้งปวงให้นาความในวรรคหนึ่งมาใช้บังคับ กับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย”

(3) พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

สาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ในส่วนที่เกี่ยวข้อง มีดังนี้

ภาพรวมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แบ่งเป็น การกระทำความผิดต่อระบบ การกระทำความผิดต่อข้อมูล การกระทำความผิด ของผู้ให้บริการ และการกระทำความผิดของพนักงานเจ้าหน้าที่ ซึ่งมีโทษ จำคุก ปรับ หรือทั้งจำทั้งปรับ ประกอบด้วย

(3.1) ระบบ
- เข้าถึงระบบของผู้อื่น โดยไม่ได้รับอนุญาต
- เผยแพร่ข้อมูล โดยไม่ได้รับอนุญาต
- ระงับ/ขัดขวาง/รบกวน ทำให้ระบบทำงานไม่ได้

(3.2) ข้อมูล
- เข้าถึง ดักจับ/ทำงาน/แก้ไข/ปลอมแปลง ข้อมูล โดยไม่ได้รับอนุญาต
- นำเข้า/ส่งต่อ ข้อมูลปลอม/ข้อมูลเท็จ/ข้อมูลที่กระทบความมั่นคงของชาติ
- ระงับ/ขัดขวาง/รบกวน ทำให้ระบบทำงานไม่ได้

(4) พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549

การที่ประเทศไทยได้เข้าสู่ยุคสมัยสังคมสารสนเทศ ซึ่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น จึงมีการสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตน โดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับ ให้หน่วยงานของรัฐ สามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทำงอิเล็กทรอนิกส์ ประกอบกับมาตรา 35 วรรค 1 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 บัญญัติว่า คำขอการอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐถ้าได้กระทำ ในรูปของ ข้อมูล อิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาแล้ว ให้ถือว่ามีผลโดยชอบ ด้วยกฎหมาย เช่นเดียวกับการดำเนินการ ตามหลักเกณฑ์ และวิธีการที่กฎหมายในเรื่องนั้นกำหนด จึงจำเป็นต้องตราพระราชกฤษฎีกากำหนด หลักเกณฑ์และวิธีการ ทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 โดยมีสาระสำคัญ ดังนี้

(4.1) ให้หน่วยงานรัฐต้องจัดให้มีระบบเอกสารในรูปแบบอิเล็กทรอนิกส์ ในมาตรา 3 ได้กำหนดให้การทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ หน่วยงานของรัฐ จะต้องจัดให้มี ระบบเอกสารที่ทำในรูปแบบอิเล็กทรอนิกส์ โดยมีลักษณะดังต่อไปนี้

(4.1.1) เอกสารที่จัดทำในรูปของข้อมูล อิเล็กทรอนิกส์นั้นต้องอยู่ในรูปแบบที่เหมาะสม โดยสามารถ แสดงหรืออ้างอิง เพื่อใช้ในภายหลัง และยังคงความครบถ้วน ของข้อความ ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

(4.1.2) ต้องกำหนดระยะเวลาเริ่มต้นและสิ้นสุดในการยื่นเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์โดยปกติให้ยึดถือวันเวลาของการปฏิบัติงานหน่วยงานของรัฐนั้นเป็นหลัก และอาจกำหนดระยะเวลาในการดำเนินการพิจารณา ของหน่วยงานของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ไว้ด้วยก็ได้เว้นแต่ จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(4.1.3) ต้องกำหนดวิธีการที่ทำให้สามารถระบุตัวเจ้าของลายมือชื่อ ประเภทลักษณะ หรือรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ และสามารถแสดงได้ว่า เจ้าของลายมือชื่อได้รับรองข้อความในข้อมูล อิเล็กทรอนิกส์

(4.1.4) ต้องกำหนดวิธีการแจ้งการตอบรับด้วยวิธีการทางอิเล็กทรอนิกส์หรือด้วยวิธีการอื่นใด เพื่อเป็นหลักฐานว่า ได้มีการดำเนินการด้วย วิธีการทางอิเล็กทรอนิกส์ ไปยังอีกฝ่ายหนึ่งแล้ว

(4.2) ให้มีระบบเอกสารในรูปแบบอิเล็กทรอนิกส์ในการพิจารณาคดีทางปกครองโดยวิธีการทางอิเล็กทรอนิกส์ของรัฐตามบทบัญญัติแห่งมาตรา 4 นอกจากที่บัญญัติไว้ในมาตรา 3 ในกรณีที่หน่วยงานของรัฐจัดทำกระบวนการพิจารณาทางปกครองโดยวิธีการทางอิเล็กทรอนิกส์ ระบบเอกสารที่ทำ

ในรูป ของข้อมูลอิเล็กทรอนิกส์ต้องมีลักษณะดังต่อไปนี้ด้วย เว้นแต่จะมีกฎหมาย ในเรื่องนั้น กำหนดไว้เป็นอย่างอื่น

(4.2.1) มีวิธีการสื่อสารกับผู้ยื่นคำขอในกรณีที่เอกสารมีข้อบกพร่องหรือมีข้อความ ที่ผิดหลง อันเห็นได้ชัดว่าเกิดจาก ความไม่รู้หรือความเลินเล่อ ของผู้ยื่นคำขอหรือการขอ ข้อเท็จจริงเพิ่มเติม รวมทั้งมีวิธีการแจ้งสิทธิและหน้าที่ในกระบวนการพิจารณาทางปกครอง ตามความจำเป็นแก่กรณีในกรณีที่กฎหมายกำหนดให้ต้องแจ้งให้คู่กรณีทราบ

