



**แผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนา  
ระบบโครงสร้างพื้นฐานและระบบความมั่นคง  
ปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร  
ของอาคารรัฐสภา  
ประจำปีงบประมาณ พ.ศ.๒๕๖๔**

คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัย  
ด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๕ ปี  
(พ.ศ. ๒๕๖๒-๒๕๖๕)

## สารบัญ

บทที่	เรื่อง	หน้า
๑	สาระสำคัญ	๑
๒.	วัตถุประสงค์	๒
๓.	แผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ - ๒๕๖๕)	๒
๔.	เป้าหมายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๔	๕
๕.	เป้าหมายการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒ - ๒๕๖๕)	๖
๖.	เป้าหมายในการขับเคลื่อนแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบ โครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของอาคารรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๔	๑๐
๗.	กรอบตัวชี้วัดการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ พ.ศ.๒๕๖๔	๑๑
๘.	แผนปฏิบัติการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔	๑๔
	ภาคผนวก	๒๑
	- คำสั่งแต่งตั้งคณะกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยี สารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕)	

## ๑. สาระสำคัญ

แผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ เป็นแผนปฏิบัติการที่จัดทำขึ้นมาเพื่อใช้เป็นกรอบแนวทางการดำเนินงานตามตัวชี้วัดที่ ๑.๔.๒ ตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ซึ่งกำหนดให้มีการประเมินประสิทธิผลการปฏิบัติราชการเป็นประจำทุกปี สำหรับตัวชี้วัดดังกล่าวนี้เป็นตัวชี้วัดร่วมของหน่วยงานด้านเทคโนโลยีสารสนเทศสังกัดรัฐสภา ได้แก่ สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร และสำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา ซึ่งเป็นหน่วยงานหลัก และเป็นเจ้าภาพร่วมในการรายงานผลการดำเนินการด้านการพัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากลเพื่อรองรับการปฏิบัติงานสำหรับอาคารรัฐสภา โดยในปีงบประมาณ ๒๕๖๔ ได้กำหนดแผนงาน โครงการ กิจกรรมในการขับเคลื่อนการดำเนินงานตามแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕) ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากล และแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ ๔ ปี (๒๕๖๒-๒๕๖๕) เพื่อให้ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา มีประสิทธิภาพ และมีความมั่นคงปลอดภัย เป็นไปตามมาตรฐานสากล มีความพร้อมรองรับกับการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศที่จะเกิดขึ้นที่มีผลกระทบต่อองค์กร รวมทั้งรองรับกับการปฏิบัติงานในอาคารรัฐสภา และการสนับสนุนการปฏิบัติงานในกระบวนการนิติบัญญัติได้อย่างมีประสิทธิภาพ มีความทันสมัย และสอดคล้องกับแนวนโยบายของรัฐสภา และเป็นกรอบกำหนดทิศทางของการรักษาความมั่นคงปลอดภัย และเป็นเครื่องมือในการป้องกันไม่ให้เกิดความเสียหายต่อระบบสารสนเทศและการสื่อสารของรัฐสภาต่อไป

## ๒. วัตถุประสงค์

๑) เพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา มีแผนปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ซึ่งจะเป็นกรอบแนวทางการดำเนินการด้านการรักษาความปลอดภัย ให้เป็นไปตามสากลที่สอดคล้องกับแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ ๔ ปี (๒๕๖๒-๒๕๖๕)

๒) เพื่อให้หน่วยงานด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา มีความมั่นคงปลอดภัยในอันที่จะสร้างความรู้ ความเข้าใจและความเชื่อมั่นแก่สมาชิกรัฐสภา และบุคลากรในวงงานของรัฐสภา

๓) เพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา มีแผนงานโครงการและการติดตามประเมินผลในการขับเคลื่อนการดำเนินงานด้านระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารตามกรอบตัวชี้วัดตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ ๒๕๖๔

## ๓. แผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕)

### วิสัยทัศน์

“รัฐสภาดิจิทัล (Digital Parliament)”

หมายถึง องค์กรที่สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลได้อย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใด เพื่อสนับสนุนงานด้านนิติบัญญัติ

