แผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล
ของสำนักงานเลขาธิการวุฒิสภา
ประจำปี พ.ศ. 2563 - 2565

แผนการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา
ประจำปี พ.ศ. ๒๕๖๓ - ๒๕๖๕

จัดทำโดย

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา

พฤษภาคม ๒๕๖๓

สารบัญ

สารบัญรูป

สารบัญตาราง

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล

๑. หลักการและเหตุผล

การเปลี่ยนแปลงสภาพแวดล้อมในการดำเนินงานด้านระบบเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา ทั้งปัจจัยภายใน อาทิ การปรับเปลี่ยนแผนยุทธศาสตร์ กลยุทธ์ แผนพัฒนาเทคโนโลยีดิจิทัล การเปลี่ยนแปลงทรัพยากรภายในสำนักงาน การเปลี่ยนแปลงสถานที่และด้านการปฏิบัติงาน รวมถึงปัจจัยภายนอก อาทิ เหตุการณ์ความไม่สงบทางการเมือง ภัยธรรมชาติ โรคระบาด เป็นต้น อาจส่งผลกระทบให้การดำเนินงาน ของสำนักงานไม่เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงาน และแผนกลยุทธ์ ซึ่งจะ ก่อให้เกิดความเสี่ยงต่อสำนักงานโดยรวม การบริหารความเสี่ยงเป็นองค์ประกอบของการกำกับดูแลกิจการที่ดี ซึ่งนอกจากจะสนับสนุนให้องค์กร สามารถดำเนินงานได้บรรลุตามเป้าหมายที่กำหนดแล้ว ยังสามารถสร้างมูลค่าเพิ่มให้แก่ผู้มีส่วนได้ส่วนเสียของ องค์กร (Stakeholders) ได้อีกทางหนึ่ง สำนักงานเลขาธิการวุฒิภา จึงได้นำกรอบแนวทางการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ (Enterprise Risk Management – Integrated Framework) ตามแนวทาง COSO ERM มาประยุกต์ใช้เป็นกรอบและแนวทางในการพัฒนาระบบการบริหารความเสี่ยงของสำนักงาน ซึ่งมีวัตถุประสงค์ในการให้ผู้บริหาร เจ้าหน้าที่ที่เกี่ยวข้องในองค์กรตระหนักถึงความสำคัญของ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร และมีความเข้าใจตรงกันในคำนิยาม เป้าหมายและวัตถุประสงค์ อันจะเป็นการสร้าง ความรับผิดชอบอย่างทั่วถึงและเป็นไปในทิศทางเดียวกันทั่วทั้งสำนักงานได้อย่างมีประสิทธิภาพ เพื่อใช้เป็นแนวทางให้ผู้บริหาร เจ้าหน้าที่ทั่วทั้งองค์กร เป็นส่วนหนึ่งของการพัฒนา กระบวนการบริหารความเสี่ยงเพื่อสนับสนุนการดำเนินงานขององค์กรให้เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนเพื่อให้สำนักงานมีกรอบการดำเนินการที่ตอบสนองต่อเหตุการณ์ที่อาจส่งผลให้เกิดความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลและเทคโนโลยีสารสนเทศได้อย่างเป็นระบบและมีมาตรฐาน รวมทั้งมีการดำเนินการเพื่อสร้างพื้นฐานในการป้องกันความเสี่ยงระยะยาวที่สำคัญให้สำนักงาน เพื่อเป็นกลไกในการพัฒนาองค์ความรู้ด้านการบริหารความเสี่ยงสำหรับผู้บริหาร เจ้าหน้าที่ และสนับสนุนให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรได้อย่างยั่งยืน มีความตระหนักและมีความเข้าใจตรงกันถึงเป้าหมายวัตถุประสงค์ รวมทั้งแนวทางการบริหารความเสี่ยงด้านเทคโนลยีสารสนเทศและการสื่อสารของสำนักงาน เพื่อร่วมกันสร้างความพึงพอใจให้แก่ผู้มีส่วนได้ส่วนเสีย (Stakeholders) และสร้างมูลค่าเพิ่มให้องค์กร โดยพิจารณาถึงผลกระทบต่อเป้าหมายการดำเนินงานของสำนักงานให้เป็นไปตามหลักการกำกับดูแลกิจการที่ดี

การบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลและเทคโนโลยี เป็น องค์ประกอบสำคัญของการดำเนินงานด้านระบบเทคโนโลยีดิจิทัลเทคโนโลยีสารสนเทศและการสื่อสาร และด้านเทคโนโลยีดิจิทัล ของสำนักงานเลขาธิการวุฒิสภาเป็นอย่างมาก จึงมีความจำเป็นในการกำหนดนโยบายบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา เพื่อบังคับใช้ กับทุกหน่วยงานที่เกี่ยวข้องของสำนักงานเลขาธิการวุฒิสภาโดยมีวัตถุประสงค์เพื่อให้เจ้าหน้าที่ทุกระดับมีความรู้ความเข้าใจและตระหนักถึงหน้าที่ ความรับผิดชอบต่อการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจทัล และเทคโนโลยีสารสนเทศอยู่เสมอ และยังสนับสนุนให้เจ้าหน้าที่ทุกระดับชั้นเข้าใจ รวมถึงมีส่วนร่วมในการบริหารและจัดการความเสี่ยงด้านงระบบเทคโนโลยีดิจิทัล และเทคโนโลยีสารสนเทศในทุกขั้นตอนปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสาร ประกอบด้วยการวางระบบการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศภายในหน่วยงานของตนเองได้อย่างมีประสิทธิภาพ และเป็นการป้องกัน ควบคุม และลด ผลกระทบจากเหตุการณ์ความเสียหายที่อาจเกิดขึ้นต่อ โดยกระบวนการดังกล่าวจะอยู่ภายใต้การดูแลของ หัวหน้าส่วนงาน ผู้อำนวยกา และมีการกำกับ ดูแลและสั่งการโดย คณะทำงานด้านการบริหารความเสี่ยง

ข้าราชการฝ่ายนิติบัญญัติได้นำแนวนโยบายและแนวปฏิบัติของฝ่ายบริหารมาดำเนินการด้วยหลักการบริหารจัดการภาครัฐแนวใหม่ตามพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. ๒๕๔๖ มุ่งเน้นการพัฒนาระบบราชการไทยให้มีขีดสมรรถนะสูง สามารถรองรับการเปลี่ยนแปลงภายใต้สภาพแวดล้อมที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ไม่แน่นอน หน่วยงานภาครัฐต้องมีการบริหารจัดการความเสี่ยงภายใต้ยุคไร้พรมแดนโดยเฉพาะการเติบโตและวิวัฒนาการเร็วด้านเทคโนโลยีสารสนเทศและการสื่อสารส่งผลทำให้ประเทศทั่วโลกมีการติดต่อสื่อสารกันตลอดเวลา ๒๔ ชั่วโมงไม่มีวันหยุด และต่อเนื่องอยู่ตลอดเวลา อันเป็นกลไกหลักในการพัฒนาองค์กรให้มีประสิทธิภาพและประสิทธิผล พระราชกฤษฎีกาดังกล่าวยังส่งผลให้ส่วนราชการต้องจัดทำคำรับรองการปฏิบัติราชการ การบริหารราชการเพื่อให้เกิดผลสัมฤทธิ์ต่อภารกิจของรัฐ สำนักงานเลขาธิการวุฒิสภาได้จัดทำคำรับรองการปฏิบัติราชการของส่วนราชการสังกัดรัฐสภา ปีงบประมาณ พ.ศ. ๒๕๖๓ โดยการจัดทำระบบบริหารความเสี่ยงเป็นส่วนหนึ่งของตัวชี้วัดในคำรับรองการปฏิบัติราชการของสำนักงานเลขาธิการวุฒิสภา และเป็นการดำเนินการตามแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๓ – ๒๕๖๕ ดังนั้น สำนักงานเลขาธิการวุฒิสภาจึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสารสนเทศและการสื่อสารประจำปี ๒๕๖๓ - ๒๕๖๕

๒. วัตถุประสงค์

๒.๑ เพื่อให้มีการวิเคราะห์ความเสี่ยงของระบบเทคโนโลยีดิจิทัล

๒.๒ จัดทำแผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา ประจำปีงบประมาณ พ.ศ. ๒๕๖๓ - ๒๕๖๕

๒.๓ เพื่อให้มีมาตรการ การวางแผน ควบคุม และแก้ไขความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล การโจมตีการปฏิบัติการทางไซเบอร์ ของสำนักงานฯ ได้อย่างเหมาะสมในเวลาที่จำกัดอย่างมีประสิทธิภาพ

๒.๔ เพื่อช่วยเพิ่มประสิทธิภาพในการบริหารความเสี่ยงอันจะมีผลกระทบต่อการดำเนินงานให้เป็นไปตามแนวนโยบาย และเป้าประสงค์ เพื่อพิจารณาดำเนินการหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มดำเนินงาน หรือดำเนินงานตามแผน

๒.๕ เพื่อเป็นแนวทางในการดำเนินการ การกำกับดูแล ตรวจสอบการบริหารจัดการ ข้อมูลสารสนเทศ ระบบการทำงานที่ปรับเป็นดิจิทัลเต็มรูปแบบ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล ของสำนักงานฯ ให้บุคลากรสำนักงานฯ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ และตรงตามความต้องการ

๒.๖ เพื่อให้ผู้ปฏิบัติงานตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นได้ และดำเนินการจัดการความเสี่ยงที่เกี่ยวข้องให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านระบบเทคโนโลยีทิจิทัล เทคโนโลยีสารสนเทศและการสื่อสาร มีความเข้าใจกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานฯ อย่างถ่องแท้

๒.๗ เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับแผนงานด้านเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสารให้ได้รับการยอมรับและมีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและมีความต่อเนื่อง

๓. วิสัยทัศน์ และ พันธกิจ ตามแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๓ – ๒๕๖๕ ที่เกี่ยวข้องด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา

๓.๑ วิสัยทัศน์ ของสำนักงานเลขาธิการวุฒิสภา

กำหนดไว้ว่า “เป็นองค์กรหลักด้านนิติบัญญัติของประเทศที่มีสมรรถนะสูงในการสนับสนุนภารกิจวุฒิสภาเพื่อประชาชนและประโยชน์ส่วนรวม”

๓.๒ พันธกิจ

กำหนดไว้ว่า

(๑) สนับสนุนการขับเคลื่อนภารกิจด้านนิติบัญญัติ

(๒) สนับสนุนภารกิจด้านการติดตาม เสนอแนะ และเร่งรัดการปฏิรูปประเทศและการดำเนินการตามยุทธศาสตร์ชาติ

(๓) ยกระดับการพัฒนางานด้านกฎหมายและงานด้านวิชาการของวุฒิสภา

(๔) บริหารจัดการให้เป็นองค์กรที่มีสมรรถนะสูง ทันสมัย ตามหลักธรรมาภิบาลและทันต่อการเปลี่ยนแปลง

๓.๓ แผนงานและแนวทางการพัฒนา

(๑) แผนปฏิบัติราชการเรื่องที่ ๑ ยกระดับการสนับสนุนงานด้านนิติบัญญัติ

เป้าหมายที่ ๑ สนับสนุนงานด้านนิติบัญญัติอย่างมีประสิทธิภาพ

เป้าหมายที่ ๒ พัฒนางานด้านกฎหมายและด้านวิชาการ รวมทั้งข้อมูลการวิจัยที่ตอบสนองต่อความต้องการของวุฒิสภา

แนวทางการพัฒนา (๑) ยกระดับการพัฒนางานด้านกฎหมาย งานด้านวิชาการ และข้อมูลการวิจัยให้เป็นไปอย่างมีประสิทธิภาพ (๒) พัฒนาเครือข่าย และความร่วมมือของภาคส่วนต่าง ๆ เพื่อสนับสนุนงานวุฒิสภา

(๒) แผนปฏิบัติราชการเรื่องที่ ๒ พัฒนางานด้านการติดตาม เสนอแนะ และเร่งรัดการดำเนินการตามแผนการปฏิรูปประเทศ และการดำเนินการตามยุทธศาสตร์ชาติ

เป้าหมาย สนับสนุนการติดตาม เสนอแนะ และเร่งรัดการดำเนินการตามแผนการปฏิรูปประเทศ และการดำเนินการตามยุทธศาสตร์ของวุฒิสภาอย่างมีประสิทธิภาพ

แนวทางการพัฒนา พัฒนากลไกการสนับสนุนการขับเคลื่อนภารกิจของวุฒิสภาในการติดตาม เสนอแนะ และเร่งรัดการดำเนินการตามแผนการปฏิรูปประเทศ และการดำเนินการตามยุทธศาสตร์ชาติ

(๓) แผนปฏิบัติราชการเรื่องที่ ๓ พัฒนาศักยภาพของบุคลากรเพื่อให้สอดคล้องกับความต้องการของผู้รับบริการเชิงรุก และทันต่อการเปลี่ยนแปลงในอนาคต

เป้าหมายที่ ๑ เพื่อให้มีนโยบายและระบบหรือกลไกในการบริหารงานบุคคลที่สอดคล้องกับยุทธศาสตร์และการเปลี่ยนแปลงในอนาคต

เป้าหมายที่ ๒ เพื่อพัฒนาบุคลากรทุกประเภทให้มีความรู้ ความสามารถสูง มีทักษะการคิดวิเคราะห์และสามารถปรับตัวให้ทันต่อการเปลี่ยนแปลง

แนวทางการพัฒนา (๑) พัฒนาระบบบริหารทรัพยากรบุคคลให้สอดรับและสนับสนุนภารกิจขององค์กร ทั้งในปัจจุบันและอนาคตอย่างมีประสิทธิภาพ (๒) พัฒนาบุคลากรให้มีศักยภาพขับเคลื่อนยุทธศาสตร์องค์กรได้อย่างเป็นระบบและหลากหลาย (๓) สร้างเสริมและพัฒนาคุณภาพชีวิตการทำงานของบุคลากรทั้งสภาพแวดล้อมและบรรยากาศในการปฏิบัติงานภายในองค์กร (๔) ส่งเสริมให้บุคลากรปฏิบัติตนตามประมวลจริยธรรม เพื่อให้เอื้อต่อการบรรลุเป้าหมายขององค์กร

(๔) แผนปฏิบัติราชการเรื่องที่ ๔ พัฒนาขีดความสามารถองค์กรให้มีสมรรถนะสูง

เป้าหมายที่ ๑ เพื่อพัฒนาการบริหารจัดการองค์กรให้มีประสิทธิภาพ มีขีดสมรรถนะสูงและทันสมัย

เป้าหมายที่ ๒ เพื่อพัฒนาระบบข้อมูลสารสนเทศของสำนักงานเลขาธิการวุฒิสภาให้มีการเชื่อมโยงและบูรณาการ เพื่อสามารถสนับสนุนกระบวนการนิติบัญญัติได้อย่างมีประสิทธิภาพ

