แผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ประจำปีงบประมาณ 2563

สารบัญ

๑. สาระสำคัญ

แผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา ประจำปีงบประมาณ ๒๕๖๓ เป็นแผนปฏิบัติการที่จัดทำขึ้นมาเพื่อใช้เป็นกรอบแนวทางการดำเนินงานตามตัวชี้วัดที่ ๑.๔.๒ ตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๓ ซึ่งกำหนดให้มีการประเมินประสิทธิผลการปฏิบัติราชการเป็นประจำทุกปี สำหรับตัวชี้วัดดังกล่าวนี้ เป็นตัวชี้วัดร่วมของหน่วยงานด้านเทคโนโลยีสารสนเทศสังกัดรัฐสภา ได้แก่ สำนักสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร และสำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา ซึ่งเป็นหน่วยงานหลัก และเป็นเจ้าภาพร่วมในการรายงานผลการดำเนินการด้านการพัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากลเพื่อรองรับการปฏิบัติงานสำหรับอาคารรัฐสภา โดยในปีงบประมาณ ๒๕๖๓ 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 และเป็นกรอบกำหนดทิศทางของการรักษาความมั่งคงปลอดภัย และเป็นเครื่องมือในการป้องกันไม่ให้เกิดความเสียหายต่อระบบสารสนเทศและการสื่อสารของรัฐสภาต่อไป

๒. วัตถุประสงค์

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

๒) เพื่อให้งานด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภามีความมั่นคงปลอดภัย ในอันที่จะสร้างความรู้ ความเข้าใจและความเชื่อมั่นแก่สมาชิกรัฐสภา และบุคลากรในวงงานของรัฐสภา

๓) เพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภามีแผนงานโครงการและการติดตามประเมินผลในการขับเคลื่อนการดำเนินงานด้านระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารตามกรอบตัวชี้วัดตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ ๒๕๖๓

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. ระบบข้อมูลและสารสนเทศของรัฐสภามีการเชื่อมโยงและบูรณาการเพื่อให้บริการอย่างมีประสิทธิภาพ

๒. ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา มีประสิทธิภาพและมีความมั่นคงปลอดภัย เป็นไปตามมาตรฐานสากล

๓. สมาชิกรัฐสภาและบุคคลในวงงานรัฐสภารู้เท่าทัน สามารถใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร 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 ให้สมาชิกรัฐสภา และบุคคลในวงงานรัฐสภา มีความรู้ ความสามารถและทักษะในการประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ

การเชื่อมโยงความสัมพันธ์ระหว่างยุทธศาสตร์ กลยุทธ์ และเป้าประสงค์เชิงยุทธศาสตร์

ยุทธศาสตร์	กลยุทธ์	เป้าประสงค์เชิงยุทธศาสตร์
ยุทธศาสตร์ที่ ๑ พัฒนาระบบและบูรณาการข้อมูลมุ่งสู่การเป็น Digital Parliament	๑.๑ พัฒนาระบบและบูรณาการข้อมูลมุ่งสู่การเป็น Digital Parliament	ระบบข้อมูลและสารสนเทศของรัฐสภามีการเชื่อมโยงและบูรณาการเพื่อให้บริการอย่างมีประสิทธิภาพ
	๑.๒ พัฒนาระบบบริการด้านสารสนเทศ ให้มีข้อมูลที่ถูกต้อง ทันสมัย รองรับความต้องการของผู้รับบริการและประชาชน	ผู้รับบริการและประชาชนได้รับข้อมูลสารสนเทศของรัฐสภาที่ถูกต้อง รวดเร็ว และทันสมัย ตรงกับความต้องการ
ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากล	๒.๑ พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา	ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภามีประสิทธิภาพ และมีความมั่นคงปลอดภัย เป็นไปตามมาตรฐานสากล
	๒.๒ พัฒนาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากลรองรับการให้บริการได้อย่างทั่วถึงและเท่าเทียม	