### พันธกิจ

๑. พัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้ผู้รับบริการและประชาชนได้รับข้อมูลสารสนเทศของรัฐสภาที่ถูกต้อง รวดเร็ว และทันสมัย ตรงกับความต้องการ

๒. พัฒนาและส่งเสริมสมาชิกรัฐสภา และบุคคลในวงงานรัฐสภาให้รู้เท่าทัน การใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างสร้างสรรค์

### เป้าประสงค์เชิงยุทธศาสตร์

๑. ระบบข้อมูลและสารสนเทศของรัฐสภา มีการเชื่อมโยงและบูรณาการเพื่อให้บริการอย่างมีประสิทธิภาพ

๒. ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา มีประสิทธิภาพ และมีความมั่นคงปลอดภัย เป็นไปตามมาตรฐานสากล

๔. สมาชิกรัฐสภาและบุคคลในวงงานรัฐสภาผู้เท่าทัน สามารถใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสาร อย่างสร้างสรรค์

๕. ผู้รับบริการและประชาชนได้รับข้อมูลสารสนเทศของรัฐสภาที่ถูกต้อง รวดเร็ว และทันสมัย ตรงกับความต้องการ

**ยุทธศาสตร์ของแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕) มีดังนี้**

๑. พัฒนาระบบและบูรณาการข้อมูลมุ่งสู่การเป็น Digital Parliament
๒. พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากล
๓. ส่งเสริมและสนับสนุน ให้สมาชิกรัฐสภา และบุคคลในวงงานรัฐสภา มีความรู้ ความสามารถ และทักษะในการประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ

**การเชื่อมโยงความสัมพันธ์ระหว่างยุทธศาสตร์ กลยุทธ์ และเป้าประสงค์เชิงยุทธศาสตร์**

ยุทธศาสตร์	กลยุทธ์	เป้าประสงค์เชิงยุทธศาสตร์
ยุทธศาสตร์ที่ ๑ พัฒนาระบบ และบูรณาการข้อมูลมุ่งสู่การเป็น Digital Parliament	๑.๑ พัฒนาระบบและบูรณาการ ข้อมูลมุ่งสู่การเป็น Digital Parliament	ระบบข้อมูลและสารสนเทศของรัฐสภา มีการเชื่อมโยงและบูรณาการ เพื่อให้บริการอย่างมีประสิทธิภาพ
	๑.๒ พัฒนาระบบบริการด้าน สารสนเทศ ให้มีข้อมูลที่ถูกต้อง ทันสมัย รองรับความต้องการของผู้รับบริการและประชาชน	ผู้รับบริการและประชาชนได้รับ ข้อมูลสารสนเทศของรัฐสภาที่ ถูกต้อง รวดเร็ว และทันสมัย ตรงกับ ความต้องการ
ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้าง พื้นฐาน และระบบความมั่นคง ปลอดภัยด้านเทคโนโลยี สารสนเทศและการสื่อสาร ให้ เป็นไปตามมาตรฐานสากล	๒.๑ พัฒนาโครงสร้างพื้นฐานด้าน เทคโนโลยีสารสนเทศและการ สื่อสารของรัฐสภา	ระบบโครงสร้างพื้นฐานด้าน เทคโนโลยีสารสนเทศและการ สื่อสารของรัฐสภา มีประสิทธิภาพ และมีความมั่นคงปลอดภัย เป็นไป ตามมาตรฐานสากล
	๒.๒ พัฒนาระบบความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ให้เป็นไปตาม มาตรฐานสากลรองรับการ	

ยุทธศาสตร์	กลยุทธ์	เป้าประสงค์เชิงยุทธศาสตร์
	ให้บริการได้อย่างทั่วถึงและเท่าเทียม	
ยุทธศาสตร์ที่ ๓ ส่งเสริมและสนับสนุน ให้สมาชิกรัฐสภา และบุคคลในวงงานรัฐสภา มีความรู้ความสามารถ และทักษะในการประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ	๓.๑ พัฒนาสมรรถนะบุคลากรของรัฐสภาด้าน การใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร	สมาชิกรัฐสภาและบุคคลในวงงานรัฐสภา รู้เท่าทัน สามารถใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างสร้างสรรค์
	๓.๒ ส่งเสริม สนับสนุนให้สมาชิก รัฐสภาและบุคคลในวงงานของรัฐสภาใช้ระบบเทคโนโลยี สารสนเทศและการสื่อสารอย่าง สร้างสรรค์	
	๓.๓ ส่งเสริม สนับสนุนบุคลากร ให้ มีการศึกษา วิจัย และพัฒนา ทางด้านนวัตกรรมและเทคโนโลยี รองรับความต้องการของ ผู้รับบริการและประชาชน	