เป้าหมายที่ ๓ เพื่อพัฒนาโครงสร้างพื้นฐานและระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภาให้เป็นไปตามมาตรฐานสากล รองรับการให้บริการได้อย่างทั่วถึงและเท่าเทียม

เป้าหมายที่ ๔ เพื่อพัฒนาขีดความสามารถและเสริมสร้างศักยภาพของสมาชิกวุฒิสภาและบุคลากรของสำนักงานเลขาธิการวุฒิสภา ให้สามารถใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารได้อย่างมีประสิทธิภาพ มีการคิดวิเคราะห์ปรับใช้เทคโนโลยีใหม่ได้ตลอดเวลา

แนวทางการพัฒนา (๑) พัฒนาระบบบริหารจัดการองค์กรให้มีขีดสมรรถนะสูงและทันสมัย (๒) ส่งเสริมการสร้างนวัตกรรมในการปฏิบัติงาน (๓) พัฒนาระบบงานและฐานข้อมูล โดยมีการบูรณาการ การเปิดกว้างและเชื่อมโยงกันเพื่อมุ่งสู่การเป็น Digital Senate (๔) พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นไปตามมาตรฐานสากล (๕) ส่งเสริมและสนับสนุนให้สมาชิกวุฒิสภา และบุคลากร

มีความรู้ ความสามารถในการประยุกต์ใช้ระบบ Digital อย่างมีประสิทธิภาพ มีการคิดวิเคราะห์ปรับใช้เทคโนโลยีใหม่ได้ตลอดเวลา

(๕) แผนปฏิบัติราชการเรื่องที่ ๕ พัฒนาและเสริมสร้างการเมืองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข และส่งเสริมการมีส่วนร่วมของประชาชน

เป้าหมายที่ ๑ ประชาชนมีความรู้ ความเข้าใจ และการรับรู้ที่ดีในทางการเมือง การปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

เป้าหมายที่ ๒ ประชาชนและภาคประชาสังคมมีส่วนร่วมทางการเมืองตามรัฐธรรมนูญ

แนวทางการพัฒนา (๑) เสริมสร้างความรู้ ความเข้าใจ และมีส่วนร่วมอย่างถูกต้องต่อการเมือง การปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข และวัฒนธรรมทางการเมืองในระบอบประชาธิปไตย (๒) จัดทำสื่อเกี่ยวกับการให้ความรู้ทางด้านการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข เพื่อเผยแพร่ให้แก่ประชาชนผ่านหน่วยงานและช่องทางต่าง ๆ (๓) ส่งเสริมการมีส่วนร่วมในทางการเมือง การปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข และวัฒนธรรมทางการเมืองในระบอบประชาธิปไตยของวุฒิสภา

๔. วิสัยทัศน์ และยุทธศาสตร์ ตามแผนขับเคลื่อนแผนพัฒนา Digital Parliament ของสำนักงานเลขาธิการวุฒิสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ – ๒๕๖๕)

๔.๑ วิสัยทัศน์

กำหนดไว้ว่า “รัฐสภาดิจิทัล (Digital Pariament)” หมายถึงองค์กรที่สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลได้อย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใด เพื่อสนับสนุนงานด้านนิติบัญญัติ

๔.๒ ยุทธศาสตร์ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร เป้าประสงค์หลัก และกลยุทธ์

<u>ยุทธศาสตร์ที่ ๑</u> พัฒนาระบบและบูรณาการฐานข้อมูลมุ่งสู่การเป็น Digital Parliament

<u>กลยุทธ์</u>

๑.๑ พัฒนาระบบข้อมูลและสารสนเทศของรัฐสภามีการเชื่อมโยงและบูรณาการเพื่อให้บริการอย่างมีประสิทธิภาพ

๑.๒ พัฒนาระบบบริการด้านสารสนเทศ ให้มีข้อมูลที่ถูกต้อง ทันสมัย รองรับความต้องการของผู้บริการและประชาชน

<u>ยุทธศาสตร์ที่ ๒</u> พัฒนาโครงสร้างพื้นฐาน และระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามมาตรฐานสากล

<u>กลยุทธ์</u>

๒.๑ พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

๒.๒ พัฒนาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นไปตามมาตรฐานสากลรองรับการให้บริการได้อย่างทั่วถึงและเท่าเทียม

<u>ยุทธศาสตร์ที่ ๓</u> ส่งเสริมและสนับสนุน ให้สมาชิกรัฐสภา และบุคคลในวงงานรัฐสภา มีความรู้ ความสามารถ และทักษะในการประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ

<u>กลยุทธ์</u>

๓.๑ พัฒนาสมรรถนะบุคลากรของรัฐสภาด้านการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓.๒ ส่งเสริม สนับสนุนให้สมาชิกรัฐสภาและบุคลากรในวงงานของรัฐสภาใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสร้างสรรค์

๓.๓ ส่งเสริม สนับสนุน บุคลากร ให้มีการศึกษา วิจัย และพัฒนาทางด้านนวัตกรรมและเทคโนโลยี รองรับความต้องการของผู้รับบริการและประชาชน

