Information and Cyber Security Management Manual

คู่มือการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร

Submitted by:
MWA Digital

คู่มือการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร

Information and Cyber Security Management Manual

หมายเลขเอกสาร	
วันที่มีผลบังคับใช้	๑ กันยายน ๒๕๖๖
ปรับปรุงครั้งที่	๐๑
ประเภทเอกสาร	ภายใน
เจ้าของเอกสาร	สายงานเทคโนโลยีดิจิทัล
ทบทวนโดย	ทีมงานดำเนินการข้อ ๕.๑
มีผลบังคับใช้กับ	หน่วยงานภายใน กปน.
อนุมัติโดย	รองผู้ว่าการ (เทคโนโลยีดิจิทัล)

ประวัติการแก้ไขเอกสาร

ครั้งที่	รายละเอียดการแก้ไข	วันที่มีผลบังคับใช้
1	นำคู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ Information Security Management Systems Manual ภายใต้มาตรฐาน ISO27001/2013 เป็นแนวทางในการจัดทำคู่มือฉบับนี้	1 กันยายน 2566

การอนุมัติเอกสาร

ผู้จัดทำ	
ชื่อ นายทรงศักดิ์ ศรีโดวัน ตำแหน่ง ผอ.กขม.ฝคท. วันที่ 17 ส.ค. 66	ลงชื่อ ..... (นายทรงศักดิ์ ศรีโดวัน) ผอ.กขม.ฝคท. ( )
ผู้สอบทาน	
ชื่อ นายภาคภูมิ พิระชัย ตำแหน่ง ผอ.ฝคท. วันที่ 24 ส.ค. 66	ลงชื่อ ..... (นายภาคภูมิ พิระชัย) ผอ.ฝคท. ( )
ผู้อนุมัติ	
ชื่อ นายธำรง บูรณตระกูล ตำแหน่ง รวก.(ท) วันที่ 25 ส.ค. 66	ลงชื่อ ..... (นายธำรง บูรณตระกูล) รองผู้ว่าการ (เทคโนโลยีดิจิทัล) ( )

สารบัญ

หน้า

1. วัตถุประสงค์

คู่มือการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร (Information Security Management Manual) มีวัตถุประสงค์ดังนี้

- เพื่อให้ระบบเทคโนโลยีสารสนเทศและไซเบอร์ของการประปานครหลวง เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง
- เพื่อเป็นแนวทางในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กรโดยให้สอดคล้องกับมาตรฐานสากล ISO/IEC27001
- เพื่อเป็นแนวทางการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจะก่อให้เกิดความเสียหายแก่องค์กร
- เพื่อดำเนินการตามกฎหมาย กฎระเบียบ และข้อบังคับด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่เกี่ยวข้อง

2. นิยามและคำจำกัดความ

- **กปน.** หมายถึง การประปานครหลวง
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของการประปานครหลวง
- **ไซเบอร์ (Cyber)** หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป (อ้างอิงจาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562)
- **ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง** การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
- **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ ผู้ใช้งานสามารถเข้าใช้ได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

- **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่างๆ ขององค์กรได้ ได้แก่ ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น
- **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
- **ผู้มีส่วนได้ส่วนเสีย** หมายถึง ผู้รับผิดชอบ พนักงาน ผู้ส่งมอบ คู่ค้าที่สำคัญ ลูกค้า และผู้มีส่วนได้ส่วนเสียอื่นที่เกี่ยวข้อง (ผู้มีส่วนได้ส่วนเสียขององค์กร ในคู่มือความรับผิดชอบต่อสังคม กปน.)

3. หน้าที่ความรับผิดชอบ

ลำดับ	ตำแหน่ง	หน้าที่ความรับผิดชอบ
1	คณะอนุกรรมการเทคโนโลยีดิจิทัลของ กปน.	● อนุมัตินโยบายความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ● กำกับดูแล ติดตาม การดำเนินงานตามกระบวนการการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร
2	ผู้ว่าการการประปานครหลวง	● ลงนามประกาศนโยบายความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ● เป็นผู้รับผิดชอบต่อความเสี่ยง ความ เสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์หรือข้อมูลเกิดความเสียหาย หรือ อันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยรองผู้ว่าการสายงานต่าง ๆ มีหน้าที่
3	รองผู้ว่าการสายงานต่างๆ	● กำกับดูแลรับผิดชอบให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการ รักษาความมั่นคงปลอดภัยด้านสารสนเทศ
4	ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล	● เป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษาแก่ผู้ปฏิบัติงานระดับปฏิบัติ
5	ทีมจัดทำ/ทบทวน คู่มือบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร	● กำหนด/ทบทวน คู่มือบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร ● ประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม ● กำหนด/ทบทวน การวัด ติดตาม วิเคราะห์ ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการดำเนินด้านการบริหารจัดการความมั่นคง

ลำดับ	ตำแหน่ง	หน้าที่ความรับผิดชอบ
		ปลอดภัยสารสนเทศและไซเบอร์ขององค์กร โดยสามารถวัดผลได้อย่างเป็นรูปธรรม เพื่อนำมาปรับปรุงและพัฒนากระบวนการอย่างต่อเนื่อง ● นำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน การกำกับดูแลด้านการบริหารจัดการดิจิทัล / จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้เพื่อนำไปปรับปรุงและทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล
6	พนักงานและผู้ปฏิบัติงานสายงานเทคโนโลยีดิจิทัล (สายงาน DT)	● รับทราบและดำเนินการตาม นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และคู่มือการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร
7	พนักงานและผู้ปฏิบัติงาน กปน. และผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการ	● รับทราบและดำเนินการตาม นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

4. ขอบเขตการดำเนินการด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร

เพื่อกำหนดกรอบและวิธีปฏิบัติสำหรับการทำงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Information and Cyber Security Framework) สำหรับบริหารจัดการระบบเทคโนโลยีสารสนเทศที่สำคัญของการประปานครหลวง ซึ่งประกอบด้วย

- ขอบเขตที่อยู่ในการขอใบรับรองมาตรฐานสากล สำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 สำหรับการดำเนินการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) โดยขอบเขตครอบคลุมศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรองของ กปน. (เอกสารคู่มือการจัดการระบบความมั่นคงปลอดภัยสารสนเทศ)
- ขอบเขตที่ไม่อยู่ในการขอใบรับรองมาตรฐานสากล การประปานครหลวงให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีทั้งระบบเครือข่ายและความมั่นคงปลอดภัยครอบคลุมทั้งองค์กร โดยปฏิบัติตามมาตรฐานที่เกี่ยวข้อง

5. กรอบปฏิบัติสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework)

กปน. ได้นำวิธีการสำหรับบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามรูปแบบ ที่ใช้ในมาตรฐานสากล ISO/IEC 27001:2013 โดยประกอบด้วย 4 ขั้นตอนหลัก ได้แก่

5.1 Plan: ขั้นตอนในระยะการวางแผน ได้แก่

- จัดทำเอกสารแสดงขอบเขต และบริบทขององค์กร
- ทบทวนขั้นตอนปฏิบัติการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- รวบรวมทรัพย์สินสารสนเทศ และประเมินความเสี่ยงด้านความมั่นคงปลอดภัย
- จัดทำรายงานผลการประเมินความเสี่ยง และแผนจัดการความเสี่ยง
- จัดทำหรือทบทวนเอกสารขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ
- กำหนดหรือทบทวนนโยบาย และแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสารสนเทศ
- กำหนดเกณฑ์วัดเป้าหมายด้านความมั่นคงปลอดภัยสารสนเทศ
- จัดทำคู่มือสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (SOA)
- การบริหารจัดการความเสี่ยง (Risk Management) ซึ่งประกอบด้วยการประเมินความเสี่ยง (Risk Assessment) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการควบคุมหรือบำบัดความเสี่ยง (Risk Treatment) ตลอดจนมีการกำหนดแผนการจัดการ มีมาตรฐาน และขั้นตอนการปฏิบัติงานสำหรับการควบคุมความเสี่ยง