#### ๔. เป้าหมายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

เป้าหมายในการดำเนินงานคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ดังนี้

๑) การประเมินระบบสารสนเทศของรัฐสภา (Vulnerability Assessment) จัดทำขึ้นเพื่อหาช่องโหว่หรือจุดอ่อนของระบบสารสนเทศของรัฐสภาว่ามีช่องโหว่หรือไม่ และช่องโหว่นั้นมีระดับความรุนแรง และมีผลกระทบต่อระบบสารสนเทศของรัฐสภาอย่างไร เพื่อหาแนวทางป้องกันการถูกโจมตีจากการใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนของระบบสารสนเทศของรัฐสภาและใช้เป็นแนวทางในการพัฒนาระบบสารสนเทศของรัฐสภาให้มีความปลอดภัยมากยิ่งขึ้น

๒) แผนการตอบสนองภัยคุกคาม (Incident Response Plan) ของรัฐสภา จัดทำเพื่อตอบสนองสถานการณ์ด้านความมั่นคงปลอดภัยและเฝ้าระวังและตรวจจับเหตุการณ์ที่ผิดปกติเพื่อมาดำเนินการจัดหามาตรการที่เหมาะสม ในการตอบสนองเหตุการณ์ผิดปกติ ดังนั้นสำนักงานควรมีการกำหนดขั้นตอนการจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ยกตัวอย่างเช่น การล้มเหลวของระบบสารสนเทศ ผลกระทบจากซอฟต์แวร์ไม่ประสงค์ดี (Malicious code) การปฏิเสธการให้บริการ (Denial of Service) เป็นต้น

๓) การจัดทำทะเบียนทรัพย์สินทางด้าน ICT ของรัฐสภา (Inventory of Assets) การจัดทำบัญชีรายการทรัพย์สินของอุปกรณ์ภายในห้อง (Data Center) จะช่วยให้สำนักงานรู้ว่ามียุทธภัณฑ์ใดบ้างที่ต้องบริหารจัดการดูแลให้เกิดความมั่นคงปลอดภัยภายในห้อง (Data Center) โดยให้ความสำคัญกับทรัพย์สินที่มีผลกระทบต่อสำนักงาน สามารถนำนโยบายในการบริหารจัดการอุปกรณ์ภายในห้อง (Data Center)

๔) การทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา โดยจะมีการทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารเมื่อย้าย (Data Center) จากสำนักงานเลขาธิการสภาผู้แทนราษฎร และสำนักงานเลขาธิการวุฒิสภาไปยังอาคารรัฐสภา ศึกษากาย ในการดำเนินงานด้าน (Data Center) ของส่วนราชการสังกัดรัฐสภาาร่วมกัน

๕) กิจกรรมเสริมสร้างการเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Information Security) เพื่อรองรับการก้าวสู่มาตรฐาน ISO ๒๗๐๐๑ : ๒๐๑๓ (Data Center) ของรัฐสภา

๕. เป้าหมายการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕)

เป้าหมายการดำเนินงาน			
ปีงบประมาณ ๒๕๖๒	ปีงบประมาณ ๒๕๖๓	ปีงบประมาณ ๒๕๖๔	ปีงบประมาณ ๒๕๖๕
<p>๑. จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา ประกาศเมื่อวันที่ ๑ ตุลาคม ๒๕๖๒</p> <p>๒. สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยระบบสารสนเทศให้กับผู้ใช้งาน</p> <p>๓. มีระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ทันสมัยสำหรับอาคารรัฐสภาแห่งใหม่</p> <p>๔. แนวทางการเตรียมความพร้อมด้านระบบเทคโนโลยีสารสนเทศสำหรับอาคารรัฐสภา เกียกกาย</p>	<p>๑. จัดทำแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา สำนักงานเลขาธิการสภาผู้แทนราษฎร ประกาศเมื่อวันที่ ๑๖ กันยายน ๒๕๖๓ สำนักงานเลขาธิการวุฒิสภา ประกาศเมื่อวันที่ ๒๗ สิงหาคม ๒๕๖๓</p> <p>๒. ผู้ใช้งานได้รับความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p> <p>๓. ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความ</p>	<p>๑. ประเมินความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภาโดยหน่วยงานเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา</p> <p>๒. ทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา และทดสอบ</p> <p>๓. ผู้ใช้งานได้รับความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p> <p>๔. การประเมินระบบสารสนเทศของรัฐสภา (Vulnerability Assessment)</p>	<p>๑. ประเมินความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภาโดยหน่วยงานภายนอก</p> <p>๒. ได้รับการประเมินความมั่นคงปลอดภัยตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๑๓</p>