ยุทธศาสตร์	กลยุทธ์	เป้าประสงค์เชิงยุทธศาสตร์
ยุทธศาสตร์ที่ ๓ ส่งเสริมและสนับสนุน ให้สมาชิกรัฐสภา และบุคคลในวงงานรัฐสภา มีความรู้ความสามารถ และทักษะในการประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ	๓.๑ พัฒนาสมรรถนะบุคลากรของรัฐสภาด้านการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร	สมาชิกรัฐสภาและบุคคลในวงงานรัฐสภารู้เท่าทัน สามารถใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสร้างสรรค์
	๓.๒ ส่งเสริม สนับสนุนให้สมาชิกรัฐสภาและบุคคลในวงงานของรัฐสภาใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสร้างสรรค์	
	๓.๓ ส่งเสริม สนับสนุนบุคลากร ให้มีการศึกษา วิจัย และพัฒนาทางด้านนวัตกรรมและเทคโนโลยี รองรับความต้องการของผู้รับบริการและประชาชน	

๔. เป้าหมายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ประจำปีงบประมาณ ๒๕๖๓

เป้าหมายในการดำเนินงานคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภาระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) ประจำปีงบประมาณ พ.ศ. ๒๕๖๒ ดังนี้

๔.๑ จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan)

๔.๒ จัดทำแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Business Continuity Plan)

๔.๓ ระบบเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ (ระบบความมั่นคงปลอดภัย) ประกอบด้วย

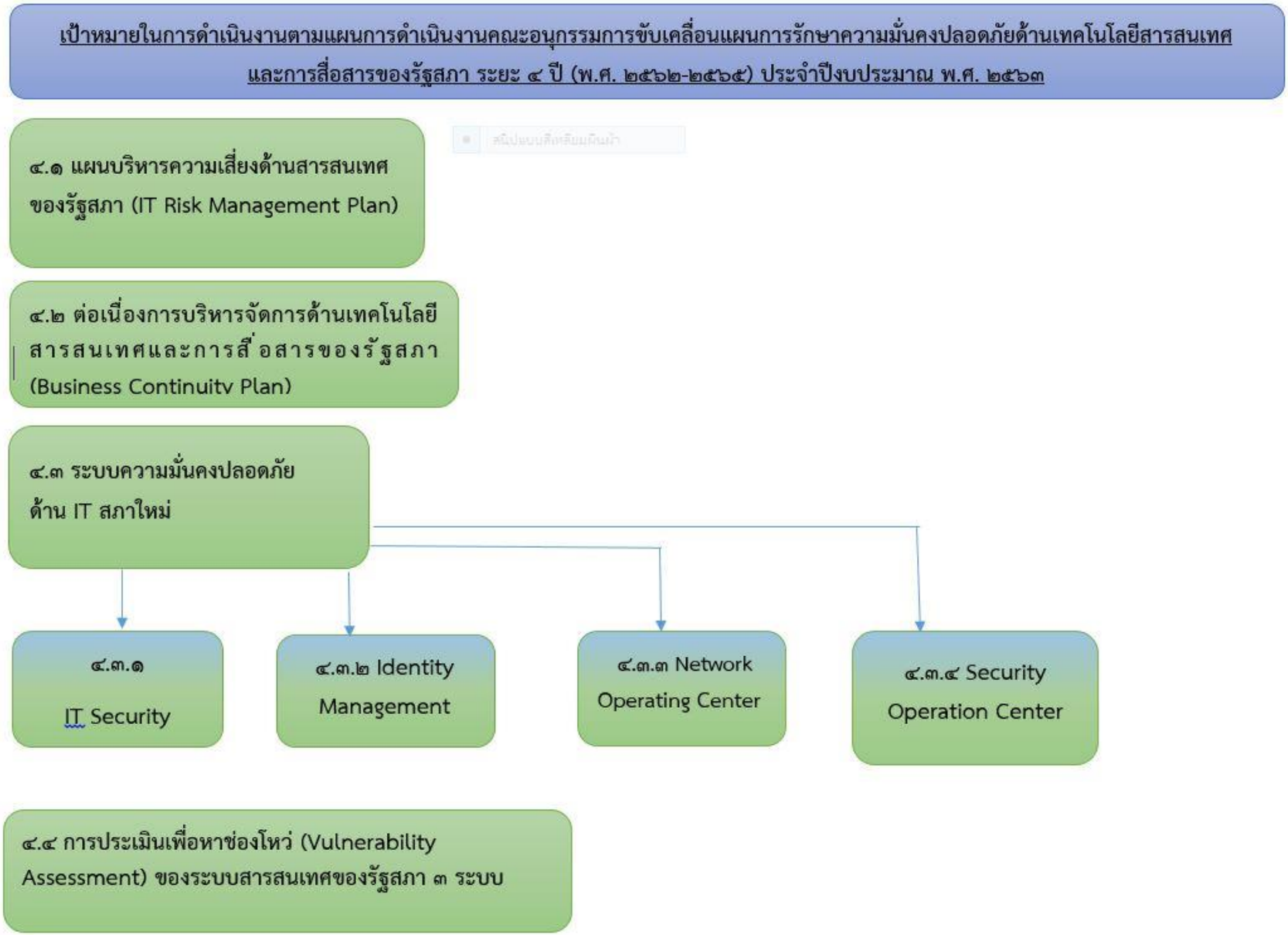
๔.๔.๑ ระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