5.2 Operation: ขั้นตอนในระยะนำไปปฏิบัติ ได้แก่

- สื่อสารแผนจัดการความเสี่ยง และดำเนินการตามแนวทางจัดการความเสี่ยง
- ดำเนินการตามมาตรการควบคุมระบบความมั่นคงปลอดภัยสารสนเทศ
- ตรวจสอบสถานะของการจัดทำแผนความต่อเนื่องทางธุรกิจ และเอกสารต่างๆ ที่เกี่ยวข้อง
- อบรม เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

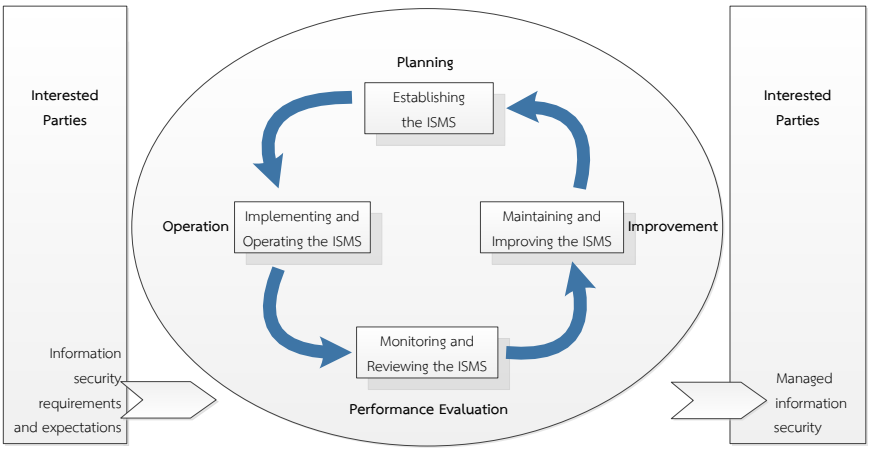
5.3 Evaluation: ขั้นตอนในระยะการตรวจสอบและทบทวน ได้แก่

- ติดตามการดำเนินการตามเกณฑ์วัดเป้าหมายความมั่นคงปลอดภัยสารสนเทศ
- การตรวจประเมินภายใน (Internal Audit) ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ
- จัดทำบันทึกการตรวจสอบ และรายงานผลการตรวจสอบภายใน
- การทบทวนระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Management Review)

5.4 Improvement: ขั้นตอนในระยะปรับปรุงอย่างต่อเนื่อง ได้แก่

- การดำเนินการปรับปรุงระบบบริหารความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง
- ดำเนินการปรับปรุงแก้ไขความไม่สอดคล้องที่พบ

รูปที่ 1 แสดงกรอบปฏิบัติระบบบริหารจัดการรักษาความมั่นคงปลอดภัยสารสนเทศ



6. กรอบปฏิบัติสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework)

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework) จัดขึ้นตามประกาศคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564 ซึ่งสามารถสรุปกิจกรรมที่ต้องดำเนินการต่างๆ ได้ดังต่อไปนี้

รูปที่ 2 แสดงกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

6.1 การระบุ (Identify) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากร และกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล และขีดความสามารถ

6.2 การป้องกัน (Protect) เป็นการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐานสำคัญ โดยมีวัตถุประสงค์เพื่อจำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมการฝึกอบรมและการสร้างความตระหนัก มาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี

6.3 การตรวจจับ (Detect) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตามต่อเนื่อง

6.4 การตอบสนอง (Respond) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

6.5 การคืนสภาพ (Recover) เป็นการจัดทำและดำเนินกิจกรรมตามแผนงาน เพื่อรองรับการดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนทั้งด้านขีดความสามารถและบริการให้ได้ตามที่กำหนด

7. บริบทภายใน (Internal Context)

หมายถึง สภาพแวดล้อมภายในที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กร รวมถึงประเด็นของผู้มีส่วนได้ส่วนเสียภายใน และปัจจัยภายในต่างๆ ที่สามารถมีอิทธิพลต่อวิถีทางที่องค์กรจะบริหารความเสี่ยง และดำเนินการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ในทิศทางเดียวกับวัฒนธรรมองค์กร การดำเนินงาน โครงสร้าง และกลยุทธ์

7.1 ลักษณะองค์กร

การประปานครหลวง (กปน.) ก่อตั้งเมื่อวันที่ 16 สิงหาคม 2510 โดยรัฐบาลได้ตราพระราชบัญญัติการประปานครหลวง พ.ศ. 2510 ด้วยการรวมกิจการกองประปากรุงเทพ สังกัดกรมโยธาเทศบาล กองประปานครธนบุรี สังกัดเทศบาลนครธนบุรี การประปาสมุทรปราการ สังกัดเทศบาลสมุทรปราการ และหมวดการประปานนทบุรี ของกองประปาภูมิภาค สังกัดกรมโยธาเทศบาล รวม 4 แห่ง เข้าไว้ด้วยกัน และกำหนดให้เป็นหน่วยงานรัฐวิสาหกิจในกลุ่มสาธารณูปการ สังกัดกระทรวงมหาดไทย ให้บริการน้ำประปาในเขตกรุงเทพมหานคร นนทบุรี และสมุทรปราการ

จากประสบการณ์อันยาวนานในการดำเนินกิจการประปาทำให้ กปน. มีองค์ความรู้ทั้งด้านการผลิตและการบริการ และถ่ายทอดองค์ความรู้เหล่านั้นจากพนักงานรุ่นเก่าสู่รุ่นใหม่ ทำให้พนักงานมีความรู้ด้านงานประปาและสามารถพัฒนาต่อยอดให้ทันสมัยตอบสนองความต้องการ และความคาดหวังของผู้ใช้บริการได้มากยิ่งขึ้น

7.2 วิสัยทัศน์ ค่านิยม พันธกิจ ภารกิจ

7.2.1 วิสัยทัศน์

"ประปาคุณภาพ เพื่อชีวิตที่ดี Quality Water for Quality Living"

7.2.2 ค่านิยม

"คุณภาพที่ยั่งยืน มุ่งมั่นเพื่อสิ่งที่ดียิ่งขึ้น ปรับตัวว่องไว ฉลาดใช้เทคโนโลยี มองธุรกิจกว้างไกล สร้างชื่อเสียงความภูมิใจให้ กปน."

7.2.3 พันธกิจ

- ดำเนินธุรกิจหลักด้านน้ำอย่างครบวงจรโดยให้บริการน้ำที่มีมาตรฐานคุณภาพเพื่อคุณภาพชีวิตที่ดีของประชาชนอย่างทั่วถึง
- องค์กรที่มีความสามารถในการรับมือวิกฤตการณ์อย่างมีประสิทธิภาพ
- ดำเนินธุรกิจที่เกี่ยวเนื่อง เพื่อสร้างคุณค่าแก่ผู้มีส่วนได้ส่วนเสีย และสร้างการเติบโตขององค์กรอย่างยั่งยืน

7.3 วิสัยทัศน์ของสายงานเทคโนโลยีดิจิทัล

"ให้บริการเทคโนโลยีสารสนเทศและการสื่อสารที่มั่นคงปลอดภัย ด้วยบุคลากรคุณภาพตอบสนองการพัฒนาองค์กรอย่างยั่งยืน"

7.4 ภารกิจของสายงานเทคโนโลยีดิจิทัล

7.4.1 ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (ฝคท.)

- บริหารงาน วางแผน พัฒนาและจัดหาระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบการสื่อสารข้อมูล การประมวลผล และการปฏิบัติการคอมพิวเตอร์ให้สอดคล้องเหมาะสมกับแผนพัฒนาเทคโนโลยีสารสนเทศของ กปน.
- กำหนดมาตรฐานด้านการประมวลผลข้อมูล ระบบเครื่องคอมพิวเตอร์ และเครือข่ายสื่อสารข้อมูล รวมถึงอุปกรณ์เทคโนโลยีสารสนเทศอื่นที่เกี่ยวข้อง
- กำหนดมาตรฐานการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- บริหารจัดการด้านบุคลากร สนับสนุนวิชาการ ประสานงานด้านระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบประมวลผลข้อมูลกับหน่วยงานที่เกี่ยวข้อง

7.4.2 ฝ่ายยุทธศาสตร์และนวัตกรรมดิจิทัล (ฝยท.)

