<u>ระเบียบวาระที่ ๑.๔</u> ผลการศึกษาและข้อมูลประกอบการพิจารณาการจัดทำ (ร่าง) แผนบริหารความพร้อมต่อสภาวะวิกฤติ (Business Continuity Management : BCM) ของสำนักงานเลขาธิการวุฒิสภา

แผนบริหารความพร้อมต่อสภาวะวิกฤติ ของสำนักงานเลขาธิการวุฒิสภา<u>ที่ผ่านมา</u> (และชื่อเรียกอื่น)

ชื่อแผน	ภัยพิบัติและภาวะฉุกเฉิน	การดำเนินงาน
๑.แผนบริหารความต่อเนื่องของสำนักงานเลขาธิการวุฒิสภา ปีงบประมาณ พ.ศ. ๒๕๕๗ 	ภัยธรรมชาติ อุบัติเหตุ หรือการมุ่งร้ายต่อองค์กร เช่น อุทกภัย อัคคีภัย การก่อการประท้วง การก่อการจลาจล การก่อวินาศกรรม	- ดำเนินการให้เป็นไปตามเกณฑ์การพัฒนาคุณภาพการบริหารจัดการภาครัฐ (PMQA) หมวด ๖ การจัดการกระบวนการ - คณะอนุกรรมการ ฯ หมวด ๖ การจัดกระบวนการดำเนินการร่วมกับสำนักบริหารงานกลาง - มีการจัดทำแผนบริหารความต่อเนื่อง โดยนำภารกิจสำคัญของสำนักงานฯ มาเป็นตัวกำหนดและนำกลยุทธ์การบริหารความต่อเนื่องเข้ามารองรับ - มีการซักซ้อมแผนดำเนินการเพื่อรองรับภัยพิบัติและภาวะฉุกเฉิน เช่น แผนการซ้อมหนีไฟและการดับเพลิง
๒.แผนสำรองฉุกเฉินเพื่อป้องกันผลกระทบต่อการจัดการกระบวนการของสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๐ 	๑. อัคคีภัย ๒. แผ่นดินไหว ๓. อุทกภัย ๔. กรณีสถานการณ์ทางการเมือง/การชุมนุม ๕. วัตถุระเบิด หรือ วัตถุที่ต้องสงสัย ๖. กรณีไฟฟ้าดับ หรือไฟฟ้าขัดข้อง	- ดำเนินการต่อเนื่องมาจาก **แผนบริหารความต่อเนื่องของสำนักงานเลขาธิการวุฒิสภา ปีงบประมาณ พ.ศ. ๒๕๕๗** - จัดทำโดยสำนักบริหารงานกลาง - จัดทำแผนสำรองฉุกเฉินฯ โดยกำหนดภัยพิบัติและภาวะฉุกเฉิน ๖ ด้าน มาเป็นแผนรองรับภัยพิบัติและภาวะฉุกเฉิน ทั้งหมด ๖ แผนดำเนินการ - มีการซักซ้อมแผนดำเนินการเพื่อรองรับภัยพิบัติและภาวะฉุกเฉิน เช่น แผนการซ้อมหนีไฟและการดับเพลิง และมีการซักซ้อมความพร้อมของเจ้าหน้าที่ และความพร้อมของอุปกรณ์ - มีการกำหนดกระบวนการให้สัมภาษณ์ข่าวให้เป็นหน้าที่ของผู้บังคับบัญชาระดับสูง