จากวิสัยทัศน์ และ พันธกิจ ตามแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๓ – ๒๕๖๕ ที่เกี่ยวข้องด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภาและแผนขับเคลื่อนแผนพัฒนา Digital Parliament ของสำนักงานเลขาธิการวุฒิสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ – ๒๕๖๕) ข้างต้น สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา ซึ่งมีหน้าที่หลักในการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน ฯ จะเป็นผู้รับผิดชอบดำเนินการในการกำหนดแผนการปฏิบัติงานตามแนวทางและแผนในการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล โดยได้พิจารณาจากแนวทางด้านการพัฒนาฐานข้อมูลและสารสนเทศและการสื่อสาร และเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภาที่มีส่วนหลักๆ หลายด้าน เช่น

๑) ด้านระบบดิจิทัล (Digital System)

๒) ด้านคอมพิวเตอร์แม่ข่าย (Server)

๓) ด้านคอมพิวเตอร์ลูกข่าย และอุปกรณ์ต่อพ่วง (Clients and Peripherals)

๔) ด้านบุคลากร (Human Resources)

๕) ด้านเครือข่าย (Networks)

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร ในฐานะผู้ดูแลระบบเครือข่ายสารสนเทศและการสื่อสาร ซึ่งหมายถึง ผู้ที่ได้รับมอบหมายจากเลขาธิการวุฒิสภา ให้มีหน้าที่

รับผิดชอบในการดูแล บำรุงรักษาเครือข่ายสารสนเทศและการสื่อสารของสำนักงานฯ ที่สามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ ระบบการสื่อสารข้อมูล ระบบสารสนเทศและการสื่อสารของสำนักงานฯ เพื่อการบริหารจัดการ นอกเหนือจากนั้นยังเป็นผู้รับผิดชอบการบริหารจัดการให้เป็นไปตามแผนบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Risk Management) รวมถึงความเสี่ยงทางด้านระบบเทคโนโลยีดิจิทัล เพราะหากมีการวางแผนที่ดีและมีการจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพแล้ว จะลดความเสี่ยงระบบเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสาร ที่อาจจะเกิดขึ้นได้ตามสภาวการณ์ต่างๆ อีกทั้งยังอำนวยความสะดวกในการดำเนินการ สอดคล้องกับกรอบการปฏิบัติงานราชการสำนักงานฯ มีแนวทางในการป้องกันและแก้ไขความเสี่ยงที่อาจจะเกิดขึ้นได้ ซึ่งจะช่วยให้การบริหารงานของสำนักงานฯ รวมถึงการให้บริการแก่สมาชิกวุฒิสภา คณะกรรมาธิการ ผู้มีส่วนได้ส่วนเสีย และประชาชนได้อย่างมีประสิทธิภาพสูงสุด และเพื่อเป็นการรองรับการให้บริการตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

การบริหารความเสี่ยงนั้น มีความสำคัญอย่างยิ่งต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ตามพระราชกฤษฎีกาว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ. ๒๕๔๖ เนื่องจากการบริหารความเสี่ยง เป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้สำนักงานฯ บรรลุเป้าประสงค์ที่ตั้งไว้ และเป็นการพัฒนาผลการปฏิบัติงานของสำนักงานฯ ที่จะนำไปสู่การใช้ทรัพยากรอย่างมีประสิทธิภาพและคุ้มค่า ตลอดจนสามารถพัฒนาคุณภาพบริการที่ดีให้แก่ผู้รับบริการและประชาชนทั่วไป

๕. ความเสี่ยง ลักษณะของความเสี่ยง และการบริหารความเสี่ยง

๕.๑ ความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ใดๆ ที่อาจจะเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งจะส่งผลกระทบหรือสร้างความเสียหาย ทั้งที่สามารถตีมูลค่าเป็นตัวเงินได้ และที่ไม่สามารถตีมูลค่าเป็นตัวเงินได้ หรือ อาจก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุเป้าประสงค์ตามภารกิจหลักและเป็นไปตามแผนปฏิบัติราชการของสำนักงานฯ

๕.๒ ลักษณะของความเสี่ยง

ลักษณะของความเสี่ยงสามารถแบ่งออกได้เป็น ๓ ลักษณะ ดังนี้

๑) ปัจจัยเสี่ยง หมายถึง สาเหตุที่จะทำให้เกิดความเสี่ยง

๒) เหตุการณ์เสี่ยง หมายถึง เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงานหรือนโยบาย

๓) ผลกระทบของความเสี่ยง หมายถึง ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์เสี่ยง

๕.๓ การบริหารความเสี่ยง

การบริหารความเสี่ยง หมายถึง ระบบการบริหารและควบคุม รวมทั้งกระบวนการดำเนินงานต่างๆ เพื่อที่จะลดสาเหตุของโอกาสที่จะก่อให้เกิดความเสียหาย เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ สามารถประเมินผลควบคุม และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าประสงค์ตามภารกิจหลัก และเป้าหมายตามแผนปฏิบัติราชการของสำนักงานฯ เป็นสำคัญ