(4.2.2) ในกรณีที่มีความจำเป็นตามลักษณะเฉพาะของธุรกรรมทาง อิเล็กทรอนิกส์ภาครัฐใด หน่วยงานของรัฐนั้นอาจกำหนดเงื่อนไขว่า คู่กรณียินยอม ตกลงและยอมรับการดำเนินการพิจารณาทางปกครองของหน่วยงานของรัฐโดยวิธีการทางอิเล็กทรอนิกส์

(4.3) ให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศจากบทบัญญัติในมาตรา 5 พระราชกฤษฎีกา ธุรกรรมอิเล็กทรอนิกส์ภาครัฐฯ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติ ในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ ซึ่งแนวนโยบาย และแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(4.3.1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(4.3.2) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(4.3.3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

(4.4) ให้หน่วยงานภาครัฐจัดทำนโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ในมาตรา 6 ในกรณีที่มี การรวบรวมจัดเก็บ ใช้หรือเผยแพร่ข้อมูล หรือข้อเท็จจริง ที่ทำให้สามารถระบุ ตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐ จัดทำแนวนโยบาย และแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

(4.5) ให้หน่วยงานของรัฐจัดทำประกาศ นโยบายและแนวปฏิบัติ ในการ รักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ และนโยบายและแนวทางปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคล ในมาตรา 7 แนวนโยบายและแนวปฏิบัติตามมาตรา 5 และมาตรา 6 ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการ หรือหน่วยงาน ที่คณะกรรมการมอบหมายจึงมีผลใช้บังคับได้ โดยหน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้และจัดให้มีการตรวจสอบ การปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

(4.6) ให้คณะกรรมการจัดทำตัวอย่างเบื้องต้น สำหรับการดำเนินการของหน่วยงานของรัฐให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้น สำหรับ การดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐ แห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้น อาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ

สภาพความพร้อมใช้งาน และความมั่นคง ปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

(4.7) การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐตามหลักเกณฑ์และวิธีการตามพระราชกฤษฎีกานี้ ไม่มีข้อยกเว้นในมาตรา 9 การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐตามหลักเกณฑ์และวิธีการตามพระราชกฤษฎีกานี้ ไม่มีผลเป็นการยกเว้น กฎหมายหรือหลักเกณฑ์ และวิธีการ ที่กฎหมายในเรื่องนั้นกำหนดไว้เพื่อการอนุญาต อนุมัติ การให้ความเห็นชอบ หรือการวินิจฉัย

(5) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. 2553 และที่แก้ไขเพิ่มเติม

ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้มีการกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ เพื่อให้หน่วยงานภาครัฐมีการดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ และมีระบบรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ และเชื่อถือได้ ตลอดจน มีมาตรฐาน เป็นที่ยอมรับ ในระดับสากล มีสาระสำคัญ ดังนี้

(5.1) หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

(5.2) หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงาน

(5.3) ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย โดยต้องมีข้อปฏิบัติ ดังนี้

(5.3.1) มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ

(5.3.2) ข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ

(5.3.3) ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เฉพาะผู้ที่ ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตร การสร้างความตระหนักเรื่องความมั่นคง ปลอดภัยสารสนเทศเพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

(5.3.4) ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตการเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

(5.3.5) ให้มีการควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่าย โดยไม่ได้รับอนุญาต

(5.3.6) ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

(5.3.7) ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

(5.3.8) หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง

(5.3.9) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยง ด้านสารสนเทศ

(5.3.10) หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด

(5.3.11) หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง

(5.3.12) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(5.3.13) หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่า ข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า

ตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม พ.ศ. 2551 สาระสำคัญเพื่อรับรองสถานะทางกฎหมาย ของข้อมูลอิเล็กทรอนิกส์ ที่ใช้ในการทำธุรกรรม หรือสัญญาให้มีผลเช่นเดียวกับการทำสัญญาตามหลักเกณฑ์ที่กฎหมายปัจจุบัน (ประมวลกฎหมายแพ่ง และพาณิชย์) กำหนดไว้ ได้แก่ การทำเป็นหนังสือ หลักฐานเป็นหนังสือ การลงลายมือชื่อ กล่าวคือ ถ้ามีการทำสัญญาระหว่างบุคคล ที่ใช้ข้อมูลอิเล็กทรอนิกส์ หรือลายมือชื่ออิเล็กทรอนิกส์ ตามความหมายของกฎหมายแล้วกฎหมายนี้ถือว่า การทำสัญญานั้นได้ทำตามหลักเกณฑ์ ข้างต้นของกฎหมายแพ่งและพาณิชย์แล้ว เป็นผลทำให้สัญญานั้นมีผลสมบูรณ์ หรือใช้บังคับได้ตามกฎหมาย ทั้งนี้ เป็นไปตามเงื่อนไขที่กฎหมาย ธุรกรรมทางอิเล็กทรอนิกส์กำหนด นอกจากนี้ ในมาตรา 12/1 วรรค 2 กำหนดให้การจัดทำแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูล อิเล็กทรอนิกส์ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด ดังนั้น คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศ เรื่อง “หลักเกณฑ์และวิธีการในการจัดทำ หรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553” โดยมีวัตถุประสงค์ เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ และมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิมโดยมีสาระสำคัญ ดังนี้

