



# แผนปฏิบัติการ

เพื่อขับเคลื่อนการดำเนินการพัฒนาระบบ  
โครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัย  
ด้านเทคโนโลยีสารสนเทศและการสื่อสารของ  
อาคารรัฐสภาแห่งใหม่

ประจำปีงบประมาณ พ.ศ.๒๕๖๕

อนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้าน  
เทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี  
[พ.ศ. ๒๕๖๒ - ๒๕๖๕]

## สารบัญ

	หน้า
๑. สารสำคัญ	๑
๒. วัตถุประสงค์	๒
๓. แผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕) และแผนรักษา ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (พ.ศ.๒๕๖๒-๒๕๖๕)	๒
๔. เป้าหมายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ประจำปีงบประมาณ ๒๕๖๕	๕
๕. กรอบตัวชี้วัดการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๕	๕
๖. แผนปฏิบัติการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยี สารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕	๑๑
ภาคผนวก	
- คำสั่งแต่งตั้งคณะกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕)	

## ๑. สาระสำคัญ

แผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ เป็นแผนปฏิบัติการที่จัดทำขึ้นมาเพื่อใช้เป็นกรอบแนวทางการดำเนินงานตามตัวชี้วัดที่ ๑.๓.๒ ตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ซึ่งกำหนดให้มีการประเมินประสิทธิผลการปฏิบัติราชการเป็นประจำทุกปี สำหรับตัวชี้วัดดังกล่าวนี้เป็นตัวชี้วัดร่วมของหน่วยงานด้านเทคโนโลยีสารสนเทศสังกัดรัฐสภา ได้แก่ สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร และสำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา ซึ่งเป็นหน่วยงานหลัก และเป็นเจ้าภาพร่วมในการรายงานผลการดำเนินการด้านการพัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากลเพื่อรองรับการปฏิบัติงานสำหรับอาคารรัฐสภา โดยในปีงบประมาณ ๒๕๖๕ 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 มีความพร้อมรองรับกับการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศที่จะเกิดขึ้น ที่มีผลกระทบต่อองค์กร รวมทั้งรองรับกับการปฏิบัติงานในอาคารรัฐสภา และการสนับสนุนการปฏิบัติงานในกระบวนการนิติบัญญัติได้อย่างมีประสิทธิภาพ มีความทันสมัย และสอดคล้องกับแนวนโยบายของรัฐสภา และเป็นกรอบกำหนดทิศทางของการรักษาความมั่นคงปลอดภัย และเป็นเครื่องมือในการป้องกันไม่ให้เกิดความเสียหายต่อระบบสารสนเทศและการสื่อสารของรัฐสภาต่อไป

## ๒. วัตถุประสงค์

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

๒) เพื่อให้งานด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภามีความมั่นคงปลอดภัยในอันที่จะสร้างความรู้ ความเข้าใจและความเชื่อมั่นแก่สมาชิกรัฐสภา และบุคลากรในวงงานของรัฐสภา

๓) เพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา มีแผนงานโครงการและการติดตามประเมินผลในการขับเคลื่อนการดำเนินงานด้านระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารตามกรอบตัวชี้วัดตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

## 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

๓. สมาชิกวุฒิสภาและบุคคลในวงงานรัฐสภารู้เท่าทัน สามารถใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสาร อย่างสร้างสรรค์

๔. 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 ให้สมาชิกวุฒิสภา 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 ให้มีข้อมูลที่ต้องการ ทันสมัย รองรับความต้องการของ ผู้รับบริการและประชาชน	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
	๒.๒ พัฒนาระบบความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ให้เป็นไปตาม มาตรฐานสากลรองรับการ	และมีความมั่นคงปลอดภัย เป็นไป ตามมาตรฐานสากล