- บริหารงาน วางแผน จัดทำแผนแม่บทด้านเทคโนโลยีสารสนเทศและการสื่อสารของ กปน. ให้มีความเหมาะสมสอดคล้องกับการพัฒนา กปน. พร้อมทั้งติดตามประเมินผลโครงการด้านสารสนเทศ
- บริหารงาน วางแผน จัดการการบูรณาการข้อมูลด้านสารสนเทศให้มีความถูกต้องทันสมัยครบถ้วน พร้อมใช้งาน

- บริหารจัดการด้านบุคลากร และสนับสนุนพัฒนาความรู้วิชาการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้กับพนักงานในหน่วยงานต่างๆ ให้เหมาะสมกับความต้องการกับการใช้งานให้ทันสมัย
- บริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือแผนความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- บริหาร วางแผนวิเคราะห์การใช้งานระบบสารสนเทศ ประเมินผลการใช้เทคโนโลยีสารสนเทศให้เป็นไปตามเป้าหมายที่กำหนด

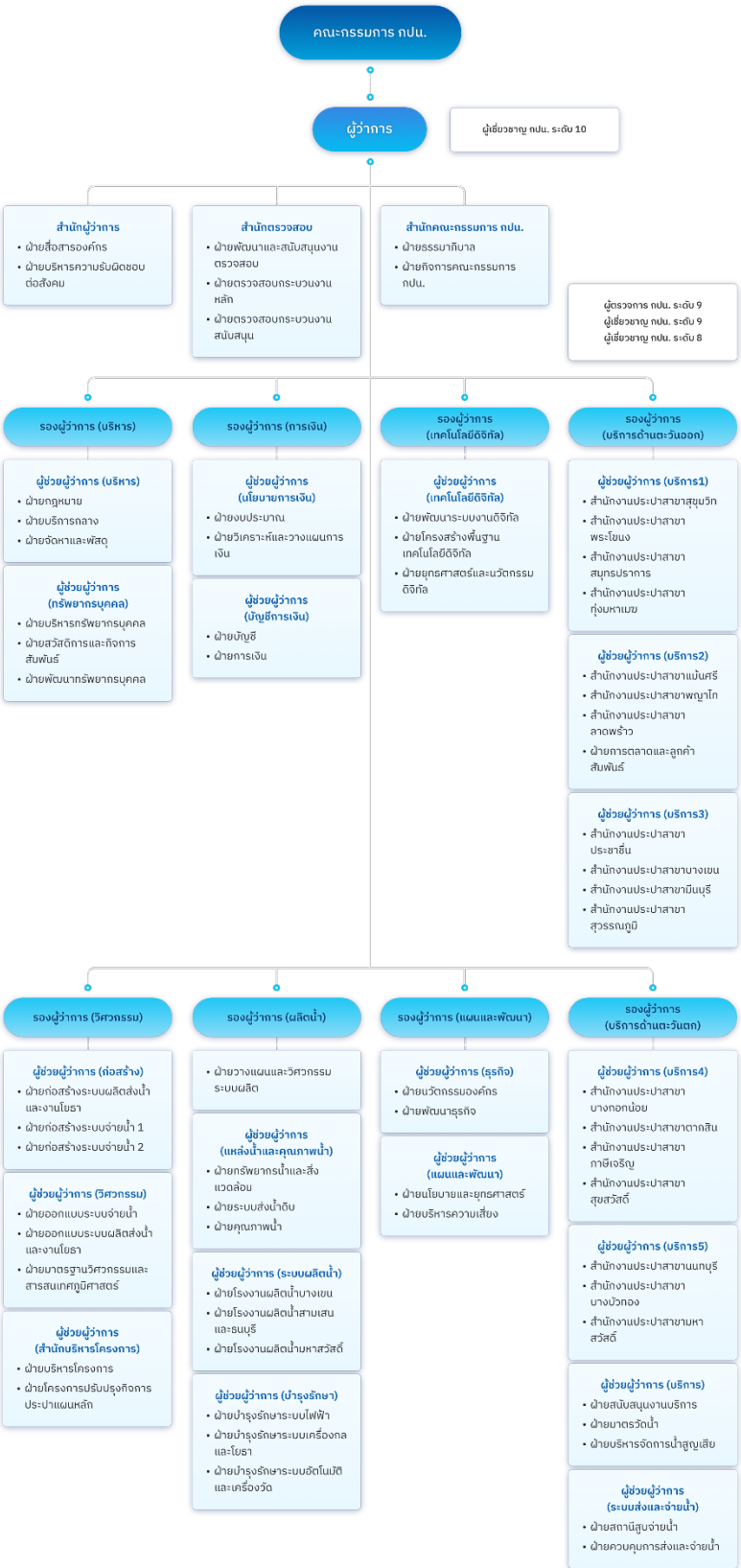
7.4.3 ฝ่ายพัฒนาระบบงานดิจิทัล (ฝพท.)

- บริหารงาน วางแผน พัฒนาและจัดหาระบบงานคอมพิวเตอร์ให้สอดคล้องเหมาะสมกับแผนพัฒนาเทคโนโลยีสารสนเทศของ กปน.
- กำหนดมาตรฐานด้านเอกสาร วิธีการของการวิเคราะห์ระบบ การออกแบบระบบ การจัดทำคำสั่งหรือโปรแกรมคอมพิวเตอร์ การทดสอบระบบ การติดตั้งใช้งานและสนับสนุนการใช้งานอย่างมีประสิทธิภาพ
- กำหนดมาตรฐานการรักษาความปลอดภัยของระบบงานคอมพิวเตอร์ของ กปน.
- บริหารจัดการด้านบุคลากร สนับสนุนวิชาการ ประสานงานด้านระบบสารสนเทศกับผู้ใช้งานทั้งหน่วยงานภายใน และภายนอก กปน.
- บริหาร จัดการและบำรุงรักษา ระบบงานคอมพิวเตอร์อย่างมีประสิทธิภาพ

7.5 โครงสร้างการบริหารงาน กปน.

กปน. เป็นรัฐวิสาหกิจซึ่งอยู่ภายใต้การกำกับดูแลสังกัดกระทรวงมหาดไทย และอยู่ภายใต้การกำกับดูแลของผู้ถือหุ้น ซึ่งกระทรวงการคลังเป็นผู้กำกับดูแล ตัวชี้วัดผลการดำเนินการ โดยคณะรัฐมนตรีทำการแต่งตั้งคณะกรรมการ กปน. ประกอบด้วยผู้ทรงคุณวุฒิในหลากหลายสาขาวิชาชีพ มีจำนวนเป็นไปตามพระราชบัญญัติ กปน. พ.ศ. ๒๕๑๐ ประกอบด้วย ประธานกรรมการ และกรรมการอื่นอีกไม่น้อยกว่า 9 คน แต่ไม่เกิน 13 คน และผู้ว่าการเป็นกรรมการ โดยตำแหน่ง มีวาระการดำรงตำแหน่งคราวละ 3 ปี บทบาทของคณะกรรมการมุ่งเน้น ในฐานะที่เป็นตัวแทนของรัฐและประชาชน ในการกำหนดนโยบายทั้งในด้านการบริหารงานและการบริหารความเสี่ยง รวมทั้งพิจารณาและให้ความเห็นชอบ กลยุทธ์ เป้าหมายทางการเงิน แผนงาน และงบประมาณ ตลอดจนกำกับดูแลการบริหารงานของฝ่ายบริหาร จัดการให้บรรลุเป้าหมายอย่างมีประสิทธิภาพสูงสุดและเป็นไปอย่างเปิดเผย โปร่งใส และตรวจสอบได้ เพื่อสร้างความเชื่อมันให้แก่ผู้มีส่วนได้ส่วนเสียทุกฝ่าย