1) ให้มีการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูล อิเล็กทรอนิกส์ ให้มีกระบวนการในการจัดทำหรือแปลงเอกสารและข้อความอย่างน้อย ดังนี้

1.1) กระบวนการจัดทำหรือแปลงเอกสารและข้อความให้เป็นข้อมูล อิเล็กทรอนิกส์ด้วยวิธีการทางอิเล็กทรอนิกส์

1.2) กระบวนการตรวจสอบและรับรองว่าข้อมูลอิเล็กทรอนิกส์ที่จัดทำหรือแปลงมานั้นมีความหมายเหมือนกับเอกสารและข้อความเดิม

1.3) กระบวนการบันทึกหลักฐานการดำเนินงานการจัดทำหรือแปลงเอกสาร และข้อความ ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

1.4) กระบวนการบันทึกเมตาดาตาในรูปแบบอิเล็กทรอนิกส์ที่เป็นข้อความบรรยายสาระสำคัญของเอกสารและข้อความซึ่งต้องครอบคลุมให้สามารถสืบค้นเอกสาร และข้อความนั้นได้ถูกต้อง

2) การจัดทำหรือแปลงเอกสารและข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ ให้มีผู้รับผิดชอบดำเนินงานในการจัดทำหรือแปลงในเรื่องของวิธีการดังกล่าว อย่างน้อยดังต่อไปนี้

2.1) จัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

2.2) ตรวจสอบและรับรองความถูกต้องและครบถ้วนของข้อมูลอิเล็กทรอนิกส์ที่ได้จากการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ว่าข้อมูลอิเล็กทรอนิกส์ มีความหมาย หรือรูปแบบเหมือนกับเอกสารและข้อความเดิม

2.3) ตรวจสอบกระบวนการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ให้เป็นไปตามที่กำหนดไว้

2.4) ตรวจสอบและรับรองความถูกต้องและครบถ้วนของเมตาดาต้า

3) การจัดทำหรือแปลงเอกสารและข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีการกำหนดมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นวิธีการที่เชื่อถือได้ อย่างน้อยต้องครอบคลุมหัวข้อต่อไปนี้

3.1) การระบุตัวตน (Identification)

3.2) การยืนยันตัวตน (Authentication)

3.3) อนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization)

3.4) ความรับผิดชอบต่อผลของการกระทำ (Accountability)

4) การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูล อิเล็กทรอนิกส์นั้นให้ข้อมูลอิเล็กทรอนิกส์มีความละเอียดและความชัดเจนของเอกสาร และข้อความเดิม ให้ผู้จัดทำหรือแปลง มีหน้าที่รักษาและดำรงสภาพของระบบการจัดทำหรือแปลงเอกสารไว้ให้สมบูรณ์ เพื่อให้มีการกำกับดูแล หรือการตรวจสอบได้ตลอดเวลา จากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ หรือหน่วยงานอื่นที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ มอบหมายหรือหน่วยงานที่กำหนดไว้เป็นอย่างอื่น

(6) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำ หรือแปลงเอกสารและข้อความให้อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553

ตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม พ.ศ. 2551 มีสาระสำคัญเพื่อรับรองสถานะทางกฎหมาย ของข้อมูลอิเล็กทรอนิกส์ ที่ใช้ในการทำธุรกรรม หรือสัญญาให้มีผลเช่นเดียวกับการทำสัญญาตามหลักเกณฑ์ที่กฎหมายปัจจุบันคือ ประมวลกฎหมายแพ่งและพาณิชย์กำหนดไว้ได้แก่การทำเป็นหนังสือ หลักฐานเป็นหนังสือ การลงลายมือชื่อ กล่าวคือถ้ามีการทำสัญญา ระหว่างบุคคล ที่ใช้ข้อมูล อิเล็กทรอนิกส์ หรือลายมือชื่อ อิเล็กทรอนิกส์ ตามความหมายของกฎหมายแล้ว กฎหมายนี้ถือว่า การทำสัญญานั้นได้ทำตามหลักเกณฑ์ข้างต้น ของกฎหมายแพ่งและพาณิชย์แล้ว เป็นผลทำให้สัญญานั้นมีผลสมบูรณ์ หรือใช้บังคับได้ตามกฎหมาย ทั้งนี้เป็นไปตามเงื่อนไขที่กฎหมายธุรกรรมทางอิเล็กทรอนิกส์กำหนด นอกจากนี้ ในมาตรา 12/1 วรรค 2 กำหนดให้การจัดทำแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูล อิเล็กทรอนิกส์ ให้เป็นไปตามหลักเกณฑ์ และวิธีการที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด ดังนั้น คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศ เรื่อง “หลักเกณฑ์และวิธีการในการจัดทำ หรือแปลงเอกสาร และข้อความให้อยู่ในรูปของ

ข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553” โดยมีวัตถุประสงค์ เพื่อเป็นการส่งเสริม การทำธุรกรรมทางอิเล็กทรอนิกส์ ให้น่าเชื่อถือและมีผลในทางกฎหมายเช่นเดียวกับ การทำธุรกรรมโดยวิธีการทั่วไป ที่เคยปฏิบัติอยู่เดิม โดยมีสาระสำคัญ ดังนี้

(6.1) ให้มีการจัดทำหรือแปลงเอกสารและข้อความ ให้อยู่ในรูปของข้อมูล อิเล็กทรอนิกส์ ให้มีกระบวนการในการจัดทำหรือแปลงเอกสารและข้อความอย่างน้อย ดังนี้

