

รายงานสรุปผลการดำเนินงานประจำปีงบประมาณ พ.ศ. ๒๕๖๕
ในการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
และการสื่อสารของอาคารรัฐสภา

บทสรุปผู้บริหาร

การพัฒนากรอบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา ประจำปีงบประมาณ ๒๕๖๕ ขับเคลื่อนการดำเนินงานภายใต้คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) เพื่อดำเนินงานตามแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕) ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากล กำหนดทิศทางของการรักษาความมั่นคงปลอดภัย และเป็นเครื่องมือในการป้องกันไม่ให้เกิดความเสียหายต่อระบบสารสนเทศและการสื่อสารของรัฐสภา โดยมุ่งเน้นเรื่องระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้ผู้รับบริการมีความเชื่อมั่นกับความปลอดภัยของระบบเทคโนโลยีและการสื่อสาร รวมไปถึงการอำนวยความสะดวกในการเข้าถึงข้อมูล ลดความเสี่ยง ป้องกันจุดอ่อนของระบบสารสนเทศ ระบบคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายคอมพิวเตอร์ และการสื่อสารให้เป็นไปตามมาตรฐานสากล โดยผลการดำเนินงานในปีงบประมาณ พ.ศ. ๒๕๖๕ สรุปผลการดำเนินงานได้ตามกิจกรรม ดังนี้

๑. การทดสอบเจาะระบบความปลอดภัยเทคโนโลยีสารสนเทศ (IT Penetration Testing) อุปกรณ์ (Data Center) ของรัฐสภา โดยมีการทดสอบเจาะระบบจากภายใน (Internal Penetration Testing) และการทดสอบเจาะระบบจากภายนอก (External Penetration Testing) โดยผลการทดสอบเจาะระบบ พบจำนวนช่องโหว่ในการเจาะระบบครั้งที่ ๑ จำนวน ๔ ช่องโหว่ และเมื่อทำการเจาะระบบ ครั้งที่ ๒ พบจำนวนช่องโหว่เหลือเพียง จำนวน ๑ ช่องโหว่ โดยสามารถแก้ไขปัญหามาตรฐานของช่องโหว่ที่ได้ทำการตรวจพบเมื่อตรวจพบช่องโหว่สามารถแก้ไขและสามารถปิดช่องโหว่ได้

๒. ทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา เพื่อบริหารจัดการระบบสารสนเทศของรัฐสภาให้ดำเนินการได้อย่างต่อเนื่อง โดยทบทวนปรับปรุงให้แผนมีความทันสมัย รองรับการนำไปปฏิบัติ เพื่อให้ระบบเทคโนโลยีสารสนเทศของรัฐสภาสามารถทำงานได้อย่างต่อเนื่อง โดยแผนได้รับความเห็นชอบของหัวหน้าส่วนราชการให้ประชาสัมพันธ์และใช้เป็นแนวปฏิบัติกับหน่วยงานที่เกี่ยวข้อง

๓. ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา โดยทบทวนนโยบายและแนวปฏิบัติให้เหมาะสมกับสถานการณ์ที่มีการเปลี่ยนแปลงไป ซึ่งนโยบายและแนวปฏิบัติดังกล่าวได้รับความเห็นชอบของหัวหน้าส่วนราชการให้แจ้งเวียนเพื่อประชาสัมพันธ์และใช้เป็นแนวปฏิบัติต่อไป

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

๕. ประเมินความพึงพอใจในการนำระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอาคารรัฐสภา เพื่อวัดระดับความพึงพอใจของผู้ใช้บริการ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ และจะได้นำผลการประเมินไปปรับปรุงและพัฒนาเพิ่มประสิทธิภาพในการให้บริการด้านระบบเครือข่าย โดยแบ่งกลุ่มการประเมินความพึงพอใจออกเป็น ๒ กลุ่มดังนี้

กลุ่มที่ ๑ (บุคคลภายนอก) ได้แก่ สื่อมวลชนประจำรัฐสภา ผู้มาติดต่อราชการจากภายนอก ผลการประเมินความพึงพอใจในการให้บริการระบบเครือข่ายเฉลี่ย คิดเป็นร้อยละ ๘๒.๐๐

กลุ่มที่ ๒ (บุคคลภายในรัฐสภา) ได้แก่ ลูกจ้าง พนักงานราชการ ข้าราชการรัฐสภา ผลการประเมินความพึงพอใจในการให้บริการระบบเครือข่ายเฉลี่ยคิดเป็นร้อยละ ๘๑.๙๓