เป้าหมายการดำเนินงาน			
ปีงบประมาณ ๒๕๖๒	ปีงบประมาณ ๒๕๖๓	ปีงบประมาณ ๒๕๖๔	ปีงบประมาณ ๒๕๖๕
<p>สำนักงานเลขาธิการสภาผู้แทนราษฎร ประกาศเมื่อวันที่ ๒๕ กันยายน ๒๕๖๒</p> <p>สำนักงานเลขาธิการวุฒิสภา ประกาศเมื่อวันที่ ๓๐ กันยายน ๒๕๖๒</p>	<p>มั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p> <p>๔. ประเมินความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p> <p>๕. จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan) สำนักงานเลขาธิการสภาผู้แทนราษฎร ประกาศเมื่อวันที่ ๑๖ กันยายน ๒๕๖๓</p> <p>สำนักงานเลขาธิการวุฒิสภา ประกาศเมื่อวันที่ ๒๗ สิงหาคม ๒๕๖๓</p> <p>๖. จัดทำแผนต่อเนืองการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Business Continuity Plan) สำนักงานเลขาธิการสภาผู้แทนราษฎร ประกาศเมื่อวันที่ ๑๖ กันยายน ๒๕๖๓</p>	<p>๕. แผนการตอบสนองภัยคุกคาม (Incident Response Plan) ของรัฐสภา</p> <p>๖) การจัดทำทะเบียนทรัพย์สินทางด้าน ICT ของรัฐสภา (Inventory of Assets)</p> <p>๗) การทบทวนแผนต่อเนืองการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา</p> <p>๘) กิจกรรมเสริมสร้างการเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Information Security) เพื่อรองรับการก้าวสู่มาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ (Data Center) ของรัฐสภา</p>	

เป้าหมายการดำเนินงาน			
ปีงบประมาณ ๒๕๖๒	ปีงบประมาณ ๒๕๖๓	ปีงบประมาณ ๒๕๖๔	ปีงบประมาณ ๒๕๖๕
	<p>สำนักงานเลขาธิการวุฒิสภา ประกาศเมื่อวันที่ ๒๗ สิงหาคม ๒๕๖๓</p> <p>๗.ระบบเทคโนโลยีสารสนเทศและ การสื่อสารของอาคารรัฐสภาแห่ง ใหม่ (ระบบความมั่นคงปลอดภัย) ประกอบด้วย</p> <p>๗.๑ ระบบรักษาความปลอดภัยด้าน เทคโนโลยีสารสนเทศ (IT Security)</p> <p>๗.๒ ระบบบริหารจัดการตัวตน ผู้ใช้งาน (Identity Management)</p> <p>๗.๓ Network Operating Center (NOC) ศูนย์ปฏิบัติการเครือข่าย</p> <p>๗.๔ Security Operation Center (SOC) ศูนย์ปฏิบัติการการรักษา ความมั่นคงปลอดภัยทาง คอมพิวเตอร์ _</p> <p>๘. การประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ของ ระบบสารสนเทศของรัฐสภา จำนวน ๓ ระบบ ได้แก่ ระบบ บริหารการประชุมรัฐสภา ระบบ</p>		