ยุทธศาสตร์	กลยุทธ์	เป้าประสงค์เชิงยุทธศาสตร์
	ให้บริการได้อย่างทั่วถึงและเท่าเทียม	
ยุทธศาสตร์ที่ ๓ ส่งเสริมและสนับสนุน ให้สมาชิกรัฐสภา และบุคคลในวงงานรัฐสภา มีความรู้ ความสามารถ และทักษะในการประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ	๓.๑ พัฒนาสมรรถนะบุคลากรของรัฐสภาด้าน การใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสาร	สมาชิกรัฐสภาและบุคคลในวงงานรัฐสภา รู้เท่าทัน สามารถใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างสร้างสรรค์
	๓.๒ ส่งเสริม สนับสนุนให้สมาชิก รัฐสภาและบุคคลในวงงานของ รัฐสภาใช้ระบบเทคโนโลยี สารสนเทศและการสื่อสารอย่าง สร้างสรรค์	
	๓.๓ ส่งเสริม สนับสนุนบุคลากร ให้ มีการศึกษา วิจัย และพัฒนา ทางด้านนวัตกรรมและเทคโนโลยี รองรับความต้องการของ ผู้รับบริการและประชาชน	

#### แผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕)

แผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (๒๕๖๒-๒๕๖๕) จัดทำขึ้นมาเพื่อใช้เป็นกรอบกำหนดทิศทางของการรักษาความมั่นคงปลอดภัย และเป็นเครื่องมือในการป้องกันไม่ให้เกิดความเสียหายต่อระบบสารสนเทศและการสื่อสารของรัฐสภา รวมทั้งหน่วยงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภามีแผนงานโครงการและการติดตาม ประเมินผลในการขับเคลื่อนการดำเนินงานด้านระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและ

การสื่อสาร เพื่อให้งานด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภามีความมั่นคงปลอดภัย ในอันที่จะสร้างความเชื่อมั่นแก่สมาชิกรัฐสภา และบุคลากรในวงงานของรัฐสภาความผิดพลาดต่าง ๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA ๓ ประการ ได้แก่

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

ซึ่งกล่าวได้ว่าความมั่นคงปลอดภัยไซเบอร์ ถือว่ามีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้น การที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีกระบวนการในการดำเนินการ

ซึ่งกระบวนการเหล่านั้นได้ถูกกำหนดเอาไว้เป็นมาตรฐานที่เป็นที่ยอมรับ โดยมีองค์กรหรือสถาบันที่มีชื่อเสียงเป็นผู้กำหนดเกณฑ์และแนวทางในการปฏิบัติ ซึ่งองค์กรสามารถเลือกมาตรฐานที่มีความเหมาะสมกับหน่วยงานของตน และอาจเพิ่มเติมหรือยกเว้นการปฏิบัติในบางส่วนได้หากมีเหตุผลเพียงพอ จากเหตุผลข้างต้น จึงนามาสู่การจัดทำแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) ซึ่งเป็นการพัฒนามาตรฐาน การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของรัฐสภา โดยมีเป้าหมายเพื่อศึกษานโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐสภา ศึกษามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล เพื่อเสนอแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐสภาให้ได้มาตรฐานระดับสากล เป็นไปตามที่รัฐสภาได้ประกาศใช้แผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕) เพื่อนำมาใช้เป็นกรอบแนวทางการดำเนินงานตาม แผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕)

#### ๔. เป้าหมายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

##### ประจำปีงบประมาณ พ.ศ.๒๕๖๕

เป้าหมายในการดำเนินงานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ดังนี้

๔.๑ การประเมินความเสี่ยงด้วยการทดสอบเจาะระบบความปลอดภัยเทคโนโลยีสารสนเทศ (IT Penetration Testing) อุปกรณ์ (Data Center) ของรัฐสภา โดยมีการทดสอบเจาะระบบจากภายใน (Internal Penetration Testing) และการทดสอบเจาะระบบจากภายนอก (External Penetration Testing) โดยมีการจัดทำรายงานผลการทดสอบเจาะระบบ สิ่งที่ตรวจพบ ช่องโหว่/จุดอ่อน ผลกระทบ/ความเสี่ยง ข้อเสนอแนะในการแก้ไข ช่องโหว่/จุดอ่อน รวมทั้งรายงานรายละเอียดสิ่งที่ตรวจพบและวิธีการตรวจพบ (Technical Detailed Report) ข้อเสนอแนะในการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายและอุปกรณ์ (Data Center) ของรัฐสภา

๔.๒ ทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา เพื่อบริหารจัดการระบบสารสนเทศของรัฐสภาให้ดำเนินการได้อย่างต่อเนื่อง