รูปที่ 3 โครงสร้างองค์กรการประปานครหลวง



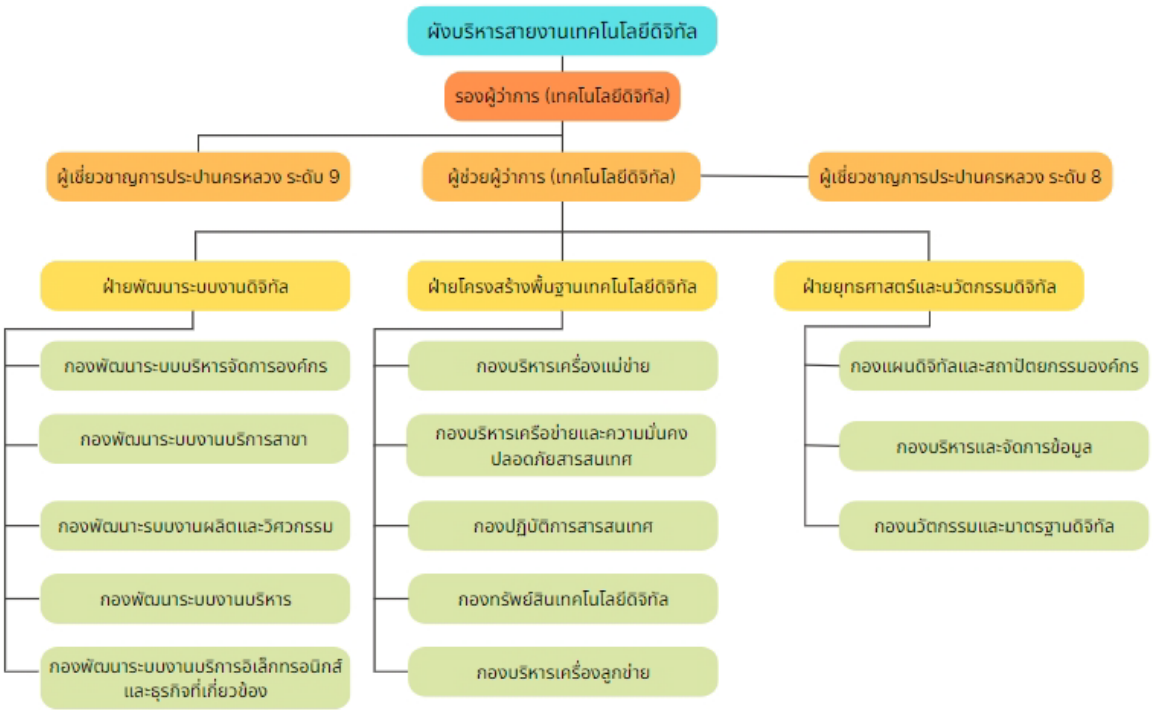
7.6 โครงสร้างหน่วยงานด้านเทคโนโลยีดิจิทัลของการประปานครหลวง

หน่วยงานด้านเทคโนโลยีดิจิทัลของ กปน. มีโครงสร้างดังแสดงในรูปที่ 3 และ รูปที่ 4 โดยประกอบด้วยหน่วยงาน 3 หน่วยงาน คือ

- ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล
- ฝ่ายยุทธศาสตร์และนวัตกรรมดิจิทัล
- ฝ่ายพัฒนาระบบงานดิจิทัล

ทั้งนี้หน่วยงานข้างต้นอยู่ภายใต้ผู้บริหารระดับสูง คือ รองผู้ว่าการ (เทคโนโลยีดิจิทัล) และผู้ช่วยผู้ว่าการ (เทคโนโลยีดิจิทัล)

รูปที่ 4 โครงสร้างของหน่วยงานด้านเทคโนโลยีดิจิทัลของการประปานครหลวง



7.7 ผู้มีส่วนได้ส่วนเสียภายในองค์กร

- ผู้บริหาร หมายถึง ผู้ว่าการ กปน. คณะกรรมการ กปน. คณะอนุกรรมการเทคโนโลยีดิจิทัลของ กปน. คณะกรรมการ ISMS
- ผู้ดูแลระบบ หมายถึง บุคคลที่ต้องดำเนินกิจกรรมในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์

- ผู้ปฏิบัติงาน หมายถึง ผู้บริหารระดับต้น (ระดับ 6-7) พนักงาน (ระดับ 1-5) รวมถึงลูกจ้างของบริษัทที่เข้าทำงานใน กปน. หรือผู้ที่ใช้บริการระบบเทคโนโลยีสารสนเทศ

7.8 ประเด็นภายในองค์กร

- มีข้อมูลสารสนเทศที่สำคัญอยู่ภายในระบบที่ใช้งานภายในองค์กร
- พนักงานไม่ได้ตระหนักถึงความมั่นคงปลอดภัยสารสนเทศอย่างเพียงพอ
- มีการกำหนด คำสั่ง กฎระเบียบ ต่าง ๆเพื่อใช้ในการปฏิบัติงานภายในองค์กร
- มีการจ้างผู้ให้บริการภายนอกในการดูแลระบบต่าง ๆ

7.9 นโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง

เพื่อรักษาความมั่นคงปลอดภัยให้แก่ทรัพย์สินของ กปน. โดยเฉพาะข้อมูลสำคัญ เพื่อให้พ้นจากภัยคุกคาม และความเสี่ยงทั้งจากภายในและภายนอกองค์กร กปน. จึงได้กำหนดนโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง โดยมีเอกสารแนบท้ายเป็น แนวปฏิบัติในการรักษาความปลอดภัยระบบสารสนเทศและไซเบอร์ของการประปานครหลวง

8. บริบทภายนอกองค์กร (External Context)

บริบทภายนอกองค์กร หมายถึง สภาพแวดล้อมภายนอกที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กร โดยพิจารณาประเด็น และปัจจัยที่อาจมีผลกระทบต่อการดำเนินงานขององค์กร เพื่อให้มั่นใจว่าวัตถุประสงค์และประเด็นของผู้มีส่วนได้เสียภายนอกได้รับการพิจารณาสำหรับการพิจารณาความเสี่ยง และบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

8.1 ผู้มีส่วนได้ส่วนเสียภายนอกองค์กร

- หน่วยงานกำกับดูแล หมายถึง กระทรวงมหาดไทย กระทรวงการคลัง สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สศช.) สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) สำนักงบประมาณ
- หน่วยงานที่เกี่ยวข้องในเชิงภารกิจ หมายถึง กรมชลประทาน กรมทรัพยากรน้ำ กรมทรัพยากรน้ำบาดาล กรมโยธาธิการและผังเมือง สำนักผังเมือง สำนักการระบายน้ำ สำนักยุทธศาสตร์การประปาส่วนภูมิภาค สำนักการโยธา ตัวแทนจากภาคขนส่งมวลชน กรมทางหลวง กรมทางหลวงชนบท กรมควบคุมมลพิษ
- ลูกค้า หมายถึง ผู้ใช้น้ำ ผู้ชำระค่าน้ำ
- ชุมชน หมายถึง ชุมชนโดยรอบ
- ผู้ส่งมอบ หมายถึง หน่วยงานผู้ให้บริการด้านเทคโนโลยีสารสนเทศ ตัวแทนช่องทางรับชำระค่าบริการ

- ผู้รับบริการด้านเทคโนโลยีสารสนเทศ หมายถึง บุคคลภายนอก/หน่วยงาน ที่ขอใช้บริการด้านเทคโนโลยีสารสนเทศเป็นการชั่วคราว

8.2 ประเด็นภายนอกองค์กร

- ปัญหา อุปสรรค ความเสี่ยงต่างๆ จากภายนอก
- มีกฎหมาย ข้อบังคับที่ต้องให้องค์กรปฏิบัติตาม
- สร้างความมั่นใจต่อผู้ใช้น้ำ (ลูกค้า)