เป้าหมายการดำเนินงาน			
ปีงบประมาณ ๒๕๖๒	ปีงบประมาณ ๒๕๖๓	ปีงบประมาณ ๒๕๖๔	ปีงบประมาณ ๒๕๖๕
	<p>บริหารจัดการห้องประชุมอัจฉริยะ</p> <p>ระบบบริหารจัดการเอกสารการ</p> <p>ประชุมดิจิทัล</p> <p>๙. การจัดฝึกอบรมให้ความรู้</p> <p>เกี่ยวกับความมั่นคงปลอดภัย</p> <p>(Information Security</p> <p>Awareness) แก่บุคลากรด้าน</p> <p>สารสนเทศของรัฐสภา ซึ่งมี</p> <p>รายละเอียดหลักสูตร ประกอบด้วย</p> <p>ความตระหนักในความมั่นคง</p> <p>ปลอดภัยด้านสารสนเทศ</p> <p>(Information Security</p> <p>Awareness) ความรู้ความเข้าใจใน</p> <p>นโยบายและแนวปฏิบัติในการรักษา</p> <p>ความมั่นคงปลอดภัยด้าน</p> <p>สารสนเทศของรัฐสภา ความรู้</p> <p>ความเข้าใจเกี่ยวกับพระราชบัญญัติ</p> <p>ว่าด้วยการกระทำความผิดเกี่ยวกับ</p> <p>คอมพิวเตอร์</p>		

๖. เป้าหมายในการขับเคลื่อนแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

๑) การประเมินระบบสารสนเทศของรัฐสภา (Vulnerability Assessment)

๒) แผนการตอบสนองภัยคุกคาม (Incident Response Plan) ของรัฐสภา

๓) การจัดทำทะเบียนทรัพย์สินทางด้าน ICT ของรัฐสภา (Inventory of Assets)

๔) การทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา

๕) กิจกรรมเสริมสร้างการเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Information Security)

๗. กรอบตัวชี้วัดการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

ตัวชี้วัดที่ ๑.๔ ระดับความสำเร็จของการพัฒนาเทคโนโลยีสารสนเทศเพื่อมุ่งสู่รัฐสภาดิจิทัล (Digital Parliament)

ตัวชี้วัด	น้ำหนัก	เกณฑ์การให้คะแนน				
		๑	๒	๓	๔	๕
ตัวชี้วัดที่ ๑.๔.๑ ระดับความสำเร็จของการพัฒนาระบบสารสนเทศเพื่อรองรับอาคารรัฐสภา	๕	๑	๒	๓	๔	๕
ตัวชี้วัดที่ ๑.๔.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา	๕	๑	๒	๓	๔	๕
ตัวชี้วัดที่ ๑.๔.๓ การพัฒนาทักษะด้านดิจิทัล (Digital Skill) ของข้าราชการสังกัดรัฐสภาเพื่อขับเคลื่อนไปสู่รัฐสภาดิจิทัล (Digital Parliament)	๕	๑	๒	๓	๔	๕

ตัวชี้วัดที่ ๑.๔.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา

รัฐสภาได้นำระบบเทคโนโลยีสารสนเทศและการสื่อสารมาเป็นเครื่องมือในการให้บริการและการปฏิบัติงาน ของส่วนราชการสังกัดรัฐสภา โดยมีการใช้งานระบบสารสนเทศอย่างแพร่หลายและต่อเนื่อง เพื่อใช้เป็นช่องทางในการดำเนินงาน ประชาสัมพันธ์ เผยแพร่ข่าวสาร ข้อมูล รวมไปถึงการอำนวยความสะดวก ในการเข้าถึงข้อมูลทั้งในด้านข่าวสาร ผ่านระบบเครือข่ายคอมพิวเตอร์ ซึ่งจากการให้บริการในรูปแบบดังกล่าวนี้มีความสำคัญเป็นอย่างยิ่งในปัจจุบันและอนาคต ในการพัฒนาระบบดังกล่าวข้างต้นมีความจำเป็นอย่างยิ่งในการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ เพื่อให้มีประสิทธิภาพ และต้องคำนึงถึงความปลอดภัย และลดความเสี่ยง ป้องกันจุดอ่อนของระบบสารสนเทศ ระบบคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายคอมพิวเตอร์ ซึ่งแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕) ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นไปตามมาตรฐานสากล ซึ่งมุ่งเน้นเรื่องระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้ผู้รับบริการมีความเชื่อมั่นกับความปลอดภัยของระบบเทคโนโลยีและการสื่อสาร ดังนั้น เพื่อให้ระบบสารสนเทศของส่วนราชการสามารถให้บริการและรองรับการปฏิบัติงานได้โดยไม่ต้องหยุด ให้บริการระบบสารสนเทศ สามารถให้บริการระบบสารสนเทศและระบบเครือข่ายได้อย่างต่อเนื่องมั่นคง และมีเสถียรภาพ โดยมีกิจกรรมที่ดำเนินการ ปี พ.ศ. ๒๕๖๔ ประกอบด้วย