(6.1.1) กระบวนการจัดทำหรือแปลงเอกสารและข้อความให้เป็นข้อมูลอิเล็กทรอนิกส์ ด้วยวิธีการทางอิเล็กทรอนิกส

(6.1.2) กระบวนการตรวจสอบและรับรองว่าข้อมูลอิเล็กทรอนิกส์ ที่จัดทำหรือแปลงนั้นมีความหมายเหมือนกับเอกสารและข้อความเดิม

(6.1.3) กระบวนการบันทึกหลักฐานการดำเนินงานการจัดทำหรือแปลงเอกสาร และข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

(6.1.4) กระบวนการบันทึกเมตาดาตาในรูปแบบอิเล็กทรอนิกส์ ที่เป็นข้อความบรรยายสาระสำคัญของเอกสารและข้อความซึ่งต้องครอบคลุมให้สามารถสืบค้นเอกสารและข้อความนั้นได้ถูกต้อง

(6.2) การจัดทำหรือแปลงเอกสารและข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ ให้มีผู้รับผิดชอบดำเนินงานในการจัดทำหรือแปลงในเรื่องของวิธีการดังกล่าว อย่างน้อยดังต่อไปนี้

(6.2.1) จัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

(6.2.2) ตรวจสอบและรับรองความถูกต้องและครบถ้วนของข้อมูลอิเล็กทรอนิกส์ที่ได้จากการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ว่าข้อมูลอิเล็กทรอนิกส์ มีความหมาย หรือรูปแบบเหมือนกับเอกสารและข้อความเดิม

(6.2.3) ตรวจสอบกระบวนการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ให้เป็นไปตามที่กำหนดไว้

(6.2.4) ตรวจสอบและรับรองความถูกต้องและครบถ้วนของเมตาดาต้า

(6.3) การจัดทำหรือแปลงเอกสารและข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ ให้มีการกำหนดมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นวิธีการที่เชื่อถือได้ อย่างน้อยต้องครอบคลุมหัวข้อต่อไปนี้

(6.3.1) การระบุตัวตน (Identification)

(6.3.2) การยืนยันตัวตน (Authentication)

(6.3.3) อนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization)

(6.3.4) ความรับผิดชอบต่อผลของการกระทำ (Accountability)

(6.4) การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้น ให้ข้อมูลอิเล็กทรอนิกส์มีความละเอียดและความชัดเจนของเอกสารและข้อความเดิม ให้ผู้จัดทำหรือแปลงมีหน้าที่รักษาและดำรงสภาพของระบบการจัดทำหรือแปลงเอกสารไว้ให้สมบูรณ์ เพื่อให้มีการกำกับดูแลหรือการตรวจสอบได้ตลอดเวลา จากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ หรือหน่วยงานอื่น

ที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมาย หรือหน่วยงานที่กำหนดไว้เป็นอย่างอื่น

(7) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

- **มาตรา 54** หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบ ภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง
- **มาตรา 57** เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานหรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ และสำนักงานหรือหน่วยงานต้องแจ้งเหตุไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยเร็วที่สุด
- **มาตรา 58** ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน

(8) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

- **มาตรา 37** หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (หน่วยงานราชการ) ต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง หรือเปิดเผยข้อมูลโดยมิชอบ
- **มาตรา 39** ต้องมีบันทึกรายการ (Record of Processing) เพื่อให้เจ้าของข้อมูลหรือสำนักงานฯ ตรวจสอบได้

(9) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

- **มาตรา 26** ผู้ให้บริการ (ซึ่งรวมถึงส่วนราชการที่ให้บริการ Wi-Fi หรือระบบเครือข่าย) ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ไม่น้อยกว่า 90 วัน เพื่อใช้ในกรณีที่มีการสืบสวนหาผู้กระทำผิด

2.นโยบายและแผนที่เกี่ยวข้อง

นโยบายและแผนที่เกี่ยวข้อง ซึ่งได้ทำการศึกษาประกอบการจัดทำ ได้แก่

2.1 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และ (ฉบับที่ 2) พ.ศ. 2556 ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้มีการกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ เพื่อให้หน่วยงานภาครัฐ มีการดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ และมีระบบรักษาความมั่นคงปลอดภัยด้านสารสนเทศและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล มีสาระสำคัญ ดังนี้

2.1.1 หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษรดังนี้

2.1.2 หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

2.1.3 ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย โดยต้องมีข้อปฏิบัติ ดังนี้

(1) มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ

(2) มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ

(3) ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศเพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

(4) ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตการเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

2.2 แผนปฏิบัติการดิจิทัลจังหวัดสุรินทร์ พ.ศ. 2568 - 2570

ประกอบไปด้วยยุทธศาสตร์จำนวน 3 ข้อ ดังนี้

ยุทธศาสตร์ที่ ๑ บูรณาการระบบงานด้านสารสนเทศของจังหวัดสุรินทร์

กลยุทธ์ที่ ๑.๑) บูรณาการระบบงานด้านสารสนเทศข้อมูลสถิติของจังหวัดสุรินทร์ ผ่านแพลตฟอร์มข้อมูลกลางภาครัฐ (Government Data Catalog : GDC) ให้สามารถเชื่อมโยงข้อมูลด้วย API และนำเสนอผลด้วย Interactive dashboard ได้ เพื่อรองรับความต้องการใช้ข้อมูลเชิงวิเคราะห์และส่งเสริมให้ทุกภาคส่วนนำข้อมูลสถิติไปใช้ในการบริหารจัดการ