๑. บทนำ

การดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสารของอาคารรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ โดยดำเนินงานตามกรอบแนวทางการดำเนินงานตามตัวชี้วัดที่ ๑.๓.๒ ตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ซึ่งกำหนดให้มีการประเมินประสิทธิผลการปฏิบัติราชการเป็นประจำทุกปี สำหรับตัวชี้วัดดังกล่าวนี้ เป็นตัวชี้วัดร่วมของหน่วยงานด้านเทคโนโลยีสารสนเทศสังกัดรัฐสภา 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 และเป็นกรอบกำหนดทิศทางของการรักษาความมั่นคงปลอดภัย และเป็นเครื่องมือในการป้องกันไม่ให้เกิดความเสียหายต่อระบบสารสนเทศและการสื่อสารของรัฐสภาต่อไป

ยุทธศาสตร์ของแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕)
ตามประเด็นยุทธศาสตร์ที่ ๒. พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ให้เป็นไปตามมาตรฐานสากล

การเชื่อมโยงความสัมพันธ์ระหว่างยุทธศาสตร์ กลยุทธ์ และเป้าประสงค์เชิงยุทธศาสตร์

ยุทธศาสตร์	กลยุทธ์	เป้าประสงค์เชิงยุทธศาสตร์
ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ให้เป็นไปตามมาตรฐานสากล	๒.๑ พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา	ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา มีประสิทธิภาพ และมีความมั่นคงปลอดภัย เป็นไปตามมาตรฐานสากล
	๒.๒ พัฒนาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ให้เป็นไปตามมาตรฐานสากลรองรับการให้บริการได้อย่างทั่วถึงและเท่าเทียม	

๒. เป้าหมายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ประจำปีงบประมาณ ๒๕๖๕ มีดังนี้

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

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

๓. ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา

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

๓. กรอบตัวชี้วัดการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ ๒๕๖๓

ตัวชี้วัดที่ ๑.๓ ระดับความสำเร็จของการพัฒนาเทคโนโลยีสารสนเทศเพื่อบูรณาการสู่รัฐสภาดิจิทัล (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 ซึ่งจากการให้บริการในรูปแบบดังกล่าวข้างต้นมีความจำเป็นอย่างยิ่งในการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภาแห่งใหม่ เพื่อให้มีประสิทธิภาพ และต้องคำนึงถึงความปลอดภัย และลดความเสี่ยง ป้องกันจุดอ่อนของระบบสารสนเทศ ระบบคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายคอมพิวเตอร์ ซึ่งแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑-๒๕๖๕) ยุทธศาสตร์ที่ ๒ พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากล ซึ่งมุ่งเน้นเรื่องระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้ผู้รับบริการมีความเชื่อมั่นกับความปลอดภัยของระบบเทคโนโลยีและการสื่อสาร และขับเคลื่อนตามเป้าหมายของแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕)

กิจกรรมการดำเนินงานในปีงบประมาณ 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

กลยุทธ์ที่ ๒.๑ พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐบาล

ตัวชี้วัดตามคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ประจำปีงบประมาณ ๒๕๖๕

ตัวชี้วัดที่ ๑.๓.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคาร
รัฐสภา

แผนปฏิบัติการดำเนินการพัฒนาระบบโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา

[illegible]

ผลการดำเนินงานตัวชี้วัดที่ ๑.๓.๒ ระดับความสำเร็จของการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของอาคารรัฐสภา

กิจกรรม	ผลการดำเนินงานตามตัวชี้วัด
<p>๑. การทดสอบเจาะระบบความปลอดภัยเทคโนโลยีสารสนเทศ (IT Penetration Testing) อุปกรณ์ (Data Center) ของรัฐสภา</p>	<p>ผลผลิต</p> <p>การทดสอบเจาะระบบความปลอดภัยเทคโนโลยีสารสนเทศ (IT Penetration Testing) อุปกรณ์ (Data Center) ของรัฐสภา ระบบสารสนเทศรัฐสภา https://pis.parliament.go.th/</p> <ol style="list-style-type: none"> ๑) ระบบบริหารจัดการห้องประชุมอัจฉริยะ ๒) ระบบบริหารจัดการเอกสารการประชุมดิจิทัล ๓) ระบบบริหารการประชุมรัฐสภา ๔) ระบบบริหารจัดการบัตรรัฐสภา ๕) ระบบบริหารข้อมูลป้ายประกาศดิจิทัล ๖) ระบบบริหารการประชุมรัฐสภาระหว่างประเทศ ๗) ระบบบันทึกการลงเวลาปฏิบัติราชการ ๘) ระบบบริหารจัดการไฟล์อัจฉริยะ ๙) ระบบศูนย์แลกเปลี่ยนข้อมูลรัฐสภา ๑๐) ระบบเผยแพร่ข้อมูลการประชุมรัฐสภา <p>ผลลัพธ์</p> <p>รายงานผลทดสอบเจาะระบบเทคโนโลยีสารสนเทศ (IT Penetration Testing) อุปกรณ์ (Data Center) ของรัฐสภา รัฐสภา ได้ดำเนินการทดสอบเจาะระบบสารสนเทศรัฐสภา ภายใน domain เดียวกัน จำนวน ๑๐ ระบบ ตามหลักเทคนิคของ Open Web Application Security Project (OWASP) Top ๑๐ Vulnerabilities ประกอบด้วย เทคนิคทดสอบการเจาะระบบจากภายใน จำนวน ๓๕ เทคนิค และจากภายนอก จำนวน ๑๐ เทคนิค พบช่องโหว่ จำนวน ๔ ช่องโหว่ ในการทดสอบการเจาะครั้งที่ ๑ และเมื่อทดสอบการเจาะระบบครั้งที่ ๒ จำนวน พบช่องโหว่จำนวน ๑ ช่องโหว่ และสามารถแก้ไขปัญหาการตรวจสอบพบช่องโหว่ได้</p>
<p>๒. ทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Business Continuity Plan: BCP) ของรัฐสภา</p>	<p>ผลผลิต :</p> <ul style="list-style-type: none"> - รายงานผลการทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา <p>ผลลัพธ์ :</p> <ul style="list-style-type: none"> - ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีความมั่นคงปลอดภัย

กิจกรรม	ผลการดำเนินงานตามตัวชี้วัด
	<p>- ปรับปรุงและทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา ให้มีความเหมาะสมและทันสมัย</p>
<p>๓. ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของรัฐสภา</p>	<p>ผลผลิต :</p> <p>- รายงานผลการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p> <p>ผลลัพธ์ :</p> <p>- ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีความมั่นคงปลอดภัย</p> <p>- ปรับปรุงและทบทวนแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา ให้มีความเหมาะสมและทันสมัย</p>
<p>๔. รายงานการจัดกิจกรรมเสริมสร้างการเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐสภา (Technology Information Security) ห้อง Data Center รัฐสภา</p>	<p>ผลผลิต :</p> <p>กิจกรรมการฝึกอบรม/สัมมนา/อบรมเชิงปฏิบัติการ ซึ่งประกอบด้วยหลักสูตร ดังนี้</p> <p>๑) ความตระหนักในความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness)</p> <p>๒) ความรู้ความเข้าใจในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภา</p> <p>๓) ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์</p> <p>๔) การเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศของรัฐสภา (Technology Information Security) ห้อง Data Center รัฐสภา</p> <p>ผลลัพธ์ :</p> <p>๑) ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจเพิ่มขึ้นและสามารถปฏิบัติตามกฎ/ระเบียบ/มาตรการ/แนวปฏิบัติด้วยความมั่นคงปลอดภัยด้านสารสนเทศของรัฐสภาได้</p> <p>๒) ผู้เข้ารับการฝึกอบรมมีความพึงพอใจในการฝึกอบรม</p> <p>ผลการจัดกิจกรรม จำนวน ๓ หลักสูตร ดังนี้</p> <p>ผลการดำเนินงานกิจกรรมในหัวข้อ (๑) ความตระหนักในความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness) (๒)</p>