๔.๔.๒ ระบบบริหารจัดการตัวตนผู้ใช้งาน (Identity Management)

๔.๔.๓ Network Operating Center (NOC) ศูนย์ปฏิบัติการเครือข่าย

๔.๔.๔ Security Operation Center (SOC) ศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์

๔.๔ การประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ของระบบสารสนเทศของรัฐสภาอย่างน้อย ๓ ระบบ


เป้าหมายในการดำเนินงานตามแผนการดำเนินงานคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) ประจำปีงบประมาณ พ.ศ. ๒๕๖๓
๔.๑ แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan)
๔.๒ ต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Business Continuitv Plan)
๔.๓ ระบบความมั่นคงปลอดภัยด้าน IT สภาใหม่
๔.๓.๑ IT Security
๔.๓.๒ Identity Management
๔.๓.๓ Network Operating Center
๔.๓.๔ Security Operation Center
๔.๔ การประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ของระบบสารสนเทศของรัฐสภา ๓ ระบบ

๕. กรอบตัวชี้วัดการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ ๒๕๖๓

ตัวชี้วัดที่ ๑.๔ ระดับความสำเร็จของการพัฒนาเทคโนโลยีสารสนเทศเพื่อมุ่งสู่รัฐสภาดิจิทัล (Digital Parliament)

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

ตัวชี้วัดที่ ๑.๔.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่

รัฐสภาได้นำระบบเทคโนโลยีสารสนเทศและการสื่อสารมาเป็นเครื่องมือในการให้บริการและการปฏิบัติงาน ของส่วนราชการสังกัดรัฐสภา โดยมีการใช้งานระบบสารสนเทศอย่างแพร่หลายและต่อเนื่อง เพื่อใช้เป็นช่องทางในการดำเนินงาน ประชาสัมพันธ์ เผยแพร่ข่าวสาร ข้อมูล รวมไปถึงการอำนวยความสะดวกในการเข้าถึงข้อมูลทั้งในด้านข่าวสาร ผ่านระบบเครือข่ายคอมพิวเตอร์ ซึ่งจากการให้บริการในรูปแบบดังกล่าวนับว่ามีความสำคัญเป็นอย่างยิ่งในปัจจุบันและอนาคต 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 เพื่อให้ระบบสารสนเทศของส่วนราชการสามารถให้บริการและรองรับการปฏิบัติงานได้โดยไม่ต้องหยุดให้บริการระบบสารสนเทศ สามารถให้บริการระบบสารสนเทศและระบบเครือข่ายได้อย่างต่อเนื่อง มั่นคงและมีเสถียรภาพ โดยมีกิจกรรมที่ดำเนินการ ประกอบด้วย