ยุทธศาสตร์ที่ ๒ ขับเคลื่อนการปฏิบัติงานทางราชการภายใต้นโยบายและมาตรฐานดิจิทัล และนำดิจิทัลมาใช้พัฒนาการดำเนินงาน

กลยุทธ์ที่ ๒.๑) ส่งเสริมการปฏิบัติงานให้เป็นไปตามมาตรฐาน/ระเบียบ/ข้อกฎหมายที่เกี่ยวข้อง

กลยุทธ์ที่ ๒.๒) เพิ่มประสิทธิภาพการปฏิบัติงานสู่การเป็นองค์กรดิจิทัล พัฒนาแพลตฟอร์มดิจิทัลบริการภาครัฐ และพัฒนาเศรษฐกิจดิจิทัล (Digital Economy)

ยุทธศาสตร์ที่ ๓ พัฒนาทักษะและศักยภาพบุคลากรด้านดิจิทัลของจังหวัดสุรินทร์

กลยุทธ์ที่ ๓.๑) จัดอบรม กิจกรรม สัมมนา เกี่ยวกับการพัฒนาทักษะด้านดิจิทัล

กลยุทธ์ที่ ๓.๒) ส่งเสริมการเรียนรู้ด้วยตนเองผ่านระบบ E – Learning สร้างแรงจูงใจในการเรียนรู้และพัฒนาตนเองอย่างต่อเนื่องตลอดชีวิต พัฒนาการรู้เท่าทันดิจิทัล การเขียนโปรแกรม (Coding) การใช้ AI ในการปฏิบัติงาน, Prompt Engineering

กลยุทธ์ที่ ๓.๓) บูรณาการความร่วมมือกับสถาบันการศึกษาหรือภาคเอกชน เพื่อพัฒนาบุคลากรให้มีทักษะความรู้ด้านดิจิทัลอย่างเพียงพอ

กลยุทธ์ที่ ๓.๔) จัดกิจกรรม ๑ หน่วยงาน ๑ ดิจิทัล เพื่อส่งเสริมให้แต่ละหน่วยงานได้พัฒนาทักษะความรู้ ความสามารถ และเป็นเวทีแสดงผลงานด้านเทคโนโลยีดิจิทัล

2. แผน (Strategic & Operational Plans)

แผนปฏิบัติการที่ครอบคลุมมิติต่างๆ เพื่อความยั่งยืนของระบบ ประกอบด้วย

- แผนการยกระดับโครงสร้างพื้นฐานดิจิทัล (Infrastructure Plan)
  - การติดตั้งและอัปเกรดระบบ Firewall และระบบตรวจจับการบุกรุก (IDS/IPS) ในศูนย์ข้อมูลกลางของจังหวัด
  - การบริหารจัดการระบบสำรองข้อมูลแบบหลายจุด (Off-site Backup) เพื่อรองรับสถานการณ์ภัยพิบัติในพื้นที่
- แผนการบริหารจัดการเหตุการณ์ (Incident Management Plan)
  - การจัดทำคู่มือขั้นตอนการปฏิบัติงาน (Standard Operating Procedure : SOP) เมื่อตรวจพบภัยคุกคามในระดับต่างๆ (ต่ำ กลาง สูง วิกฤต)
  - การซักซ้อมแผนเผชิญเหตุไซเบอร์ (Cyber Exercise) ระหว่างหน่วยงานภายในจังหวัดเป็นประจำทุกปี
- แผนการพัฒนาทักษะบุคลากร (Capacity Building Plan)
  - การอบรมเชิงลึกสำหรับเจ้าหน้าที่เทคนิคด้าน Network Security และ Digital Forensics
  - การจัดกิจกรรม "Cyber Awareness Day" สำหรับข้าราชการและเจ้าหน้าที่ท้องถิ่น เพื่อสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์และดิจิทัล
- KPI รายปี
  - ระยะเวลาเฉลี่ยในการกู้คืนระบบ (Recovery Time) เมื่อเกิดเหตุ ต้องไม่เกิน 4 ชั่วโมง สำหรับระบบวิกฤต
  - จำนวนเหตุการณ์ข้อมูลรั่วไหล (Data Breach) จากความประมาทของเจ้าหน้าที่ต้องเป็นศูนย์

แผน (Plan) ตารางเวลา (Roadmap) และ KPI รายปี

การดำเนินงานในระยะ 1 ปี จะเน้นการสร้างพื้นฐานและยกระดับสู่มาตรฐานสากล

ปี พ.ศ. 2570 ปีแห่งการสร้างความมั่นคง (Stabilization & Awareness) และการยกระดับมาตรฐาน (Optimization & Standards)

- Roadmap
  - ไตรมาส 1 เจ้าหน้าที่ภาครัฐในจังหวัดฯ ไม่น้อยกว่า 80% ผ่านการทดสอบด้าน Cyber Literacy และเริ่มการตรวจสอบความปลอดภัยเชิงลึก (Penetration Testing) ในระบบ One-Plan
  - ไตรมาส 2 ระบบสำคัญของจังหวัด (Critical Systems) มีการสำรองข้อมูล (Backup) ครบ 100% และปรับปรุงระบบรักษาความปลอดภัยตามมาตรฐาน NIST Framework
  - ไตรมาส 3 พัฒนา Dashboard ติดตามสถานะความปลอดภัยแบบ Real-time ของจังหวัด
  - ไตรมาส 4 ประเมินผลความสำเร็จและจัดทำแผนต่อเนื่องปี 2571-2575
- KPI รายปี
  - ระยะเวลาเฉลี่ยในการกู้คืนระบบ (Recovery Time) เมื่อเกิดเหตุ ต้องไม่เกิน 4 ชั่วโมง สำหรับสถานการณ์เมื่อระบบเกิดวิกฤต
  - จำนวนเหตุการณ์ข้อมูลรั่วไหล (Data Breach) จากความประมาทเลินเล่อของเจ้าหน้าที่ต้องเป็นศูนย์