8.3 กฎหมาย กฎระเบียบ และข้อบังคับด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

กฎหมาย กฎระเบียบ มาตรฐาน และกรอบการดำเนินงานด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง ได้แก่

- พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และฉบับแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑
- พระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ และฉบับแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๘ (ฉบับที่ ๓) พ.ศ. ๒๕๕๘ (ฉบับที่ ๔) พ.ศ. ๒๕๖๑
- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙
- พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕
- ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔
- ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒
- พระราชบัญญัติว่าด้วยการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. ๒๕๕๘
- พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ๒๕๖๐
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

9. กระบวนการและการวิเคราะห์ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ

SIPOC กระบวนการดำเนินการด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

Supplier	Input	Process	Output	Customer
1. คณะกรรมการ กปน. 2. คณะอนุกรรมการเทคโนโลยีดิจิทัล ของ กปน. 3. คณะกรรมการ ISMS 4. คณะทำงาน ISMS 5. ฝคท. 6. ฝยท. 7. ฝพท.	- วิสัยทัศน์ ภารกิจ พันธกิจ ของกปน. และสายงานเทคโนโลยีดิจิทัล - โครงสร้างการบริหารของกปน. และสายงานเทคโนโลยีดิจิทัล - รายงาน การรับรู้นโยบาย และ ผลการดำเนินงานตามคู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - รายงานผลการดำเนินงานตามมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของปีที่ผ่านมา - ข้อเสนอแนะเพื่อนำไปปรับปรุงของปีที่ผ่านมา - รายงานผลการตรวจประเมินของปีที่ผ่านมา	1. วางแผนและกำหนดขอบเขตและบริบทขององค์กร ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (คณะทำงาน ISMS)	- ขอบเขตการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ - วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ	คณะทำงาน ISMS, ฝพท., ฝยท., ฝคท.
คณะทำงาน ISMS, ฝพท., ฝยท., ฝคท.	- ขอบเขตการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ - วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ - รายการข้อมูลทรัพย์สินสารสนเทศ	2. รวบรวมทรัพย์สินสารสนเทศ (คณะทำงาน ISMS)	- ทะเบียนทรัพย์สิน ภายใต้ขอบเขตการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	คณะทำงาน ISMS, ผู้ดูแลระบบ ฝพท., ฝยท., ฝคท.

Supplier	Input	Process	Output	Customer
คณะทำงาน ISMS ฝบส., ฝพท., ฝยท., ฝคท.	- ทะเบียนทรัพย์สิน ภายใต้ขอบเขตการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ - แผนประเมินความเสี่ยงองค์กร	3. กำหนดขั้นตอนปฏิบัติการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (รายละเอียดในข้อ 5.2) - จัดทำรายงานแผนการประเมินความเสี่ยงและแผนจัดการความเสี่ยง (รายละเอียดในข้อ 5.2) (คณะทำงาน ISMS)	- รายงานการประเมินความเสี่ยง - รายงานผลการจัดการความเสี่ยง - แผนการจัดการความเสี่ยง	คณะทำงาน ISMS
คณะทำงาน ISMS	- พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 - พ.ร.ก. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ.2553 - พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 - รายงานการประเมินความเสี่ยง - รายงานผลการจัดการความเสี่ยง - แผนการจัดการความเสี่ยง	4. กำหนดหรือทบทวนนโยบายและแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสารสนเทศ (คณะทำงาน ISMS)	- นโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์ - คู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - มาตรการความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก	คณะกรรมการ ISMS คณะทำงาน ISMS ฝคท.

Supplier	Input	Process	Output	Customer
คณะทำงาน ISMS	- นโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์	5. พิจารณาเห็นชอบนโยบาย (คณะกรรมการ ISMS) (ผวก. ลงนาม)	- นโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์	พนักงาน กปน.
คณะทำงาน ISMS	- คู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - มาตรการความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก	6. พิจารณาเห็นชอบ คู่มือและมาตรการความมั่นคงปลอดภัย (รวก.(ท))	- คู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - มาตรการความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก	ฝคท., ฝพท., ฝยท., คู่ค้า
คณะทำงาน ISMS ฝคท.	- นโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์	7. จัดทำหรือทบทวนเอกสารขั้นตอนปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (คณะทำงาน ISMS และ ฝคท.)	- คู่มือขั้นตอนปฏิบัติงานด้านรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	ผู้ดูแลระบบ ฝพท., ฝยท., ฝคท.,
คณะทำงาน ISMS, ผู้ดูแลระบบ ฝพท., ฝยท., ฝคท.,	- นโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์ - คู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - คู่มือขั้นตอนปฏิบัติงานด้านรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	8. สื่อสาร - นโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์ - คู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - คู่มือขั้นตอนปฏิบัติงานด้านรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	- รายงาน การรับรู้นโยบาย และ ผลการดำเนินงานตามคู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	คณะกรรมการ ISMS คณะทำงาน ISMS ฝคท.,คู่ค้า

	- มาตรการความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก	- มาตรการความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก (รวก.(ท.))		
ผู้ดูแลระบบ ฝคท.,ฝพท.,ฝยท.	- คู่มือขั้นตอนปฏิบัติด้านรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	9. ดำเนินการตามมาตรฐานการควบคุมระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (ผู้ดูแลระบบ ฝคท. ,ฝพท.,ฝยท.)	รายงานผลการดำเนินงานตามมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	รวก.(ท.), ชวก.(ท.) ฝคท. ,ฝพท.,ฝยท.
รวก.(ท.), ชวก.(ท.)	รายงาน หรือผลการดำเนินงานตามมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	10. ตรวจสอบการดำเนินการตามเกณฑ์วัดเป้าหมายความมั่นคงปลอดภัยสารสนเทศ (คณะกรรมการ ISMS)	ข้อเสนอแนะเพื่อนำไปปรับปรุง	คณะทำงาน ISMS
รวก.(ท.), ชวก.(ท.) ฝคท.,ฝพท.,ฝยท.	- รายงานผลการดำเนินงานตามมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	11 ตรวจประเมินภายใน (Internal Audit) ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ตามกระบวนการข้อ 5.3 (สตส.)	รายงานผลการตรวจประเมิน	คณะกรรมการ ISMS ฝคท.

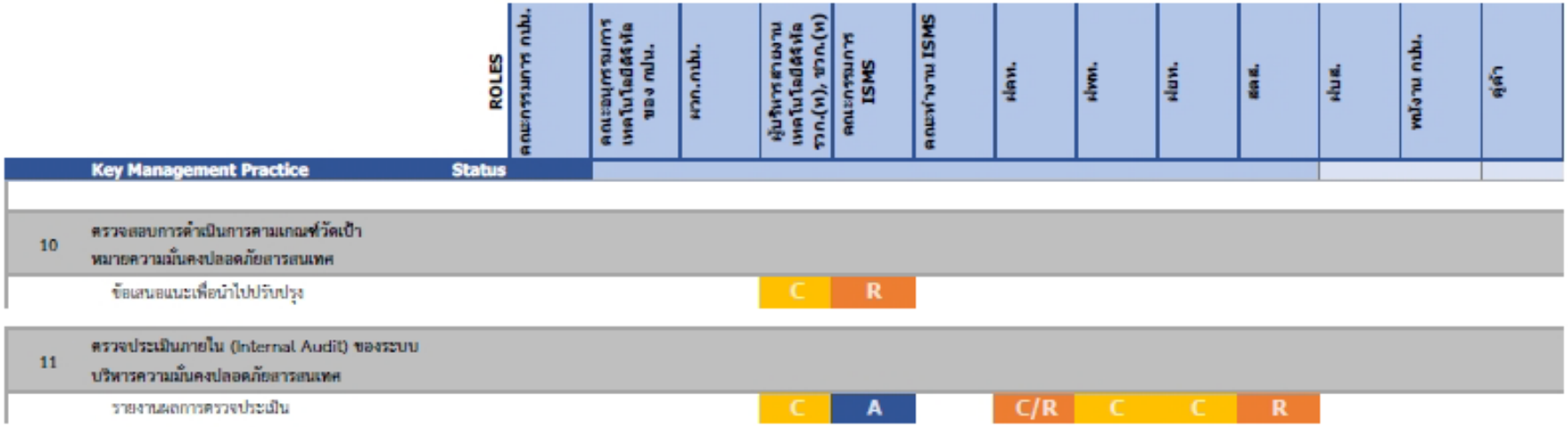
คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee Team) มีอำนาจดังต่อไปนี้

1. กำหนดมาตรฐานและนโยบายในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
2. พิจารณา และกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สามารถยอมรับได้
3. กำกับดูแล และสั่งการให้หน่วยงานที่เกี่ยวข้องดำเนินการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ
4. ให้คำปรึกษา แนะนำ และประเมินผลการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ
5. บริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้เป็นไปตามระบบประเมินคุณภาพรัฐวิสาหกิจ

RACI กระบวนการดำเนินการด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

	ROLES	คณะกรรมการ กมั่น.	คณะอนุกรรมการเทคโนโลยีดิจิทัลของ กมั่น.	หวก.กมั่น.	ผู้บริหารเทคโนโลยีสารสนเทศ รวก.(ท), ชวก.(ท)	คณะกรรมการ ISMS	คณะทำงาน ISMS	ผคก.	ผพท.	ผยท.	สสส.	ผมส.	หนงาน กมั่น.	คู่ค้า
	Key Management Practice **Status**													
1	**วางแผนและกำหนดขอบเขตและบริบทขององค์กรในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ**													
	- ขอบเขตการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ '- วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ		C	C			C	R	R	R	R			
2	**รวบรวมทรัพย์สินสารสนเทศในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ**													
	ทะเบียนทรัพย์สิน ภายใต้ขอบเขตการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ							C/R	C/R	C/R	C/R			
3	**กำหนดขั้นตอนปฏิบัติการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ, จัดทำแผนการประเมินความเสี่ยง**													
	- รายงานการประเมินความเสี่ยง - รายงานผลการจัดการความเสี่ยง - แผนการจัดการความเสี่ยง							C/R	C	C	C			
4	**กำหนดหรือทบทวนนโยบายและแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสารสนเทศ**													
	- นโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์ - คู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - มาตรการความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก							C/R						

	ROLES	คณะกรรมการ กนป.	คณะอนุกรรมการเทคโนโลยีสำคัญของ กนป.	ผวก.กนป.	ผู้จัดการด้านเทคโนโลยีสารสนเทศ(ท), ผช.ผอ.รวบ.(ท)	คณะทำงานระบบ ISMS	คณะทำงาน ISMS	ผคร.	ผพร.	ผอร.	ศคส.	ผบส.	หน่วย กนป.	ผู้ตร.
	Key Management Practice **Status**													
5	**พิจารณาเห็นชอบ นโยบายและแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสารสนเทศ**													
	นโยบายและแนวทางปฏิบัติเรื่องความมั่นคงปลอดภัยสารสนเทศ				A		A	R					C	
6	**พิจารณาเห็นชอบ คู่มือและมาตรการความมั่นคงปลอดภัย**													
	- คู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - มาตรการความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก					A		R	C	C	C			C
7	**จัดทำหรือทบทวนเอกสารขั้นตอนปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์**													
	คู่มือขั้นตอนปฏิบัติงานด้านรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์							C	C/R	C/R	C/R			
8	**ชื่อสาร นโยบายและแนวปฏิบัติ ฯ, คู่มือบริหารจัดการฯ , คู่มือขั้นตอนปฏิบัติงานฯ, มาตรการความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก**													
	รายงาน การรับรู้นโยบาย และ ผลการดำเนินงานตามคู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์						I	C/R	C/R	C	C			R
9	**ดำเนินการตามมาตรฐานการควบคุมระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์**													
	รายงานผลการดำเนินงานตามมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและไซเบอร์					I			R	R	R			



ROLES / Key Management Practice	Status	คณะกรรมการ กนม.	คณะอนุกรรมการเทคโนโลยีดิจิทัลของ กนม.	ผวก.กนม.	ผู้บริหารสายงานเทคโนโลยีดิจิทัล รวก.(ท), ชวก.(ท)	คณะกรรมการ ISMS	คณะทำงาน ISMS	ผคส.	ผพส.	ผบท.	ผสส.	ผบส.	พนักงาน กนม.	คู่สัญ
10 ตรวจสอบการดำเนินการตามเกณฑ์วัดเป้าหมายความมั่นคงปลอดภัยสารสนเทศ														
ข้อเสนอแนะเพื่อนำไปปรับปรุง					C	R								
11 ตรวจประเมินภายใน (Internal Audit) ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ														
รายงานผลการตรวจประเมิน					C	A		C/R	C	C	R			

R	Responsible	Assigned to complete the task or deliverable.
A	Accountable	Has final decision-making authority and accountability for completion. Only 1 per task.
C	Consulted	An adviser, stakeholder, or subject matter expert who is consulted before a decision or action.
I	Informed	Must be informed after a decision or action.
I/C		

10. การสื่อสารและการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการ

ผู้ถ่ายทอดสาร/ผู้รับผิดชอบ	ผู้รับสาร	ประเด็นสื่อสาร	ระดับการเข้าร่วม	รูปแบบ/วิธีการ/ช่องทางการสื่อสาร			การประเมินการรับรู้	
				ภายใน	ภายนอก	กำหนดเวลา	วิธีการประเมิน	กำหนดเวลา
คณะทำงาน ISMS, ฝคท.	- คณะกรรมการ กปน. - คณะอนุกรรมการเทคโนโลยีดิจิทัล ของ กปน. - คณะกรรมการ ISMS	- ทบทวนนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - ทบทวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	- การให้คำปรึกษา - การให้ข้อมูล	การประชุม		เมื่อมีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละครั้ง	รายงานการประชุมคณะทำงานฯ และคณะกรรมการฯ	ไตรมาสที่ 3
คณะทำงาน ISMS, ฝคท.	- หน่วยงานผู้ดูแลระบบ ได้แก่ ฝคท., ฝพท., ฝยท.	- นโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์ - คู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - แนวปฏิบัติงานด้านรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - มาตรการความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก	- การให้ข้อมูล - การมีส่วนร่วม	- Intranet, สารบรรณอิเล็กทรอนิกส์ - ระบบ Informa เก็บระเบียบนโยบายและคู่มือ		ปีละ 1 ครั้ง	จัดเก็บเอกสารคู่มือแนวปฏิบัติเข้าสู่ระบบ Infoma	ไตรมาสที่ 3

ผู้ถ่ายทอดสาร/ผู้รับผิดชอบ	ผู้รับสาร	ประเด็นสื่อสาร	ระดับการเข้าร่วม	รูปแบบ/วิธีการ/ช่องทางการสื่อสาร			การประเมินการรับรู้	
				ภายใน	ภายนอก	กำหนดเวลา	วิธีการประเมิน	กำหนดเวลา
คณะทำงาน ISMS, ฝคท.	ผู้ปฏิบัติงาน	- นโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศและไซเบอร์ - การสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์		- Intranet, สารบรรณอิเล็กทรอนิกส์ - การฝึกอบรม		ปีละ 1 ครั้ง	ประเมินผลการอบรม	ไตรมาสที่ 4
คณะทำงาน ISMS, ฝคท.	คู่ค้า	- นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third Party Access Control Policy)		- ระบุใน TOR - ประชุม Kick-off		ทุกครั้งที่มีการว่าจ้างผู้ให้บริการภายนอก	การลงนามของคู่ค้าในการยอมรับนโยบายการควบคุมหน่วยงานภายนอกข้าถึงระบบเทคโนโลยีสารสนเทศ จากการประชุม Kick-off หรือลงนามในสัญญา ที่มีนโยบายฯ ระบุไว้ใน TOR	ไตรมาสที่ 4