๔.๓ ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา

๔.๔ กิจกรรมเสริมสร้างการเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Information Security) (Data Center) ของรัฐสภา ระบบการทำงานห้อง Data Center ของรัฐสภา

## ๕. กรอบตัวชี้วัดการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ ๒๕๖๕

ตัวชี้วัดที่ ๑.๓ ระดับความสำเร็จของการพัฒนาเทคโนโลยีสารสนเทศเพื่อมุ่งสู่รัฐสภาดิจิทัล (Digital Parliament)

ตัวชี้วัด	น้ำหนัก	เกณฑ์การให้คะแนน		
		๑	๓	๕
ตัวชี้วัดที่ ๑.๓.๑ ระดับความสำเร็จของการพัฒนาระบบสารสนเทศรองรับอาคารรัฐสภา	๕	๑	๓	๕
ตัวชี้วัดที่ ๑.๓.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา	๕	๑	๓	๕
ตัวชี้วัดที่ ๑.๓.๓ ระดับความสำเร็จของการพัฒนาทักษะด้านดิจิทัล (Digital Skill) ของข้าราชการสังกัดรัฐสภาเพื่อขับเคลื่อนไปสู่รัฐสภาดิจิทัล	๕	๑	๓	๕

ตัวชี้วัดที่ ๑.๓.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา

รัฐสภาได้นำระบบเทคโนโลยีสารสนเทศและการสื่อสารมาเป็นเครื่องมือในการให้บริการและการปฏิบัติงานของส่วนราชการสังกัดรัฐสภา โดยมีการใช้งานระบบสารสนเทศอย่างแพร่หลายและต่อเนื่อง เพื่อใช้เป็นช่องทางในการดำเนินงาน ประชาสัมพันธ์ เผยแพร่ข่าวสาร ข้อมูล รวมไปถึงการอำนวยความสะดวกในการเข้าถึงข้อมูล ทั้งในด้านข่าวสารผ่านระบบเครือข่ายคอมพิวเตอร์ ซึ่งจากการให้บริการในรูปแบบดังกล่าวนี้พบว่า



มีความสำคัญเป็นอย่างยิ่งในปัจจุบันและอนาคต ในการพัฒนาระบบดังกล่าวข้างต้นมีความจำเป็นอย่างยิ่ง ในการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของ อาคารรัฐสภาแห่งใหม่ เพื่อให้มีประสิทธิภาพ และต้องคำนึงถึงความปลอดภัย และลดความเสี่ยง ป้องกันจุดอ่อน ของระบบสารสนเทศ ระบบคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายคอมพิวเตอร์ ซึ่งแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕) ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้างพื้นฐาน และระบบ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นไปตามมาตรฐานสากล ซึ่งมุ่งเน้นเรื่องระบบ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้ผู้รับบริการมีความเชื่อมั่นกับความปลอดภัยของ ระบบเทคโนโลยีและการสื่อสาร และขับเคลื่อนตามเป้าหมายของแผนการรักษาความมั่นคงปลอดภัยด้าน เทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) จึงส่งผลให้เกิดการพัฒนาระบบ สารสนเทศของส่วนราชการสามารถให้บริการและรองรับการปฏิบัติงาน โดยไม่ต้องหยุดให้บริการระบบสารสนเทศ สามารถให้บริการระบบสารสนเทศและระบบเครือข่ายได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัยและมีเสถียรภาพ และมีกิจกรรมที่ดำเนินการในปีงบประมาณ พ.ศ. ๒๕๖๑-๒๕๖๕ ประกอบด้วย

๑. แผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕)

๒. นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา และแนวปฏิบัติการรักษาความ มั่นคงปลอดภัยสารสนเทศของรัฐสภา

๓. แผนการสำรองข้อมูลรัฐสภา (Back up Plan)

๔. การโอนย้ายระบบเทคโนโลยีสารสนเทศของรัฐสภา (ระบบสารสนเทศ ระบบคอมพิวเตอร์ แม่ข่าย และระบบเครือข่ายคอมพิวเตอร์)

๕. แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan)

๖. แผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Business Continuity Plan)

๗. ระบบเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา (ระบบความมั่นคงปลอดภัย) ประกอบด้วย

๗.๑ ระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

๗.๒ ระบบบริหารจัดการตัวตนผู้ใช้งาน (Identity Management)