2.3 มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

การนำมาตรฐานการรักษาความมั่นคงปลอดภัยมาประยุกต์ใช้กับระบบสารสนเทศในองค์กรเริ่มเป็นที่แพร่หลายมากขึ้น มาตรฐาน ISO/IEC 27001 ก็เป็นมาตรฐานหนึ่งที่ได้รับความนิยมในปัจจุบันและได้รับการยอมรับจากหลายประเทศในการนำไปใช้บริหารจัดการระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานที่พัฒนามาจากมาตรฐานในตระกูล ISO/IEC 27000 ซึ่ง เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security Management System: ISMS) ได้ผ่านการปรับปรุงและเผยแพร่เมื่อเดือนตุลาคม 2548 โดย International Organization for Standardization (ISO) และ International Electrotechnical Commission (IEC) มีจุดประสงค์เพื่อให้องค์กรสามารถบริหารจัดการทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างมีระบบและเหมาะสม ต่อการดำเนินภารกิจขององค์กร โดยเริ่มแรกองค์กร ต้องทำการวิเคราะห์ความเสี่ยงของระบบจากภัยคุกคาม และจุดอ่อนต่าง ๆ โดยการประเมินความเสี่ยง และการจัดการกับความเสี่ยง เช่น ลด โอนย้าย หรือยอมรับความ เสี่ยง (Risk Assessment and Treatment) เพื่อรักษาระบบสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคง ปลอดภัยในระดับที่เหมาะสม และพอเพียง ขณะเดียวกันมาตรฐานนี้ ยังกำหนดให้องค์กรต้อง ควบคุมดูแล ระบบรักษาความมั่นคงปลอดภัย และกลไกในการพัฒนาอย่างต่อเนื่องอีกด้วย

นอกจากนี้ มาตรฐาน ISO/IEC 27001 ยังประกอบไปด้วย วงจรบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act (การวางแผน- การปฏิบัติ-การตรวจสอบ-การปรับปรุง) ดังแสดงในภาพที่ 2–1

ภาพที่ 2–1 แผนภาพวงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act

2.3.1 กระบวนการการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (อ้างอิงข้อกำหนดตามมาตรฐาน ISO/IEC 27001)

2.3.1.1 รายละเอียดของระบบบริหารจัดการความปลอดภัยสำหรับสารสนเทศ

(1) ข้อกำหนดทั่วไป

องค์กรจะต้องกำหนดลงมือปฏิบัติดำเนินการ เฝ้าระวัง ทบทวน บำรุงรักษา และปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ได้กำหนดไว้เป็นลายลักษณ์อักษร ภายในกรอบกิจกรรม การดำเนินการตามภารกิจต่าง ๆ รวมทั้งความเสี่ยงที่เกี่ยวข้อง แนวทางที่ใช้ ในมาตรฐานนี้จะนำกระบวนการ ดำเนินงานที่มีคุณภาพตามวงจร Plan-Do-Check-Act มาประยุกต์ใช้ จากภาพที่ 2-1 แสดงให้เห็นถึงแบบจำลองขั้นตอนการทำงานของระบบ ISMS ที่ตรงตาม ความต้องการของกลุ่มองค์กร รวมถึงระบบการปฏิบัติงานที่เกิดขึ้น ทำให้ระบบรักษาความมั่นคงปลอดภัยข้อมูล ตรงตามความต้องการ และความคาดหมายได้ ซึ่งแต่ละขั้นตอน ประกอบด้วยรายละเอียดโดยย่อ ดังนี้

- Plan คือ การวางแผนการกำหนดนโยบายความมั่นคงและจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) องค์กรควรกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยและกำหนดนโยบายความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะขององค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี นอกจากนี้ ยังต้องกำหนด

วิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร ระบบความเสี่ยง วิเคราะห์และประเมินความเสี่ยง ระบุและประเมินทางเลือก ในการจัดการกับความเสี่ยงการดำเนินการที่เป็นไปได้ เลือกวัตถุประสงค์และมาตรการทางด้านความปลอดภัย เพื่อจัดการกับความเสี่ยง

- Do คือ การลงมือปฏิบัติหรือดำเนินการตามระบบ ISMS องค์กรควรจัดทำแผนการจัดการความเสี่ยง ลงมือปฏิบัติตามแผนการจัดการความเสี่ยงและตามมาตรฐานที่เลือกไว้

- Check คือ การตรวจสอบและทบทวนผลการดำเนินการตามระบบ ISMS องค์กรควรลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่น ๆ สำหรับการเฝ้าระวัง และทบทวนดำเนินการทบทวน ความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ วัดความสัมฤทธิ์ผล ของมาตรการ ทางด้านความมั่นคงปลอดภัย ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้กับระดับความเสี่ยง ที่เหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ ดำเนินการตรวจสอบและทบทวนระบบบริหารจัดการความมั่นคง ปลอดภัย ปรับปรุงแผนทางด้านความปลอดภัย โดยนำผลของการเฝ้าระวังและทบทวนกิจกรรมต่าง ๆ มาพิจารณาร่วมด้วย บันทึกผลการดำเนินการ ซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