๑. แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan)

๒. แผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

๓. ระบบเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ (ระบบความมั่นคงปลอดภัย) ซึ่งประกอบด้วย

๑) ระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

๒) ระบบบริหารจัดการตัวตนผู้ใช้งาน (Identity Management)

๓) Network Operating Center (NOC) ศูนย์ปฏิบัติการเครือข่าย

๔) Security Operating Center (SOC) ศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์

๔. การประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ของระบบสารสนเทศของรัฐสภา

เกณฑ์การให้คะแนนเพื่อการประเมินตัวชี้วัด KPI ๑.๔.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่

ระดับคะแนน	เกณฑ์การให้คะแนน
๑	● มีแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ประจำปีงบประมาณ ๒๕๖๓
๒	● ดำเนินการตามแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ได้ไม่น้อยกว่า ร้อยละ ๖๐
๓	● ดำเนินการตามแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ได้ไม่น้อยกว่า ร้อยละ ๘๐
๔	● ดำเนินการตามแผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ได้ไม่น้อยกว่า ร้อยละ ๑๐๐
๕	● รายงานสรุปผลการดำเนินงานและปัญหาอุปสรรคในการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ เสนอต่อหัวหน้าส่วนราชการ

แผนปฏิบัติการเพื่อขับเคลื่อนการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ ประจำปีงบประมาณ ๒๕๖๓

ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากล
กลยุทธ์ที่ ๒.๑ พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา
ตัวชี้วัดตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ ๒๕๖๓
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. ระบบเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ (ระบบความมั่นคงปลอดภัย)													๖๐
๑.๑ ระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)													(๑๕)
งานวิเคราะห์และออกแบบระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)													
งานติดตั้งอุปกรณ์													
ทดสอบและรายงานผล													
๑.๒ ระบบบริหารจัดการตัวตนผู้ใช้งาน (Identity Management)													(๑๕)
งานวิเคราะห์และออกแบบระบบบริหารจัดการตัวตนผู้ใช้งาน (Identity Management)													
งานติดตั้งอุปกรณ์													
ทดสอบและรายงานผล													
๑.๓ ศูนย์ปฏิบัติการเครือข่าย Network Operating Center (NOC)													(๑๕)
งานวิเคราะห์และออกแบบ													
งานสร้างและสถาปัตยกรรม													
งานติดตั้งอุปกรณ์													
ทดสอบและรายงานผล													
๑.๔ ศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ Security Operation Center (SOC)													(๑๕)

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.	
งานวิเคราะห์และออกแบบ													
งานสร้างและสถาปัตยกรรม													
งานติดตั้งอุปกรณ์													
ทดสอบและรายงานผล													
๒. จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan)													**๑๕**
๒.๑ ศึกษา มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง													
๒.๒ สำรวจ สถานภาพด้านเทคโนโลยีสารสนเทศฯ ของสำนักงานเลขาธิการสภาผู้แทนราษฎร และสำนักงานเลขาธิการวุฒิสภา													
๒.๓ จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan)													
๒.๔ คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคง ฯ เพื่อพิจารณา													
๒.๕ รายงานผลการดำเนินงานต่อคณะกรรมการขับเคลื่อนแผน Digital Parliament รัฐสภา													
๒.๖ รายงานผลการดำเนินงานการจัดทำแผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan) ต่อหัวหน้าส่วนราชการ													
๓. จัดทำแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Business Continuity Plan)													**๑๕**
๓.๑ ศึกษา มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง													
๓.๒ สำรวจ สถานภาพด้านเทคโนโลยีสารสนเทศฯ ของสำนักงานเลขาธิการสภาผู้แทนราษฎร และสำนักงานเลขาธิการวุฒิสภา													
๓.๓ จัดทำแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Business Continuity Plan)													
๓.๔ คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคง ฯ เพื่อพิจารณา													
๓.๕ รายงานผลการดำเนินงานต่อคณะกรรมการขับเคลื่อนแผน Digital Parliament รัฐสภา													