- ๑) การประเมินระบบสารสนเทศของรัฐสภา (Vulnerability Assessment)
- ๒) แผนการตอบสนองภัยคุกคาม (Incident Response Plan) ของรัฐสภา
- ๓) การจัดทำทะเบียนทรัพย์สินทางด้าน ICT ของรัฐสภา (Inventory of Assets)
- ๔) การทบทวนแผนต่อเนืองการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา
- ๕) กิจกรรมเสริมสร้างการเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Information Security)

เกณฑ์การให้คะแนนเพื่อการประเมินตัวชี้วัด KPI ๑.๔.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่

ระดับคะแนน	เกณฑ์การให้คะแนน
๑	<ul style="list-style-type: none"> <li>● มีแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ โดยผ่านความเห็นชอบจากคณะกรรมการแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕)</li> </ul>
๒	<ul style="list-style-type: none"> <li>● ดำเนินการตามแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ได้ไม่น้อยกว่า ร้อยละ ๗๐</li> </ul>
๔	<ul style="list-style-type: none"> <li>● ดำเนินการตามแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ได้ไม่น้อยกว่า ร้อยละ ๘๐</li> </ul>
๔	<ul style="list-style-type: none"> <li>● ดำเนินการตามแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ได้ไม่น้อยกว่า ร้อยละ ๙๐</li> </ul>
๕	<ul style="list-style-type: none"> <li>● ดำเนินการตามแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ได้ไม่น้อยกว่า ร้อยละ ๑๐๐</li> <li>● รายงานผลการดำเนินงานเสนอต่อหัวหน้าส่วนราชการ ประกอบด้วย</li> </ul>

ระดับคะแนน	เกณฑ์การให้คะแนน
	<p>๑) รายงานผลการตรวจประเมินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา กรณีพบปัญหาด้านความมั่นคงปลอดภัยสามารถแก้ไขได้ ร้อยละ ๑๐๐</p> <p>๒) รายงานสรุปผลการดำเนินงานและปัญหาอุปสรรค ในการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา</p>

๘. แผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ และการสื่อสารของอาคารรัฐสภาแห่งใหม่ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากล  
กลยุทธ์ที่ ๒.๑ พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

ตัวชี้วัดตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

ตัวชี้วัดที่ ๑.๔.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานและระบบ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่

เป้าหมาย/กิจกรรม	ไตรมาส ๑			ไตรมาส ๒			ไตรมาส ๓			ไตรมาส ๔			ร้อยละ
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๑.แผนการตอบสนองภัยคุกคาม (Incident Response Plan) ของรัฐสภา													๒๐
๑.๑ ศึกษา มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง													๕
๑.๒ จัดทำแผนการตอบสนองภัยคุกคาม (Incident Response Plan) ของรัฐสภา													๕
๑.๓ คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคง ฯ เพื่อพิจารณา													๕
๑.๔ ขอความเห็นชอบและรายงานผลการดำเนินงานแผนการตอบสนองภัยคุกคาม (Incident Response Plan) ของรัฐสภา เสนอต่อหัวหน้าส่วนราชการผ่านคณะกรรมการขับเคลื่อนแผน Digital Parliament รัฐสภา													๕









ลำดับ		ปีงบประมาณ พ.ศ. ๒๕๖๔											
		ไตรมาส ๑			ไตรมาส ๒			ไตรมาส ๓			ไตรมาส ๔		
		(ต.ค. -ธ.ค.)			(ม.ค.-มี.ค.)			(เม.ย.-มิ.ย.)			(ก.ค.-ก.ย.)		
๕	การประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ของระบบสารสนเทศของรัฐสภา												