- Act คือ การแก้ไข บำรุงรักษา และปรับปรุงคุณภาพของระบบ ISMS เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบและมีการพัฒนาขึ้นอย่างต่อเนื่อง (Continuous Improvement) องค์กรควรปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้ รวมถึง การใช้มาตรการเชิงแก้ไขป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและองค์กรอื่น แจ้งการปรับปรุงและดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้อง และตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

ข้อกำหนดทางด้านการจัดทำเอกสาร

(1) ความต้องการทั่วไป เอกสารที่จำเป็นต้องจัดทำจะรวมถึงบันทึกแสดงการตัดสินใจของผู้บริหาร เช่น นโยบายความมั่นคงปลอดภัย ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย วิธีการประเมินความเสี่ยง เป็นต้น

(2) การบริหารจัดการเอกสาร ซึ่งเอกสารตามข้อกำหนดของระบบ บริหารจัดการความมั่นคงปลอดภัยจะต้องได้รับการป้องกันและควบคุม ขั้นตอนการปฏิบัติ ที่เกี่ยวข้องกับการจัดการเอกสาร เช่น อนุมัติการใช้งานเอกสารก่อนที่จะเผยแพร่ ทบทวน ปรับปรุงและอนุมัติเอกสารตามความจำเป็น ระบุ การเปลี่ยนแปลงและสถานภาพของเอกสารปัจจุบัน เป็นต้น

(3) การบริหารจัดการบันทึกข้อมูลหรือฟอร์มต่าง ๆ องค์กรจะต้องมี การกำหนด จัดทำ และบำรุงรักษา บันทึกข้อมูลหรือฟอร์มต่างๆ เพื่อใช้เป็นหลักฐานแสดงความสอดคล้องกับข้อกำหนดและการดำเนินการที่มีประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

2.3.1.2 หน้าที่ความรับผิดชอบของผู้บริหาร

1) การให้ความสำคัญในการบริหารจัดการ โดยผู้บริหารจะต้องแสดงถึงการให้ความสำคัญต่อการกำหนด การลงมือปฏิบัติ การดำเนินการเฝ้าระวัง การทบทวน การบำรุงรักษาและการปรับปรุง ระบบบริหารจัดการความมั่นคงปลอดภัย

2) การบริหารจัดการทรัพยากรที่จำเป็น และการอบรมการสร้างความตระหนัก และการเพิ่มขีดความสามารถ เพื่อให้บุคลากรทั้งหมดที่ได้รับมอบหมายหน้าที่ สามารถ

ปฏิบัติงานได้ตามที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย

2.3.1.3 องค์กรควรดำเนินการตรวจสอบภายในระบบบริหารจัดการความมั่นคง ปลอดภัย ตามรอบระยะเวลาที่กำหนดไว้เพื่อตรวจสอบว่า วัตถุประสงค์ มาตรการ กระบวนการ และขั้นตอนปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัยมีความสอดคล้องกับข้อกำหนดในมาตรฐานฉบับนี้ และกฎหมาย ระเบียบ ข้อบังคับต่างๆ รวมถึงสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย และได้รับการลงมือปฏิบัติ และบำรุงรักษาอย่างสัมฤทธิ์ผลและเป็นไปตามที่คาดหมายไว้ นอกจากนี้องค์กรจะต้องวางแผนตรวจสอบภายในโดยพิจารณาถึงสถานภาพและความสำคัญของกระบวนการและส่วนต่างๆ ที่จะได้รับการตรวจสอบและผลการตรวจสอบในครั้งที่ผ่านมา รวมถึงองค์กรจะต้องระบุหน้าที่ความรับผิดชอบและข้อกำหนดต่างๆ ในการวางแผนและดำเนินการตรวจสอบจัดทำรายงานผลการตรวจสอบและบันทึกข้อมูลของการตรวจสอบนั้น

2.3.1.4 ผู้บริหารจะต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนดไว้ (เช่น ปีละ 1 ครั้ง) เพื่อให้มีการดำเนินการที่เหมาะสม พอเพียงและสัมฤทธิ์ผล การทบทวนจะต้องรวมถึงการปรับปรุงหรือเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งรวมถึงนโยบายความมั่นคงปลอดภัย และวัตถุประสงค์ทางด้านความปลอดภัย ผลของการทบทวนจะต้องได้รับการบันทึกไว้เป็นลายลักษณ์อักษรและบันทึกข้อมูลที่เกี่ยวข้องกับการทบทวนไว้

2.3.2 มาตรการการจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

2.3.2.1 นโยบายความมั่นคงปลอดภัย (Security Policy) ประกอบด้วยนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ ซึ่งมีวัตถุประสงค์ เพื่อกำหนดทิศทาง และให้การสนับสนุนการดำเนินการ ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตาม หรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง โดยผู้บริหารองค์กร จะต้องมีการจัดทำนโยบายที่เป็นลายลักษณ์อักษร รวมถึงการทบทวนนโยบายตามระยะเวลาที่กำหนด หรือมีการเปลี่ยนแปลงที่สำคัญขององค์กร