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.	
๓.๖ รายงานผลการดำเนินงานการจัดทำแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Business Continuity Plan) ต่อหัวหน้าส่วนราชการ													
๔. การประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ของระบบสารสนเทศของรัฐสภา จำนวน ๓ ระบบ													**๑๐**
๔.๑ งานติดตั้งอุปกรณ์และโปรแกรม													
๔.๒ ตรวจสอบช่องโหว่													
๔.๓ รายงานผลการประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ของระบบสารสนเทศของรัฐสภา ต่อคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคง ฯ													
๔.๔ รายงานผลการดำเนินงานต่อคณะกรรมการขับเคลื่อนแผน Digital Parliament รัฐสภา													

ตัวชี้วัดที่ ๑.๔.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานและระบบ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่

ลำดับ		ปีงบประมาณ ๒๕๖๒												ปีงบประมาณ ๒๕๖๓											
		ไตรมาส ๑			ไตรมาส ๒			ไตรมาส ๓			ไตรมาส ๔			ไตรมาส ๑			ไตรมาส ๒			ไตรมาส ๓			ไตรมาส ๔		
		(ต.ค. -ธ.ค.)			(ม.ค.-มี.ค.)			(เม.ย.-มิ.ย.)			(ก.ค.- ก.ย.)			(ต.ค. -ธ.ค.)			(ม.ค.-มี.ค.)			(เม.ย.-มิ.ย.)			(ก.ค. -ก.ย.)		
มิติที่ ๔ การพัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัย																									
๑	ระบบเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ (ระบบความมั่นคงปลอดภัย) ๑.๑ ระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) ๑.๒ ระบบบริหารจัดการตัวตนผู้ใช้งาน (Identity Management) ๑.๓ ศูนย์ปฏิบัติการเครือข่าย Network Operating Center (NOC) ๑.๔ ศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัย (Security Operation Center)																									
๒	แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan)																									
๓	แผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Business Continuity Plan)																									
๔	การประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ของระบบสารสนเทศของรัฐสภา จำนวน ๓ ระบบ																									

การดำเนินงานตามตัวชี้วัดที่ ๑.๔.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานและระบบ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่

แผนงาน/โครงการ	ตัวชี้วัด	พ.ศ. 2563
1.ระบบเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ (ระบบความมั่นคงปลอดภัย)	**ผลผลิต** 1) ระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) 2) ระบบบริหารจัดการตัวตนผู้ใช้งาน (Identity Management) 3) ศูนย์ปฏิบัติการเครือข่าย Network Operating Center (NOC) 4) ศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัย (Security Operation Center) **ผลลัพธ์** ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีความมั่นคงปลอดภัย	ร้อยละ 100
2. โครงการจัดทำกฎ/ระเบียบ/มาตรการ/แนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา	**ผลผลิต :** 1) แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา (IT Risk Management Plan) 2) แผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา **ผลลัพธ์ :** ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีความมั่นคงปลอดภัย	1 ฉบับ 1 ฉบับ ร้อยละ 100
3. โครงการจ้างประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ระบบสารสนเทศของรัฐสภา	**ผลผลิต :** มีรายงานการประเมินเพื่อหาช่องโหว่ (Vulnerability Assessment) ระบบสารสนเทศของรัฐสภา **ผลลัพธ์ :** ระบบสารสนเทศของรัฐสภา สามารถป้องกันการบุกรุก โจมตี	3 ระบบ ร้อยละ 100