การดำเนินงานตามตัวชี้วัดที่ ๑.๔.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานและระบบ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา

แผนงาน/โครงการ	ตัวชี้วัด	พ.ศ. ๒๕๖๔
<p>๑. โครงการจัดทำกฎ/ระเบียบ/มาตรการ/แนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p>	<p><b>ผลผลิต :</b></p> <p>๑) แผนการตอบสนองภัยคุกคาม (Incident Response Plan) ของรัฐสภา</p> <p>๒) ทบทวนแผนต่อเนืองการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา</p> <p><b>ผลลัพธ์ :</b></p> <p>ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีความมั่นคงปลอดภัย</p>	<p>พ.ศ. ๒๕๖๔</p> <p>๑ ฉบับ</p> <p>๑ ฉบับ</p> <p>ร้อยละ ๑๐๐</p>
<p>๒ การจัดทำทะเบียนทรัพย์สินทางด้าน ICT ของรัฐสภา (Inventory of Assets)</p>	<p><b>ผลผลิต :</b></p> <p>๑) ทะเบียนทรัพย์สินทางด้าน ICT ของรัฐสภา (Inventory of Assets) (Data Center)</p> <p><b>ผลลัพธ์ :</b></p> <p>ทะเบียนทรัพย์สินทางด้าน ICT ของรัฐสภา (Inventory of Assets)</p>	<p>๑ ฉบับ</p> <p>ร้อยละ ๑๐๐</p>

แผนงาน/โครงการ	ตัวชี้วัด	พ.ศ. ๒๕๖๔
<p>๓. กิจกรรมเสริมสร้างการเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Information Security)</p>	<p><b>ผลผลิต :</b> กิจกรรมการฝึกอบรม/สัมมนา/อบรมเชิงปฏิบัติการ ซึ่งประกอบด้วยหลักสูตร ดังนี้</p> <p>๑) ความตระหนักในความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness)</p> <p>๒) ความรู้ความเข้าใจในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p> <p>๓) ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์</p> <p>๔) ความรู้เบื้องต้นมาตรฐาน ISO/IEC ๒๗๐๐๑: ๒๐๑๓</p> <p><b>ผลลัพธ์ :</b></p> <p>๑) ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจเพิ่มขึ้นและสามารถปฏิบัติตามกฎ/ระเบียบ/มาตรการ/แนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภาได้</p> <p>๒) ผู้เข้ารับการฝึกอบรมมีความพึงพอใจในการฝึกอบรม</p>	<p>พ.ศ. ๒๕๖๔</p> <p>๑ หลักสูตร ๑ หลักสูตร</p> <p>๑ หลักสูตร</p> <p>๑ หลักสูตร</p> <p>ร้อยละ ๘๐</p> <p>ร้อยละ ๘๐</p>
<p>๔. โครงการจ้างประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ระบบสารสนเทศของรัฐสภา</p>	<p><b>ผลผลิต :</b> มีรายงานการประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ระบบสารสนเทศของรัฐสภา</p> <p><b>ผลลัพธ์ :</b> รายงานการประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) สามารถกำหนดแนวทางและข้อเสนอแนะในการป้องกันการบุกรุกโจมตีระบบสารสนเทศของรัฐสภา</p>	<p>๗ ระบบ</p> <p>ร้อยละ ๑๐๐</p>

ภาคผนวก



คำสั่งคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา  
ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ - ๒๕๖๕)

ที่ ๓ /๒๕๖๒

เรื่อง แต่งตั้งคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัย  
ด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒- ๒๕๖๕)

ตามแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๒) ยุทธศาสตร์  
ที่ ๒ พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร  
ให้เป็นไปตามมาตรฐานสากล กลยุทธ์ที่ ๒.๒ พัฒนาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและ  
การสื่อสารให้เป็นไปตามมาตรฐานสากลรองรับการให้บริการได้อย่างทั่วถึงและเท่าเทียม มีเป้าประสงค์เพื่อให้  
ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภามีประสิทธิภาพและมีความมั่นคง  
ปลอดภัย เป็นไปตามมาตรฐานสากล ประกอบกับแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยี  
สารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) ซึ่งเป็นกรอบกำหนดทิศทางของ  
การรักษาความมั่นคงปลอดภัย และเป็นเครื่องมือในการป้องกันไม่ให้เกิดความเสียหายต่อระบบสารสนเทศและ  
การสื่อสารของรัฐสภา