2.3.2.2 โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Internal Organization) โดยได้กล่าวถึง บทบาทของผู้บริหารองค์กรและหัวหน้างานสารสนเทศในด้านต่าง ๆ ดังต่อไปนี้

1) โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร เพื่อบริหารและจัดการ ความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

2) โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับหน่วยงานภายนอก เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผล สารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผลหรือถูกใช้ในการติดต่อสื่อสารกับหน่วยงานภายนอก

2.3.2.3 การบริหารจัดการทรัพย์สินขององค์กร (Asset Management) โดยได้กล่าวถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานพัสดุในด้านต่าง ๆ ดังต่อไปนี้

1) หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร เพื่อป้องกันทรัพย์สินของ

องค์กรจากความเสียหายที่อาจขึ้นได้

2) การจัดหมวดหมู่สารสนเทศ เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

2.3.2.4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security) กล่าวถึงบทบาทของผู้บริหารด้านสารสนเทศ หัวหน้างานสารสนเทศ หัวหน้างานบุคคล และหัวหน้างานที่เกี่ยวข้อง ในด้านต่าง ๆ ดังต่อไปนี้

1) การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ที่ผิดวัตถุประสงค์

2) การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบ และทำความเข้าใจกับนโยบายเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

3) การสิ้นสุดและการเปลี่ยนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

2.3.2.5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) โดยได้กล่าวถึง บทบาทของหัวหน้างาน สารสนเทศ และหัวหน้างานอาคารในด้านต่างๆ ดังต่อไปนี้

1) บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหายและการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

2) ความมั่นคงปลอดภัยของอุปกรณ์ เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และทำให้กิจกรรมการดำเนินงาน ต่าง ๆ ขององค์กรเกิดการติดขัด หรือหยุดชะงัก

2.3.2.6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations Management) โดยได้กล่าวถึง บทบาทของ ผู้บริหารองค์กร ผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ ผู้ที่เป็นเจ้าของกระบวนการ ทำงานและ เจ้าหน้าที่สารสนเทศ ในด้านต่างๆ ดังต่อไปนี้

1) การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

2)การบริหารจัดการการให้บริการของหน่วยงานภายนอก เพื่อจัดทำและรักษา ระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ ระหว่างองค์กรกับหน่วยงานภายนอก

3) การวางแผนและการตรวจรับทรัพยากรสารสนเทศ เพื่อลดความเสี่ยงจาก

ความล้มเหลวของระบบ

4) การป้องกันโปรแกรมที่ไม่ประสงค์ดี เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

5) การสำรองข้อมูล เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของระบบสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

6) การบริหารจัดการทางด้านความปลอดภัยสำหรับเครือข่ายขององค์กร เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

7) การจัดการสื่อที่ใช้ในการบันทึกข้อมูล เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลง แก้ไข การลบหรือทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงัก

8) การแลกเปลี่ยนสารสนเทศ เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

9) การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และการใช้งาน

10) การเฝ้าระวังทางด้านความมั่นคงปลอดภัย เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

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

1) ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ เพื่อควบคุมการเข้าถึงสารสนเทศ

2) การบริหารจัดการการเข้าถึงของผู้ใช้ เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

3) การควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต

4) การควบคุมการเข้าถึงระบบปฏิบัติการที่ไม่ได้รับอนุญาต

5) การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศที่ไม่ได้รับอนุญาต

6) การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอก เพื่อสร้างความมั่นคงปลอดภัยให้กับอุปกรณ์และการปฏิบัติงานที่เกี่ยวข้อง

2.3.2.8 การจัดหาการพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance) โดยได้กล่าวถึง บทบาทของ หัวหน้างานสารสนเทศ ผู้พัฒนาระบบ และผู้เป็นเจ้าของระบบในด้านต่างๆ ดังต่อไปนี้

1) ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ เพื่อให้การจัดหา และพัฒนาระบบสารสนเทศได้พิจารณาถึง ประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

2) การประมวลผลสารสนเทศในแอปพลิเคชัน เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งาน

สารสนเทศที่ผิดวัตถุประสงค์

3) มาตรการการเข้ารหัสข้อมูล เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการทางการเข้ารหัสข้อมูล

4) การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

5) การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

6) การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

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

1) การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

2) การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

2.3.2.10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management) โดยได้กล่าวถึง บทบาทของผู้บริหารสารสนเทศ และหัวหน้างานสารสนเทศ ที่เกี่ยวกับหัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร เพื่อป้องกัน การติดขัดหรือ การหยุดชะงักของกิจกรรมต่างๆ เพื่อป้องกันกระบวนการทำงานที่สำคัญ อันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

2.3.2.11 การปฏิบัติตามข้อกำหนด (Compliance) โดยได้กล่าวถึง บทบาทของหัวหน้างานสารสนเทศและหัวหน้างานนิติกรในด้านต่าง ๆ ดังต่อไปนี้

1) การปฏิบัติตามข้อกำหนดทางกฎหมาย เพื่อหลีกเลี่ยงการละเมิด ข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ

2) การปฏิบัติตามนโยบายมาตรฐานความปลอดภัยและข้อกำหนดทางเทคนิค เพื่อให้ระบบเป็นตามนโยบายและมาตรฐานความมั่นคงปลอดภัยตามที่องค์กรกำหนดไว้

3) การตรวจประเมินระบบสารสนเทศ เพื่อตรวจประเมินระบบสารสนเทศให้ได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทำงานน้อยที่สุด