๗.๓ Network Operating Center (NOC) ศูนย์ปฏิบัติการเครือข่าย

๗.๔ Security Operation Center (SOC) ศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทาง คอมพิวเตอร์

๘. การประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ของระบบสารสนเทศของรัฐสภา

๙. การจัดฝึกอบรมให้ความรู้เกี่ยวกับความมั่นคงปลอดภัย (Information Security Awareness)

แก่บุคลากรของรัฐสภา

๑๐. การประเมินระบบสารสนเทศของรัฐสภา (Vulnerability Assessment)

๑๑. แผนการตอบสนองภัยคุกคาม (Incident Response Plan) ของรัฐสภา

๑๒. การจัดทำทะเบียนทรัพย์สินทางด้าน ICT ของรัฐสภา (Inventory of Assets)

๑๓. การทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา

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

**การเตรียมความพร้อมรัฐสภา ในส่วนของ Data Center เพื่อได้รับมาตรฐาน ISO ๒๗๐๐๑: ๒๐๑๓ ในปีงบประมาณ พ.ศ. ๒๕๖๖ มีการกำหนดกิจกรรมการดำเนินงานในปีงบประมาณ พ.ศ. ๒๕๖๕ ดังนี้**

๑. การทดสอบเจาะระบบความปลอดภัยเทคโนโลยีสารสนเทศ (IT Penetration Testing) อุปกรณ์ (Data Center) ของรัฐสภา โดยมีการทดสอบเจาะระบบจากภายใน (Internal Penetration Testing) และการทดสอบเจาะระบบจากภายนอก (External Penetration Testing) โดยมีการจัดทำรายงานผลการทดสอบเจาะระบบ สิ่งที่ตรวจพบ ช่องโหว่/จุดอ่อน ผลกระทบ/ความเสี่ยง ข้อเสนอแนะในการแก้ไข ช่องโหว่/จุดอ่อน รวมทั้งรายงานรายละเอียดสิ่งที่ตรวจพบและวิธีการตรวจพบ (Technical Detailed Report) ข้อเสนอแนะในการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายและอุปกรณ์ (Data Center) ของรัฐสภา

๒. ทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา เพื่อบริหารจัดการระบบสารสนเทศของรัฐสภาให้ดำเนินการได้อย่างต่อเนื่อง

๓. ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา

๔. กิจกรรมเสริมสร้างการเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Information Security) (Data Center) ของรัฐสภา

## เกณฑ์การให้คะแนน

ระดับคะแนน	เกณฑ์การให้คะแนน
๑	<p>มีแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลอาคารรัฐสภา ประจำปีงบประมาณ ๒๕๖๕ โดยผ่านความเห็นชอบจากคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕) ทั้งนี้ ผลผลิต/ผลลัพธ์ที่ต้องการให้เกิดในปีงบประมาณ พ.ศ. ๒๕๖๕ ประกอบด้วย</p> <ol style="list-style-type: none"> <li>๑. รายงานผลการประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเทคโนโลยีสารสนเทศ (IT Penetration Testing) อุปกรณ์ภายในห้อง Data Center รัฐสภา พร้อมแนวทางการแก้ไขปัญหา และข้อเสนอแนะ</li> <li>๒. รายงานผลการทบทวนแผนต่อเนื่องการบริหารจัดการ (Business Continuity Plan: BCP) ด้านเทคโนโลยีสารสนเทศ ของรัฐสภา</li> <li>๓. ผลการทบทวนแนวนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศรัฐสภา และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศรัฐสภา</li> <li>๔. รายงานการจัดกิจกรรมเสริมสร้างการเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัย</li> </ol> <p>ด้านเทคโนโลยีสารสนเทศของรัฐสภา (Technology Information Security) ห้อง Data Center รัฐสภา</p>
๓	<p>-ดำเนินการตามแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอาคารรัฐสภา ประจำปีงบประมาณ พ.ศ.๒๕๖๕ ได้ไม่น้อยกว่าร้อยละ ๘๐</p> <p>-ดำเนินการตามแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอาคารรัฐสภา ประจำปีงบประมาณ ๒๕๖๕ ได้ร้อยละ ๑๐๐</p>
๕	<p>- ประเมินความพึงพอใจในการนำระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอาคารรัฐสภาไปใช้ปฏิบัติงาน สอดคล้องกับความต้องการของผู้รับบริการ อย่าง ถูกต้อง ครบถ้วน และมีประสิทธิภาพ โดยระดับความพึงพอใจต้องไม่น้อยกว่าร้อยละ ๘๐</p> <p>- รายงานสรุปผลการดำเนินงานประจำปีงบประมาณ พ.ศ. ๒๕๖๕ และปัญหาอุปสรรคในการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสารอาคารรัฐสภา</p> <p>- รายงานผลสัมฤทธิ์ของการดำเนินการตามแผนพัฒนา Digital Parliament ระยะ ๕ ปี</p>