ชื่อแผน	ภัยพิบัติและภาวะฉุกเฉิน	การดำเนินงาน
๓.แผนสำรองฉุกเฉินเพื่อป้องกันผลกระทบต่อการจัดการกระบวนการของสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๑ 	๑. อัคคีภัย ๒. แผ่นดินไหว ๓. อุทกภัย ๔. กรณีสถานการณ์ทางการเมือง/การชุมนุม ๕. วัตถุระเบิด หรือ วัตถุที่ต้องสงสัย ๖.กรณีไฟฟ้าดับ หรือไฟฟ้าขัดข้อง	- ดำเนินการต่อเนื่องมาจาก **แผนสำรองฉุกเฉินเพื่อป้องกันผลกระทบต่อการจัดการกระบวนการของสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๐** - จัดทำโดยสำนักบริหารงานกลาง - จัดทำแผนสำรองฉุกเฉิน ฯ โดยกำหนดภัยพิบัติและภาวะฉุกเฉิน ๖ ด้าน มาเป็นแผนรองรับภัยพิบัติและภาวะฉุกเฉิน ทั้งหมด ๖ แผนดำเนินการ - มีการซักซ้อมแผนดำเนินการเพื่อรองรับภัยพิบัติและภาวะฉุกเฉิน เช่น แผนการซ้อมหนีไฟและการดับเพลิง และมีการซักซ้อมความพร้อมของเจ้าหน้าที่ และความพร้อมอุปกรณ์ - มีการกำหนดหน้าที่การให้สัมภาษณ์ข่าว โดยให้เป็นหน้าที่ของผู้บังคับบัญชาระดับสูง *(ลักษณะการดำเนินงานเช่นเดียวกับปี ๒๕๖๐)*
๔.แผนการบริหารเหตุการณ์พิเศษ ของสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๓ 	๑. สถานการณ์การชุมนุม ๒. การก่อวินาศกรรม ๓. การจับตัวประกัน ๔. เหตุชุลมุนในการประชุมสภา ๕. อัคคีภัย ๖. แผ่นดินไหว	- ดำเนินการตามคำสั่งสภานิติบัญญัติแห่งชาติที่ ๑๘๗/๒๕๕๘ เรื่องแต่งตั้งคณะกรรมการพิจารณาปรับปรุงอาคารรัฐสภาและพัฒนาระบบรักษาความปลอดภัยของตำรวจรัฐสภา จึงแต่งตั้งคณะอนุกรรมการพิจารณายกร่างแผนปฏิบัติเผชิญเหตุกรณีเหตุฉุกเฉินและระเบียบรัฐสภาว่าด้วยการรักษาความปลอดภัยสถานที่ประชุมรัฐสภาและบริเวณรัฐสภา โดยมีผู้อำนวยการสำนักบริหารงานกลาง เป็นอนุกรรมการ - มีการดำเนินงานร่วมกับหน่วยงานภายนอก อาทิ สำนักงานตำรวจแห่งชาติ กองทัพภาคที่ ๑ กรุงเทพมหานคร การไฟฟ้านครหลวง การประปานครหลวง บ.ทีโอที จำกัด กรมการแพทย์ สน.เตาปูน กองบินตำรวจ กรมควบคุมมลพิษ เป็นต้น - มีการอบรมซักซ้อมการรักษาความปลอดภัยและการบริหารเหตุการณ์พิเศษให้มีความเป็นปัจจุบัน โดยมีวิทยากรผู้เชี่ยวชาญจากภายนอกมาให้ความรู้อย่างต่อเนื่อง

แผนบริหารความพร้อมต่อสภาวะวิกฤติ (ด้านเทคโนโลยีสารสนเทศและการสื่อสาร) ที่ผ่านมา ของสำนักงานเลขาธิการวุฒิสภาและรัฐสภา

ชื่อแผน	ภัยพิบัติและภาวะฉุกเฉิน	การดำเนินงาน
๑.แผนบริหารความต่อเนื่อง (BCP)ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานเลขาธิการวุฒิสภาประจำปีงบประมาณ พ.ศ. ๒๕๖๐ – ๒๕๖๓ 	เหตุการณ์อันเนื่องมาจาก - อุทกภัย - อัคคีภัย - ไฟดับ กระแสไฟฟ้าขัดข้อง ชุมนุมประท้วง/ จลาจล และเหตุความไม่สงบทางการเมืองต่าง ๆ - โรคระบาด	- ดำเนินการโดยคณะอนุกรรมการจัดทำแผนบริหารความต่อเนื่อง (BCP) ด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา - มีการจัดตั้งคณะทำงานในภาวะฉุกเฉิน (Emergency Team) - มีแผนย่อยได้แก่ ๑. แผนการบริหารความต่อเนื่องสำหรับคอมพิวเตอร์แม่ข่ายและการสำรองข้อมูล ๒.แผนบริหารความต่อเนื่องสำหรับระบบเครือข่าย สรุปเหตุการณ์ภัยคุกคามและผลกระทบจากเหตุการณ์ ผลกระทบ ความเสี่ยงและภัยคุกคาม / ด้านอาคาร/สถานที่ปฏิบัติงานหลัก / ด้านวัสดุอุปกรณ์ที่สำคัญ / ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ / ด้านบุคลากรหลัก / ด้านคู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสียที่สำคัญ อุทกภัย √ √ √ √ √ ไฟดับ √ √ √ √ - ชุมนุมประท้วง/จราจล √ - - √ √ อัคคีภัย √ √ √ √ - โรคระบาด √ - - √ -
๒.แผนรองรับภัยพิบัติและภาวะฉุกเฉินที่อาจมีต่อระบบฐานข้อมูล และการปฏิบัติการบนไซเบอร์ พ.ศ. ๒๕๖๒ – ๒๕๖๕ (ของสำนักงานเลขาธิการวุฒิสภา) 	**ภัยพิบัติจากภายนอก** ๑. ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องคอมพิวเตอร์แม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้นอุณหภูมิ แมลงกัดแทะ ฯลฯ ๒. การโจรกรรมอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล ๓. การเชื่อมต่อระบบอินเทอร์เน็ตเกิดความขัดข้อง ๔. ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ	- ดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ - ดำเนินการตามแผนการขับเคลื่อนแผนการพัฒนา Digital Parliament ของสำนักงานเลขาธิการวุฒิสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ - ๒๕๖๕) - เพื่อเป็นกรอบแนวทางในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร และเป็นไปตามกรอบการประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ ๔.๐ - มีการวางแผนการป้องกันการโจมตีทางไซเบอร์ การเตรียมพร้อมรองรับต่อภัยพิบัติและภาวะฉุกเฉินที่อาจมีผลต่อระดับฐานข้อมูล และปฏิบัติการบนไซเบอร์ เช่น แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม เป็นต้น