ดังนั้น เพื่อให้การดำเนินการตามแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ.  
๒๕๖๑-๒๕๖๒) ในการทำให้ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา  
มีประสิทธิภาพและมีความมั่นคงปลอดภัย มีการดำเนินงานตามกรอบทิศทางของการรักษาความมั่นคงปลอดภัย  
จึงเห็นสมควรแต่งตั้งคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ  
และการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒- ๒๕๖๕) ประกอบด้วย

- |   |                        |
|---|------------------------|
| ๑. นายวีรชาติ มัตติทานนท์   | ที่ปรึกษาและอนุกรรมการ |
| ๒. ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานเลขาธิการวุฒิสภา                                     | ประธานอนุกรรมการ       |
| ๓. ผู้อำนวยการสำนักสารสนเทศ<br>สำนักงานเลขาธิการสภาผู้แทนราษฎร  | รองประธานอนุกรรมการ    |
| ๔. ผู้บังคับบัญชาในกลุ่มงานบริหารระบบเครือข่ายคอมพิวเตอร์<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร        | อนุกรรมการ             |
| ๕. ผู้บังคับบัญชาในกลุ่มงานบริการระบบคอมพิวเตอร์<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร                 | อนุกรรมการ             |
| ๖. ผู้บังคับบัญชาในกลุ่มงานวิทยาการคอมพิวเตอร์<br>สำนักเทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานเลขาธิการวุฒิสภา | อนุกรรมการ             |
| ๗. นายสุธี ยืนแน่นอน<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร   | อนุกรรมการ             |
| ๘. นางณัชชา ทรเพลิง<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร  | อนุกรรมการ             |

๙. นางสมคิด...



- |   |                               |
|---|-------------------------------|
| ๙. นางสมคิด แซ่ว่อง<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร                                  | อนุกรรมการ                    |
| ๑๐. นายประจักษ์ เพ็ญเลี้ยง<br>สำนักเทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานเลขาธิการวุฒิสภา         | อนุกรรมการ                    |
| ๑๑. นายทวีศักดิ์ น้อยภาษี<br>สำนักเทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานเลขาธิการวุฒิสภา          | อนุกรรมการ                    |
| ๑๒. นางสาวพัทธกานต์ วุฒิอักษรวัฒน์<br>สำนักเทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานเลขาธิการวุฒิสภา | อนุกรรมการ                    |
| ๑๓. นายสมหวัง เรืองพรชัย<br>สำนักเทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานเลขาธิการวุฒิสภา           | อนุกรรมการและเลขานุการ        |
| ๑๔. นายสุวิทย์ น้อยอยู่<br>สำนักเทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานเลขาธิการวุฒิสภา            | อนุกรรมการและผู้ช่วยเลขานุการ |
| ๑๕. นายชัยวัฒน์ ปันต่า<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร                               | อนุกรรมการและผู้ช่วยเลขานุการ |
| ๑๖. นายธนาเทพ มัชฌาโส<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร                                | อนุกรรมการและผู้ช่วยเลขานุการ |

ให้คณะอนุกรรมการ มีอำนาจหน้าที่ ดังต่อไปนี้

- กำกับ ดูแล และขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒- ๒๕๖๕) ให้เป็นไปตามเป้าหมายของแผนการรักษาความมั่นคงปลอดภัยฯ ที่กำหนดไว้แต่ละปีงบประมาณ
  - กำหนดระเบียบ ข้อปฏิบัติ และแนวทางการดำเนินการที่เกี่ยวข้อง เพื่อให้รองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา
  - ติดตาม ประเมินผลและรายงานผลการดำเนินงานต่อคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ - ๒๕๖๕) ทราบเป็นระยะ
  - แต่งตั้งคณะทำงานเพื่อดำเนินการตามที่คณะอนุกรรมการเห็นสมควร
  - ดำเนินการอื่นตามที่ได้รับมอบหมาย
- ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๕ สิงหาคม พ.ศ. ๒๕๖๒



(นางพรรษมนต์ ไทยวัฒนานุกุล)

ประธานคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament  
ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ - ๒๕๖๕)