ระดับคะแนน	เกณฑ์การให้คะแนน
	(พ.ศ. ๒๕๖๑-๒๕๖๕) ในการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอาครารัฐสภา และรายงานปัญหาอุปสรรคและข้อเสนอแนะแนวทางการพัฒนาระบบสารสนเทศรองรับอาครารัฐสภาเสนอต่อหัวหน้าส่วนราชการ

แผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัย  
ด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ประจำปีงบประมาณ ๒๕๖๕

ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตาม

มาตรฐานสากล

กลยุทธ์ที่ ๒.๑ พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

ตัวชี้วัดตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ ๒๕๖๕

ตัวชี้วัดที่ ๑.๓.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา

[illegible]

[illegible]







การดำเนินงานตัวชี้วัดที่ ๑.๓.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา

แผนงาน/โครงการ	ตัวชี้วัด	พ.ศ. ๒๕๖๕
๑.การทดสอบเจาะระบบความปลอดภัยเทคโนโลยีสารสนเทศ (IT Penetration Testing) อุปกรณ์ (Data Center) ของรัฐสภา	<p><u>ผลผลิต</u></p> <p>รายงานการทดสอบเจาะระบบความปลอดภัยเทคโนโลยีสารสนเทศ (IT Penetration Testing) อุปกรณ์ (Data Center) ของรัฐสภา</p> <p><u>ผลลัพธ์:</u></p> <p>มีแนวทางในการแก้ปัญหาช่องโหว่ของระบบเทคโนโลยีสารสนเทศ (IT Penetration Testing) อุปกรณ์ (Data Center) ของรัฐสภา ที่ได้จากการทดสอบ</p>	<p>๒ ฉบับ</p> <p>ร้อยละ ๑๐๐</p>
๒. โครงการจัดทำกฎ/ระเบียบ/มาตรการ/แนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา	<p>๑) การทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (BCP Plan)</p> <p><u>ผลผลิต :</u></p> <p>รายงานการทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (BCP Plan)</p>	๑ ฉบับ

แผนงาน/โครงการ	ตัวชี้วัด	พ.ศ. ๒๕๖๕
	<p><b>ผลลัพธ์ :</b> ลดผลกระทบจากการหยุดชะงักการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ให้อยู่ในระดับที่ยอมรับได้</p>	ร้อยละ ๘๐
	<p>๒) การทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p> <p><b>ผลผลิต :</b> รายงานการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p> <p><b>ผลลัพธ์ :</b> มีการดูแลการบริหารจัดการอย่างมีประสิทธิภาพตามหลักมาตรฐานสากลโดยครอบคลุมด้านการรักษาความลับ ความถูกต้อง และสภาพความพร้อมใช้ของสารสนเทศ</p>	<p>๑ ฉบับ</p> <p>ร้อยละ ๘๐</p>
<p>๓. โครงการให้ความรู้ความเข้าใจการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p>	<p><b>ผลผลิต :</b> กิจกรรมการฝึกอบรม/สัมมนา/อบรมเชิงปฏิบัติการ ซึ่งประกอบด้วยหลักสูตรดังนี้</p> <p>๑) ความตระหนักในความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness)</p> <p>๒) ความรู้ความเข้าใจในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p>	๑ หลักสูตร

แผนงาน/โครงการ	ตัวชี้วัด	พ.ศ. ๒๕๖๕
	<p>๓) ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์</p> <p>๔) การเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศของรัฐสภา (Technology Information Security) ห้อง Data Center รัฐสภา</p> <p><b>ผลลัพธ์ :</b></p> <p>๑) ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจเพิ่มขึ้นและสามารถปฏิบัติตามกฎ/ระเบียบ/มาตรการ/แนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภาได้</p> <p>๒) ผู้เข้ารับการฝึกอบรมมีความพึงพอใจในการฝึกอบรม</p>	<p>ร้อยละ ๘๐</p> <p>ร้อยละ ๘๐</p>