ชื่อแผน	ภัยพิบัติและภาวะฉุกเฉิน	การดำเนินงาน
	๖. การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศรวมทั้งความเสียหายหรือทำลายระบบข้อมูล ๗. ไวรัสคอมพิวเตอร์ ๘. การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง **ภัยพิบัติจากภายใน** ๑. ระบบคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย ๒. ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร ๓. เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน	
๓.แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล พ.ศ. ๒๕๖๒ – ๒๕๖๕ (ของสำนักงานเลขาธิการวุฒิสภา) 	๑.ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) ๒.ความเสี่ยงด้านบุคลากร (Human Risk) ๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีดิจิทัล (Hardware and Data Communication Risk)	- ดำเนินการตามยุทธศาสตร์สำนักงานเลขาธิการวุฒิสภา ฉบับที่ ๔ (พ.ศ. ๒๕๖๐ – ๒๕๖๔) และแผนขับเคลื่อนแผนพัฒนา Digital Parliament ของสำนักงานเลขาธิการวุฒิสภา ระยะ ๕ ปี (พ.ศ.๒๕๖๑ - ๒๕๖๕) - สำนักงาน ฯ ได้จัดทำคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ปีงบประมาณ พ.ศ. ๒๕๖๒ โดยการจัดทำระบบบริหารความเสี่ยงเป็นส่วนหนึ่งของตัวชี้วัดในคำรับรองการปฏิบัติราชการ

ชื่อแผน	ภัยพิบัติและภาวะฉุกเฉิน	การดำเนินงาน
	๔. ความเสี่ยงด้านระบบดิจิทัล (Software Risk) ๕. ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk) ๖. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ๗. ความเสี่ยงด้านการเงิน (Financial Risk) ๘. ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)	ของสำนักงานเลขาธิการวุฒิสภา ดังนั้น สำนักงานเลขาธิการวุฒิสภาจึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสารเทศและการสื่อสารประจำปี ๒๕๖๒-๒๕๖๕ - มีการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร และความเสี่ยงการโจมตีทางไซเบอร์ -มีการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่อยู่ในระดับสูง ๖ อันดับ ได้แก่ ๑. ลิขสิทธิ์ซอฟต์แวร์ ๒. การเชื่อมต่อระบบอินเทอร์เน็ต/ อินทราเน็ตขัดข้อง ๓. ไวรัสคอมพิวเตอร์/ Malware ๔. ช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร ๕. ความเสี่ยงจากการถูก Black List จาก Search Engine/ Spamhause ๖. การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง
๔.แผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา (Business Continuity Plan : BCP) พ.ศ. ๒๕๖๓ 	**เหตุภัยพิบัติทางธรรมชาติ เช่น** ๑. ไฟไหม้ ๒. น้ำท่วม ๓. แผ่นดินไหว เหตุการณ์อันเนื่องมาจากคน เช่น ๑) การทำงานผิดพลาด ๒) เหตุชุมนุมประท้วง หรือการจลาจล ๓) การปิดอาคาร เข้าพื้นที่ไม่ได้ ๔) การเกิดโรคระบาด **เหตุการณ์ภัยพิบัติที่ไม่สามารถปฏิบัติงานได้จากโครงสร้างพื้นฐาน เช่น** ๑) ระบบไฟฟ้าขัดข้อง ล้มเหลว เป็นเวลานาน	- ดำเนินการโดยคณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ – ๒๕๖๕) ได้มอบหมายให้คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒ – ๒๕๖๕) จัดทำแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา เพื่อเป็นกรอบแนวทางให้รัฐสามารถนำไปใช้ในการตอบสนองการปฏิบัติงานในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ - การจัดทำแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ประยุกต์ข้อกำหนดระบบ Business Continuity Management (BCM) ตามมาตรฐาน BS25999 มาตรฐาน ISO 22301-2012 (มอก.๒๒๓๐๑–๒๕๕๓)และอ้างอิงกับแนวทางการจัดทำคู่มือการเตรียมความพร้อมในสภาวะวิกฤตของ ก.พ.ร.มา