11. การวัด ติดตาม วิเคราะห์ ประเมินผล ตัววัดผลลัพธ์ กระบวนการการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร

การประเมินประสิทธิผลของกระบวนการการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ขององค์กร ดังต่อไปนี้

11.1 ตัวชี้วัด การตรวจสอบและประเมินความเสี่ยงความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์

ตัวชี้วัดที่ 1	ความสำเร็จในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ (ข้อ 5.2 และ 5.3)
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กขม.ฝคท.)
ข้อมูลประกอบตัววัด	รายงานการประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ และ รายงานปิดการตรวจสอบการด้านสารสนเทศและไซเบอร์
ความถี่ในการติดตาม	ปีละ 1 ครั้ง

11.2 ตัวชี้วัด การบริหารองค์กรและทรัพยากรมนุษย์เพื่อการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

ตัวชี้วัดที่ 2	ความสำเร็จในการสร้างความตระหนักและการเผยแพร่ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ให้กับพนักงานตามเวลาที่กำหนด
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กขม.ฝคท.)
ข้อมูลประกอบตัววัด	- การฝึกอบรมปฐมนิเทศพนักงานใหม่ประจำปี - การอบรมการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ - การเผยแพร่นโยบายและแนวปฏิบัติฯ ผ่านเวบไซต์ หรือการประชุม
ความถี่ในการติดตาม	อย่างน้อยปีละ 1 ครั้ง

11.3 ตัวชี้วัด การจัดการทรัพย์สินสารสนเทศ

ตัวชี้วัดที่ 3 **(outcome)**	ความสำเร็จในการทบทวนคู่มือการจัดการทรัพย์สินสารสนเทศภายใน ไตรมาสที่ 3 ของปีงบประมาณ
ผู้ติดตาม วัดผล	กองทรัพย์สินเทคโนโลยีดิจิทัล ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	รายงานผลการทบทวนคู่มือการจัดการทรัพย์สินสารสนเทศ
ความถี่ในการติดตาม	อย่างน้อยปีละ 1 ครั้ง
เป้าหมาย	ทบทวนแล้วเสร็จภายในไตรมาสที่ 3

หรือ

ตัวชี้วัดที่ 3 **(output)**	ร้อยละการปรับปรุงหรือตรวจสอบระเบียนสินทรัพย์ใน 12 เดือนที่ผ่านมา
ผู้ติดตาม วัดผล	กองทรัพย์สินเทคโนโลยีดิจิทัล ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	รายงานผลการตรวจนับทรัพย์สิน
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.4 ตัวชี้วัด การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ตัวชี้วัดที่ 4	ความสำเร็จในการเผยแพร่แนวปฏิบัติความรับผิดชอบของผู้ใช้งาน ในการใช้งานรหัสผ่าน (Password Use)
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กขม.ฝคท.)
ข้อมูลประกอบตัววัด	- การสำรวจการรับรู้นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยและไซเบอร์ - การอบรมพนักงานงานใหม่
ความถี่ในการติดตาม	อย่างน้อยปีละ 1 ครั้ง
เป้าหมาย	ภายในเดือนกันยายน ของปีงบประมาณ

11.5 ตัวชี้วัด การใช้งานอุปกรณ์พกพา

ตัวชี้วัดที่ 5 **(output)**	ร้อยละของการลงทะเบียน Mac Address ของอุปกรณ์พกพาที่นำมาใช้ภายในองค์กร
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กขม.ฝคท.)
ข้อมูลประกอบตัววัด	ข้อมูลจากในระบบ Wireless Monitoring
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.6 ตัวชี้วัด การควบคุมการเข้าถึงข้อมูลสารสนเทศ

ตัวชี้วัดที่ 6	ร้อยละของผู้ใช้งานที่มีสิทธิเข้าถึงตามหน้าที่ความรับผิดชอบ ของระบบงานสำคัญ เช่น CIS
ผู้ติดตาม วัดผล	กองปฏิบัติการสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กปก.ฝคท.)
ข้อมูลประกอบตัววัด	รายงานการสร้าง แก้ไข และระงับสิทธิ์การใช้งาน ผู้ใช้งานระบบ CIS WEB
ความถี่ในการติดตาม	รายไตรมาส
เป้าหมาย	100%

11.7 ตัวชี้วัด การบริหารจัดการการเข้าถึงของผู้ใช้งาน

ตัวชี้วัดที่ 7	ร้อยละของพนักงานที่เข้าใช้งานระบบสารสนเทศพื้นฐานขององค์กร
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กขม.ฝคท.)
ข้อมูลประกอบตัววัด	ข้อมูลการเข้าใช้งานเครื่องคอมพิวเตอร์ด้วย Active Directory
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.8 ตัวชี้วัด การควบคุมการเข้าถึงระบบเครือข่าย

ตัวชี้วัดที่ 8.1	ร้อยละของพนักงานเข้าใช้งานระบบเครือข่ายเป็นรายบุคคล
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กขม.ฝคท.)
ข้อมูลประกอบตัววัด	ข้อมูลการเข้าใช้งานระบบเครือข่าย Internet Web Authentication ด้วยรหัสประจำตัวของแต่ละบุคคล
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

หรือ

ตัวชี้วัดที่ 8.2	ร้อยละของการจัดเก็บบัญชีการเชื่อมต่อเครือข่ายของ กปน.
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กขม.ฝคท.)
ข้อมูลประกอบตัววัด	ข้อมูลรายละเอียดของบัญชีผู้ขอใช้บริการเครือข่าย ได้แก่ คอมพิวเตอร์ที่ขอใช้บริการ, IP Address และ สถานที่ติดตั้ง เป็นต้น
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.9 ตัวชี้วัด การควบคุมการเข้าถึงระบบปฏิบัติการ

ตัวชี้วัดที่ 9	ร้อยละของพนักงานในการปฏิบัติตามแนวทางบริหารการจัดการรหัสผ่านในการเข้าใช้งาน Operating System
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กขม.ฝคท.))
ข้อมูลประกอบตัววัด	- พนักงานทราบว่ารหัสผ่าน Active Directory มีอายุใช้งาน 90 วันและมีการแจ้งให้ผู้ใช้งานเปลี่ยนโดยอัตโนมัติ - พนักงานทราบว่ารหัสผ่านต้องมีความยากต่อการคาดเดา
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.10 ตัวชี้วัด การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่นและสารสนเทศ

ตัวชี้วัดที่ 10	ร้อยละของของผู้ใช้งานทราบถึงการจำกัดการเข้าถึงสารสนเทศ
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กขม.ฝคท.)
ข้อมูลประกอบตัววัด	ผลการรับรู้แนวปฏิบัติในการเข้าถึง Application ตามสิทธิของผู้ใช้งาน ในหน้าที่และความรับผิดชอบ และได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.11 ตัวชี้วัด การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ตัวชี้วัดที่ 11	ร้อยละของบุคคลภายนอกที่มีการควบคุมการเข้าพื้นที่ควบคุมความปลอดภัย
ผู้ติดตาม วัดผล	กองทรัพย์สินเทคโนโลยีดิจิทัล ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	- แบบฟอร์ม IT.FRM.009 ขอเข้าปฏิบัติงานในคอมพิวเตอร์สำหรับบุคคลภายนอก - แบบฟอร์ม IT.FRM.010 บันทึกเข้า-ออกศูนย์คอมพิวเตอร์
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.12 ตัวชี้วัด การควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์ (Data Center Policy)

ตัวชี้วัดที่ 12	ร้อยละของผู้ปฏิบัติงานที่มีการระบุสิทธิบุคคลที่มีการเข้า-ออกพื้นที่ปฏิบัติงาน Data Center
ผู้ติดตาม วัดผล	กองทรัพย์สินเทคโนโลยีดิจิทัล ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	- มี 2 Factor Authentication และ 2 person Authentication คือการใช้บัตรพนักงานที่ได้รับการ Authorized และผู้ดูแล Data Center ควบคุมการเข้า Data Center - แบบฟอร์ม IT.FRM.010 บันทึกเข้า-ออกศูนย์คอมพิวเตอร์
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.13 ตัวชี้วัด การเข้ารหัสข้อมูลสารสนเทศ