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

ที่ ๓ /๒๕๖๒

เรื่อง แต่งตั้งคณะกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัย  
ด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๕ 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  
ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภามีประสิทธิภาพและความมั่นคง  
ปลอดภัย เป็นไปตามมาตรฐานสากล ประกอบกับแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยี  
สารสนเทศและการสื่อสารของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) ซึ่งเป็นกรอบกำหนดทิศทางของ  
การรักษาความมั่นคงปลอดภัย และเป็นเครื่องมือในการป้องกันไม่ให้เกิดความเสียหายต่อระบบสารสนเทศและ  
การสื่อสารของรัฐสภา

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

- |   |                        |
|---|------------------------|
| ๑. นายวีระชาติ มัตติทานนท์  | ที่ปรึกษาและอนุกรรมการ |
| ๒. ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานเลขาธิการวุฒิสภา                                   | ประธานอนุกรรมการ       |
| ๓. ผู้อำนวยการสำนักสารสนเทศ<br>สำนักงานเลขาธิการสภาผู้แทนราษฎร  | รองประธานอนุกรรมการ    |
| ๔. ผู้บังคับบัญชากลุ่มงานบริหารระบบเครือข่ายคอมพิวเตอร์<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร        | อนุกรรมการ             |
| ๕. ผู้บังคับบัญชากลุ่มงานบริการระบบคอมพิวเตอร์<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร                 | อนุกรรมการ             |
| ๖. ผู้บังคับบัญชากลุ่มงานวิทยาการคอมพิวเตอร์<br>สำนักเทคโนโลยีสารสนเทศและการสื่อสาร<br>สำนักงานเลขาธิการวุฒิสภา | อนุกรรมการ             |
| ๗. นายสุธี ยืนแน่นอน<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร   | อนุกรรมการ             |
| ๘. นางณัชชา ศรีเพลิง<br>สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร   | อนุกรรมการ             |

๙. นางสมคิด...

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

ให้คณะอนุกรรมการ มีอำนาจหน้าที่ ดังต่อไปนี้

๑. กำกับ ดูแล และขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒- ๒๕๖๕) ให้เป็นไปตามเป้าหมายของแผนการรักษาความมั่นคงปลอดภัยฯ ที่กำหนดไว้แต่ละปีงบประมาณ

๒. กำหนดระเบียบ ข้อปฏิบัติ และแนวทางการดำเนินการที่เกี่ยวข้อง เพื่อให้รองรับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

๓. ติดตาม ประเมินผลและรายงานผลการดำเนินงานต่อคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ - ๒๕๖๕) ทราบเป็นระยะ

๔. แต่งตั้งคณะทำงานเพื่อดำเนินการตามที่คณะอนุกรรมการเห็นสมควร

๕. ดำเนินการอื่นตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๕ สิงหาคม พ.ศ. ๒๕๖๒



(นางพรพรรณต์ ไทยวัฒนากุล)

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



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

ที่ ๕ /๒๕๖๒

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

ตามคำสั่งคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕) ที่ ๖/๒๕๖๒ ลงวันที่ ๑๒ กรกฎาคม ๒๕๖๒ เรื่อง แต่งตั้งคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒- ๒๕๖๕) เพื่อกำกับ ดูแล และขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) ให้เป็นไปตามเป้าหมายของแผนการรักษาความมั่นคงปลอดภัยฯ ที่กำหนดไว้แต่ละปีงบประมาณ รวมทั้งเพื่อให้สามารถบรรลุตามกรอบตัวชี้วัด

ดังนั้น เพื่อให้การดำเนินงานของคณะอนุกรรมการฯ มีความครอบคลุมครบถ้วนและมีประสิทธิภาพมากยิ่งขึ้น จึงเห็นควรแต่งตั้งอนุกรรมการ เพิ่มเติม คือ นายจิรภัทร์ เต็มวุฒิโรจน์

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๖ สิงหาคม พ.ศ. ๒๕๖๒

(นางพรพรรณนต์ ไทยวัฒนากุล)

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