ชื่อแผน	ภัยพิบัติและภาวะฉุกเฉิน	การดำเนินงาน
	๒) ระบบประปาขัดข้อง ไม่มีน้ำใช้งาน ๓) ระบบเครือข่ายภายนอกล้มเหลว ๔) การสูญเสียอุปกรณ์เทคโนโลยีสารสนเทศ ๕) การล้มเหลวของโปรแกรมคอมพิวเตอร์	เป็นกรอบการวิเคราะห์ - เนื่องด้วยรัฐสภาได้มีการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับรัฐสภาแห่งใหม่และอยู่ระหว่างตรวจรับงานคาดว่าจะแล้วเสร็จภายในปีงบประมาณ ๒๕๖๓ แต่การให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารปัจจุบันยังใช้งานอยู่บนระบบงานเดิมของทั้ง ๒ องค์กร กล่าวคือ ระบบงานเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการสภาผู้แทนราษฎรและสำนักงานเลขาธิการวุฒิสภา ดังนั้นการจัดทำแผนต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภาฉบับนี้จึงพิจารณาจัดทำขึ้นภายใต้กรอบงานของระบบงานเดิมทั้งสิ้น
๕.แผนบริหารความเสี่ยงด้านสารสนเทศของรัฐสภา พ.ศ. ๒๕๖๓  	๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม ๒) ความเสี่ยงด้านบุคลากร (Human Risk) ๓) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร ๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ ๕) ความเสี่ยงด้านระบบข้อมูล	- จัดทำโดยคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒-๒๕๖๕) และดำเนินการให้เป็นไปตามแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑–๒๕๖๕) - ดำเนินการตามแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑–๒๕๖๕) - มีการจัดทำแผนภาพไดอะแกรม network ของสำนักงานเลขาธิการสภาผู้แทนราษฎรและสำนักงานเลขาธิการวุฒิสภา - มีการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศของรัฐสภา ๒๒ ด้าน และประเมินความเสี่ยงที่จะเกิดขึ้น พร้อมทั้งแนวทางรองรับ ได้แก่ ๑. ความเสี่ยงจากการใช้ซอร์ฟแวร์ที่ไม่มีลิขสิทธิ์ ๒. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง ๓. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware ๔. ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายใน

ชื่อแผน	ภัยพิบัติและภาวะฉุกเฉิน	การดำเนินงาน
		๕.ความเสี่ยงจากการถูก Black List โดย Search Engine หรือ spamhaus ๖.ความเสี่ยงจากการใช้โปรแกรมที่พัฒนาโดยผู้รับจ้างภายนอก(Outsource) และการขาดแผนบริหารความต่อเนื่อง ๗.ความเสี่ยงจากอัคคีภัย ๘.ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้ ๙. ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง ๑๐.ความเสี่ยงจากการเกิดอุทกภัย ๑๑. ความเสี่ยงจากแมลง หรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์หรือ สายไฟฟ้า /สายสัญญาณ ๑๒.ความเสี่ยงจากการโจรกรรม อุปกรณ์คอมพิวเตอร์แม่ข่ายหรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง ๑๓.ความเสี่ยงจากการไม่ทำการสำรองข้อมูลหรือทำการสำรองข้อมูลแต่ขาดการอัพเดท ๑๔.ความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์จากภายนอก ๑๕.ความเสี่ยงจากการโจมตีทางไซเบอร์สานักงานฯ ไม่ให้สามารถให้บริการได้ (Denial of Service-DoS) ๑๖.ความเสี่ยงจากระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหาย ๑๗.ความเสี่ยงจากการใช้ Wireless เข้าเครือข่ายอินทราเน็ต ๑๘.ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์ ๑๙.ความเสี่ยงจากวินาศภัย/การก่อการร้าย ๒๐.ความเสี่ยงจาก ความชื้น อุณหภูมิ ๒๑.ความเสี่ยงจากแผ่นดินไหว ๒๒.ความเสี่ยงจากการโจรกรรมฐานข้อมูล