ตัวชี้วัดที่ 13	ร้อยละของข้อมูลสำคัญที่มีการรับ-ส่งผ่านระบบเครือข่ายมีการเข้ารหัสข้อมูล เช่น ระบบ CIS ข้อมูลที่มีการับ-ส่งกับหน่วยงานภายนอก
ผู้ติดตาม วัดผล	กองปฏิบัติการสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กปก.ฝคท.)
ข้อมูลประกอบตัววัด	รายการข้อมูลที่มีการเข้ารหัส
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.14 ตัวชี้วัด การสำรองและกู้คืนข้อมูล

ตัวชี้วัดที่ 14	ความสำเร็จในการทบทวนคู่มือและการกู้คืนข้อมูล
ผู้ติดตาม วัดผล	กองบริหารเครือแม่ข่าย ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	- รายงานการทบทวนคู่มือปฏิบัติงานการสำรองและการกู้คืนข้อมูล - รายงานการสำรองข้อมูลสำคัญ
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	ทบทวนแล้วเสร็จภายในเดือนกันยายน

11.15 ตัวชี้วัด การควบคุมการใช้งานระบบเครือข่ายอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

ตัวชี้วัดที่ 15	ร้อยละของผู้ใช้งานรับทราบแนวปฏิบัติในการควบคุมการใช้งานเครือข่ายอินเทอร์เน็ตและ E-mail
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	การสำรวจการรับรู้และการเผยแพร่นโยบายและแนวปฏิบัติด้านการใช้งานเครือข่ายและ E-mail
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	70%

11.16 ตัวชี้วัด การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ตัวชี้วัดที่ 16	ร้อยละของผู้ใช้งานที่ต้องมีการยืนยันตัวตนทุกครั้งก่อนเข้าระบบเครือข่ายไร้สาย
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	การเข้าถึงระบบเครือข่ายด้วยบัญชีผู้ใช้งานและรหัสผ่านจากระบบ Active Directory
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.17 ตัวชี้วัด การควบคุมความปลอดภัยของกระบวนการจัดหา พัฒนาและบำรุงดูแลระบบสารสนเทศ

ตัวชี้วัดที่ 17	ร้อยละของระบบใหม่ที่พัฒนาขึ้นซึ่งตรงตามข้อกำหนดด้านความปลอดภัยที่กำหนดไว้ล่วงหน้า
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กขม.ฝคท.)
ข้อมูลประกอบตัววัด	การกำหนด ข้อกำหนดด้านความปลอดภัยไว้ในรายละเอียดและขอบเขตงาน
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.18 ตัวชี้วัด การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

ตัวชี้วัดที่ 18	ร้อยละของผู้ให้บริการภายนอกที่ปฏิบัติตามมาตรฐาน ข้อบังคับ และข้อตกลงขององค์กร
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	หน่วยงานภายนอกรับทราบแนวปฏิบัติ ข้อบังคับ ข้อตกลงในการเข้าปฏิบัติงานในพื้นที่ของ กปน. จากข้อกำหนดด้านความปลอดภัยที่กำหนดไว้ในรายละเอียดและขอบเขตของงาน และจากการสำรวจการรับรู้นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยและไซเบอร์ของกปน.
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100%

11.19 ตัวชี้วัด การบริหารจัดการเหตุการณ์ด้านความปลอดภัยสารสนเทศ

ตัวชี้วัดที่ 19	ความสำเร็จในการรายงานผลการเฝ้าระวังภัยคุกคามที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ภายในเวลาที่กำหนด
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	รายงานสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดเรื่องการเก็บ Log, การเฝ้าระวังและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยสารสนเทศ
ความถี่ในการติดตาม	เดือนละ 1 ครั้ง
เป้าหมาย	รายงานภายใน 7 วันทำการของเดือนถัดไป

11.20 ตัวชี้วัด การบริหารความต่อเนื่องและพร้อมใช้ของระบบสารสนเทศอย่างปลอดภัย

ตัวชี้วัดที่ 20	ความสำเร็จในการซ้อมแผนการรองรับการดำเนินการธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) (รายงานตามข้อ 6.4)
ผู้ติดตาม วัดผล	คณะทำงาน BCP
ข้อมูลประกอบตัววัด	รายงานสรุปผลการซ้อมแผนการรองรับการดำเนินการธุรกิจอย่างต่อเนื่อง
ความถี่ในการติดตาม	เดือนละ 1 ครั้ง
เป้าหมาย	ซ้อมฯตามแผนแล้วเสร็จภายในเดือน ก.ย.

11.21 ตัวชี้วัด การรักษาความมั่นคงปลอดภัยทางไซเบอร์

ตัวชี้วัดที่ 21	ความสำเร็จในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ภายในเวลาที่กำหนด
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	ผลการอบรมพนักงานด้านการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์
ความถี่ในการติดตาม	อย่างน้อยปีละ 1 ครั้ง
เป้าหมาย	อบรมภายในไตรมาสที่ 3

11.22 ตัวชี้วัด การปฏิบัติตามข้อบังคับ

ตัวชี้วัดที่ 22	ร้อยละการรับทราบข้อบังคับด้านกฎหมายเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
ผู้ติดตาม วัดผล	กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล (กสท.ฝคท.)
ข้อมูลประกอบตัววัด	การสำรวจการรับรู้ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	80%

แนวทางการนำตัวชี้วัดไปประเมินผลการปฏิบัติงานทุกระดับในสายงานเทคโนโลยีดิจิทัล และรายงานผลในระบบ COACH ทุกปี ดังนี้

ระบบในตัวชี้วัดประเภท **ตัวชี้วัดงานตามภารกิจของหน่วยงานและหน้าที่ความรับผิดชอบ**

ตัวชี้วัด	คำจำกัดความหรือสูตรการคำนวน
ความสำเร็จในการติดตาม การวัดผล การรายงานผลของการปฏิบัติได้ตามแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ได้ครบถ้วน	วัดสามารถดำเนินการตามนโยบายและแนวปฏิบัติได้ครบถ้วน โดยกำหนดค่าเกณฑ์วัด ดังนี้ คะแนนระดับ 5 : ดำเนินการตามแนวปฏิบัติได้ครบถ้วน 22 แนวปฏิบัติ คะแนนระดับ 4 : ดำเนินการตามแนวปฏิบัติได้ 18 แนวปฏิบัติ หรือ 80% คะแนนระดับ 3 : ดำเนินการตามแนวปฏิบัติได้ 15 แนวปฏิบัติ หรือ 70% คะแนนระดับ 2 : ดำเนินการตามแนวปฏิบัติได้ 11 แนวปฏิบัติ หรือ 50% คะแนนระดับ 1 : ดำเนินการตามแนวปฏิบัติได้ต่ำกว่า 11 แนวปฏิบัติ หรือต่ำกว่า 50%

12. การนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน การกำกับดูแลด้านการบริหารจัดการดิจิทัล / จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) การนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้เพื่อนำไปปรับปรุงและทำนวัตกรรม

12.1 มีการรายงานผลการชี้วัดในระบบการประเมินขององค์กร และนำเสนอต่อคณะกรรมการที่เกี่ยวข้อง

12.2 มีการทบทวนกระบวนการด้านการบริหารความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ แล้วนำไปใช้กับระบบงานสำคัญอื่นๆ ที่นอกเหนือจากขอบเขตงานเดิม

12.3 นำผลที่ได้จากการประเมินไปเรียนรู้และจัดการความรู้ โดยการจัดประชุมเพื่อแลกเปลี่ยนความรู้นำไปปรับปรุงกระบวนการและจัดทำนวัตกรรมของกระบวนการ ปีละครั้ง

13. เอกสารที่เกี่ยวข้อง

- นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
- แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของการประปานครหลวง
- คู่มือการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (ISMS Manual)