กิจกรรม	ผลการดำเนินงานตามตัวชี้วัด
	<p>ความรู้ความเข้าใจในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของรัฐบาล และ (๓) ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์</p> <p>สำนักงานเลขาธิการสภาผู้แทนราษฎร</p> <ul style="list-style-type: none"> - จัดอบรมเมื่อวันที่ ๒๙ มีนาคม ๒๕๖๕ - มีผู้เข้าร่วมกิจกรรม จำนวนรวม ๒๒๐ คน - ผู้เข้าร่วมกิจกรรมมีความรู้ ความเข้าใจเพิ่มขึ้น เฉลี่ยร้อยละ ๙๒ - คะแนนเฉลี่ยก่อนเรียน = ๖.๙๓ และคะแนนเฉลี่ยหลังเรียน = ๙.๕๗ (คะแนนเต็ม ๑๐) - ความพึงพอใจของการฝึกอบรม ร้อยละ ๘๙.๕๗ <p>สำนักงานเลขาธิการวุฒิสภา</p> <ul style="list-style-type: none"> - จัดอบรม รุ่นที่ ๑ เมื่อวันที่ ๑๔ มิถุนายน ๒๕๖๕ และรุ่นที่ ๒ เมื่อวันที่ ๑๕ มิถุนายน ๒๕๖๕ - มีผู้ผ่านเกณฑ์การอบรมจำนวน ๑๗๖ คน คิดเป็นร้อยละ ๙๔.๑๒ - บุคลากรที่ผ่านการพัฒนาทักษะ ร้อยละ ๑๐๐ มีความรู้เพิ่มขึ้น และสามารถใช้เทคโนโลยีได้อย่างมีประสิทธิภาพ - คะแนนเฉลี่ยก่อนเรียน = ๔.๑ และคะแนนเฉลี่ยหลังเรียน = ๖.๙ (คะแนนเต็ม ๑๐) - ความพึงพอใจของการฝึกอบรม ร้อยละ ๙๙.๕๐ <p>การเรียนรู้มาตรฐานในการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศของรัฐบาล (Technology Information Security) ห้อง Data Center รัฐบาล</p> <p>ฝึกอบรมเมื่อวันที่ ๒๑ กันยายน ๒๕๖๕</p> <ul style="list-style-type: none"> - มีผู้เข้าร่วมอบรม จำนวน ๗๙ คน ผู้ตอบแบบประเมินความ พึงพอใจ ๕๑ คน - ผู้เข้าร่วมอบรมมีความรู้ความเข้าใจ ก่อนเรียน ร้อยละ ๕๖.๔๗ หลังเรียน ร้อยละ ๘๓.๙๒ - ความพึงพอใจของการอบรม ร้อยละ ๘๔.๕๑
๕.ประเมินความพึงพอใจในการนำระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคง	<p>ประเมินความพึงพอใจในการนำระบบโครงสร้างพื้นฐานดิจิทัลและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอาคาร รัฐบาล เพื่อวัดระดับความพึงพอใจของผู้ใช้บริการ ประจำปีงบประมาณ</p>

กิจกรรม	ผลการดำเนินงานตามตัวชี้วัด
ปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาคารรัฐสภา	พ.ศ. ๒๕๖๕ และจะได้นำผลการประเมินไปปรับปรุงและพัฒนาเพิ่มประสิทธิภาพในการให้บริการด้านระบบเครือข่าย โดยแบ่งกลุ่มการประเมินความพึงพอใจออกเป็น ๒ กลุ่มดังนี้ กลุ่มที่ ๑ (บุคคลภายนอก) ได้แก่ สื่อมวลชนประจำรัฐสภา ผู้มาติดต่อราชการจากภายนอก ผลการประเมินความพึงพอใจในการให้บริการระบบเครือข่ายเฉลี่ย คิดเป็นร้อยละ ๘๒.๐๐ กลุ่มที่ ๒ (บุคคลภายในรัฐสภา) ได้แก่ ลูกจ้าง พนักงานราชการ ข้าราชการรัฐสภา ผลการประเมินความพึงพอใจในการให้บริการระบบเครือข่ายเฉลี่ยคิดเป็นร้อยละ ๘๑.๙๓

๕. ปัญหาและอุปสรรคการดำเนินงาน

ด้านงบประมาณ

การไม่ได้รับจัดสรรงบประมาณ จึงทำให้ไม่สามารถดำเนินการตามเป้าหมายการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) กำหนดให้ ปี ๒๕๖๕ ศูนย์ข้อมูลหลัก (Data Center) ตรวจสอบประเมินความมั่นคงปลอดภัยตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๑๓ รวมทั้งส่วนของการจัดกิจกรรมการให้ความรู้ ความเข้าใจความตระหนักในความมั่นคงปลอดภัยด้านสารสนเทศ แก่บุคลากรรัฐสภา จึงทำให้บุคลากรรัฐสภาบางส่วน

ด้านโครงสร้างและบุคลากร

ไม่มีหน่วยงานที่มีอำนาจหน้าที่ในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ขาดแคลนบุคลากรเฉพาะด้านการรักษาความปลอดภัยสารสนเทศ ซึ่งการพัฒนาทักษะบุคลากรให้มีความเชี่ยวชาญด้านนี้ยังไม่สามารถทำได้ทันต่อความต้องการ

ด้านการพัฒนาระบบสารสนเทศ

การพัฒนาระบบสารสนเทศส่วนใหญ่คำนึงถึงฟังก์ชันการใช้งานเป็นหลัก จึงละเลยด้านความมั่นคงปลอดภัย ทำให้ระบบคอมพิวเตอร์มีช่องโหว่ และความเสี่ยงต่อการถูกโจมตี