การบริหารความเสี่ยงมีความจำเป็นที่จะต้องอาศัยขั้นตอนที่ต่อเนื่อง เนื่องจากมีการระบุความเสี่ยงอันจะมีผลกระทบจากความเสี่ยง และมาตรการหรือแผนปฏิบัติการในการจัดการความเสี่ยงนั้นได้ถูกดำเนินการตามแผนที่วางไว้

๖. กระบวนการในการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสาร

ปัจจุบันระบบเทคโนโลยีดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญในการดำเนินงานของสำนักงานเลขาธิการวุฒิสภา ในส่วนของการบริหารจัดการ การจัดเก็บข้อมูลตลอดจนการใช้เครื่องคอมพิวเตอร์แม่ข่าย การจัดทำและพัฒนาระบบเทคโนโลยีดิจิทัลในภาพรวม มุ่งหวังที่จะให้ระบบดิจิทัลมีส่วนช่วยในการปฏิบัติงานรอบรับภารกิจของสำนักงานฯ มีความสะดวก รวดเร็ว และมีประสิทธิภาพมากยิ่งขึ้น แต่การนำเทคโนโลยีดิจิทัลมาใช้ ย่อมมีความเสี่ยงหลายประการด้วยกัน

การวางแผนและการบริหารความเสี่ยงของระบบเทคโนโลยีดิจิทัล จึงเป็นเรื่องสำคัญและควรมีการเตรียมการที่ดี หากสำนักงานฯ ไม่มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัลที่รัดกุมเพียงพอ อาจส่งผลกระทบต่อการดำเนินงานและสร้างความเสียหายต่อสำนักงานฯ ได้ ทั้งในด้านการพัฒนาสำนักงานฯ การสนับสนุนผู้มีส่วนได้ส่วนเสีย การพัฒนาบุคลากร และความคุ้มค่าทางด้านงบประมาณที่ใช้

ดังนั้น การบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล จึงต้องมีทั้งการวางแผนเพื่อขจัดหรือลดความเสี่ยง และการประเมินผลในการบริหารจัดการความเสี่ยง เพื่อลดโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่อาจเกิดขึ้น และสามารถประเมินเป็นเชิงปริมาณหรือเชิงคุณภาพได้ ซึ่งมีขั้นตอนในการบริหารจัดการความเสี่ยง ดังนี้

ขั้นตอนที่ ๑ ขั้นตอนของการระบุความเสี่ยงและผลกระทบที่มีผลกระทบต่อข้อมูลดิจิทัล

ขั้นตอนที่ ๒ ขั้นตอนการประเมินถึงความเป็นไปได้ที่จะเกิดความเสี่ยงและความรุนแรงของผลกระทบ โดยผลกระทบจากผลการประเมินความเสี่ยงที่จะเกิดขึ้นต่อข้อมูลดิจิทัล โดยความเสี่ยงนั้นจะส่งผลกระทบต่อระบบในหลายๆ ด้าน ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงอันจะก่อให้เกิดความเสียหายแตกต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้นขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของสำนักงานฯ

ขั้นตอนที่ ๓ ขั้นตอนการวางแผนกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยง เพื่อให้สามารถบรรลุเป้าประสงค์ หรือใกล้เคียงกับเป้าประสงค์ที่กำหนดไว้ ในการวางแผนจะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อให้สามารถลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบของสำนักงานฯ เป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ รวมถึงป้องกัน แก้ไข และควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบ โดยสามารถดำเนินการตามแผนได้

ขั้นตอนที่ ๔ ขั้นตอนการติดตามข้อมูลเพื่อทราบร่องรอยของความเสี่ยง ในขั้นตอนนี้เจ้าหน้าที่ที่รับผิดชอบต้องมีการรวบรวมและรายงานข้อมูลความเสี่ยงในระยะยาวและข้อมูลที่เกี่ยวข้อง เพื่อนำเสนอให้ผู้บังคับบัญชาทราบและมีการทำบันทึกไว้เป็นหลักฐาน

ขั้นตอนที่ ๕ ขั้นตอนการติดตาม กำกับ และตรวจสอบ การปฏิบัติการควบคุมความเสี่ยง มีการตรวจสอบการทำงานของเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรักษาความมั่นคงปลอดภัยของระบบ โดยมีหลักฐานประกอบการปฏิบัติหน้าที่ตามระยะเวลาที่กำหนดให้

๗. ประเภทความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล

เพื่อระดมความคิดเห็นเกี่ยวกับแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา คณะกรรมการกำหนดแนวนโยบายและแผนที่เกี่ยวข้องกับด้านเทคโนโลยีดิจิทัล และเจ้าหน้าที่จากสำนักเทคโนโลยีสารสนเทศและการสื่อสารได้ประชุมระดมสมองร่วมกัน เพื่อระบุความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา ประเมินถึงความเป็นไปได้ที่จะเกิดความเสี่ยง ตลอดจนความรุนแรงของผลกระทบที่อาจเกิดขึ้น การประชุมมีขึ้นเมื่อวันที่ ๒๕ มิถนายน พ.ศ. ๒๕๖๒ เวลา ๑๓.๓๐-๑๕.๓๐ น. ณ ห้องประชุมสำนักเทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๑๓ สำนักงานเลขาธิการวุฒิสภา อาคารสุขประพฤติ ผลจากการประชุมดังกล่าว การสัมภาษณ์ และการศึกษาข้อมูลจากเอกสารที่เกี่ยวข้อง สามารถแบ่งประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา ตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้เป็น ๘ ประเภท ดังนี้

๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

๒) ความเสี่ยงด้านบุคลากร (Human Risk)

๓) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีดิจิทัล (Hardware and Data Communication Risk)

๔) ความเสี่ยงด้านระบบดิจิทัล (Software Risk)

๕) ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)

๖) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

๗) ความเสี่ยงด้านการเงิน (Financial Risk)

๘) ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)

๗.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย การเกิดโรคระบาด ที่มีผลกระทบต่อกระบวนการทำงานด้านเทคโนโลยีสารสนเทศ รวมถึงการไม่มีระบบรักษาความปลอดภัยศูนย์สารสนเทศ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

การบริหารจัดการความเสี่ยงด้านกายภาพและสิ่งแวดล้อม ประกอบไปด้วย

๗.๑.๑ การกำหนดที่ตั้งของเครื่องคอมพิวเตอร์ การเดินสายไฟฟ้า สายสัญญาณของระบบต่างๆ โดยเน้นความปลอดภัย และหลีกเลี่ยงไม่ตั้งระบบไว้ในจุดที่มีความเสี่ยงสูง รวมทั้งมีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้น เช่น การตั้งเครื่องคอมพิวเตอร์แม่ข่าย การติดตั้งตู้ Rack สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Servers) การติดตั้งพื้นยก (Raised Floor) ระบบเครื่องปรับอากาศที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้น

๗.๑.๒ การควบคุมการเข้า – ออก ห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงเป็นพื้นที่ เขตหวงห้ามเฉพาะ โดยกำหนดสิทธิการเข้า - ออก ห้องคอมพิวเตอร์แม่ข่ายให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง โดยใช้ระบบเปิด-ปิดประตูอัตโนมัติด้วยแม่เหล็ก โดยใช้บัตรประจำตัว เช่น Proximity Card ที่สามารถกำหนดสิทธิ์และบันทึกการใช้งานได้ รวมถึงระบบตรวจจับความเคลื่อนไหวและบันทึกภาพภายในห้องเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง โดยสำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานฯ เป็นผู้รับผิดชอบ และมีใช้อยู่ในปัจจุบัน

๗.๑.๓ การป้องกันความเสียหายจากอัคคีภัย โดยการวางระบบป้องกันไฟที่เหมาะสม โดยทำการติดตั้งระบบตรวจจับควันไฟ ตรวจจับความร้อน และระบบดับเพลิงอัตโนมัติด้วยสารเคมีภายในสำนักเทคโนโลยีสารสนเทศฯ และห้องคอมพิวเตอร์แม่ข่ายของสำนักงานเลขาธิการวุฒิสภา ชั้น ๑๓ อาคารสุขประพฤติ และจัดเตรียมความพร้อม ทั้งในแง่ของการนำระบบบางส่วนที่ติดตั้งใช้งานอยู่ที่อาคารสุขประพฤติไปใช้ที่รัฐสภาแห่งใหม่ หรือการติดตั้งระบบใหม่ทั้งหมด ทั้งนี้ขึ้นอยู่กับระยะเวลาที่จะย้ายไปยังอาคารรัฐสภาใหม่และอายุการใช้งานของระบบปัจจุบันที่ใช้งานอยู่ ณ อาคารสุขประพฤติ ซึ่งจะมีส่วนสัมพันธ์กับการจัดเตรียมงบประมาณสำหรับดำเนินการที่อาคารรัฐสภาใหม่ ได้แก่

๑) ติดตั้งระบบตรวจจับควันไฟ และความร้อนความไวสูง (Very Early Warning Smoke Detection Aspirating System)

๒) ติดตั้งระบบดับเพลิงอัตโนมัติด้วยสารเคมี (Automatic Chemical Fire Suppression System)

๗.๑.๔ การป้องกันความเสี่ยงจากระบบไฟฟ้าขัดข้อง โดยมีการติดตั้งเครื่องสำรองไฟฟ้า (UPS) ให้มีกำลังไฟเพียงพอต่อการสำรองไฟฟ้า เพื่อการใช้งานได้อย่างน้อยไม่ต่ำกว่า ๓๐ นาที และสามารถสั่งปิด (Shutdown) เครื่องคอมพิวเตอร์แม่ข่ายได้ทั้งหมด หลังจากที่ไฟฟ้าดับเกิน ๓๐ นาที และติดตั้งระบบเครื่องกำเนิดไฟฟ้าสำรอง (Electrical Generator) สำหรับการสำรองไฟฟ้ากรณีที่ระบบไฟฟ้าปกติดับนานเกินกว่า ๓๐ นาที ทั้งนี้ ขึ้นอยู่กับความจำเป็นในการใช้งานเมื่อไฟฟ้าดับนานเกินกว่า ๓๐ นาที เพื่อสำรองให้เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสาร

เชื่อมโยงระบบเครือข่ายภายในสำนักเทคโนโลยีสารสนเทศฯ ของสำนักงานเลขาธิการวุฒิสภา ชั้น ๑๓ อาคารสุขประพฤติ สามารถใช้งานได้ ทั้งนี้ จะต้องมีการจัดเตรียมด้านสถานที่สำหรับระบบเครื่องกำเนิดไฟฟ้าสำรอง (Electrical Generator) ซึ่งต้องใช้สถานที่ที่สามารถรองรับน้ำหนักได้เพียงพอ เนื่องจากเครื่องมีน้ำหนักมาก และใช้เครื่องยนต์ดีเซล จึงอาจเกิดมลภาวะโดยรอบ และจัดเตรียมความพร้อมทั้งในแง่ของการนำระบบบางส่วนที่ติดตั้งใช้งานอยู่ที่อาคารสุขประพฤติไปใช้ที่รัฐสภาแห่งใหม่หรือการติดตั้งระบบใหม่ทั้งหมด ทั้งนี้ ขึ้นอยู่กับระยะเวลาที่จะย้ายไปยังอาคารรัฐสภาใหม่และอายุการใช้งานของระบบปัจจุบันที่ใช้งานอยู่ ณ อาคารสุขประพฤติ ซึ่งจะมีส่วนสัมพันธ์กับการจัดเตรียมงบประมาณสำหรับดำเนินการที่อาคารรัฐสภาใหม่ โดยพิจารณาขนาดและความต้องการกำลังไฟฟ้าให้เหมาะสมแก่อุปกรณ์ที่จะติดตั้ง ได้แก่

๑) ติดตั้งระบบสำรองไฟฟ้า (Uninterrupted Power Supply- UPS)

๒) ติดตั้งระบบเครื่องกำเนิดไฟฟ้าสำรอง (Electrical Generator หรือ Power Generator)

๗.๑.๕ การป้องกันความเสี่ยงจากระบบควบคุมอุณหภูมิและความชื้นให้เหมาะสม โดยการติดตั้งเครื่องปรับอากาศ แบบ Precision ที่สามารถควบคุมอุณหภูมิและค่าความชื้นให้มีระดับเหมาะสมภายในสำนักเทคโนโลยีสารสนเทศฯ ของสำนักงานเลขาธิการวุฒิสภา ชั้น ๑๓ อาคารสุขประพฤติ และจัดเตรียมความพร้อมทั้งในแง่ของการนำระบบบางส่วนที่ติดตั้งใช้งานอยู่ที่อาคารสุขประพฤติไปใช้ที่รัฐสภาแห่งใหม่ หรือการติดตั้งระบบใหม่ทั้งหมด ทั้งนี้ ขึ้นอยู่กับระยะเวลาที่จะย้ายไปยังอาคารรัฐสภาใหม่และอายุการใช้งานของระบบปัจจุบันที่ใช้งานอยู่ ณ อาคารสุขประพฤติ ซึ่งจะมีส่วนสัมพันธ์กับการจัดเตรียมความพร้อมและงบประมาณสำหรับดำเนินการที่อาคารรัฐสภาใหม่ ได้แก่

๑) ระบบปรับอากาศสำหรับศูนย์สารสนเทศ (Precision Air Conditioning System)

๒) ระบบควบคุมความชื้นสำหรับศูนย์สารสนเทศ (Humidity Control System)

๓) ระบบตรวจจับการรั่วซึมของน้ำสำหรับศูนย์สารสนเทศ (Water Leak Detection System)

๗.๑.๖ ความเสี่ยงในเรื่องการปฏิบัติงานจากภายนอกโดยเข้า VPN เครือข่ายเสมือน มีการความเสี่ยงในการบุกรุกจากภายนอกเพิ่มขึ้น ต้องมีระบบรักษาความปลอดภัยอย่างแน่นหนาเพิ่มขึ้น

๗.๑.๗ ความเสี่ยงในเรื่องงบประมาณที่จะดำเนินการได้อย่างมีประสิทธิภาพสูงสุดและเกิดความต่อเนื่อง

๗.๑.๘ ความเสี่ยงในเรื่องประเด็นนโยบายของผู้บริหาร ที่ให้น้ำหนักและความสำคัญเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร หากมีการเปลี่ยนแปลงจะส่งผลกระทบต่อการปฏิบัติงานและแนวทางในการดำเนินการขั้นตอนต่างๆ ที่เหมาะสมต่อไป

๗.๒ ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร เทคโนโลยีดิจิทัล สำนักงานเลขาธิการวุฒิสภา ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรง และทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

การบริหารจัดการความเสี่ยงด้านบุคลากร มีแนวทางดำเนินการ ดังนี้

๗.๒.๑ การกำหนดโครงสร้าง รวมถึงการมอบหมายงานในหน้าที่ให้แก่บุคลากรด้านเทคโนโลยีดิจิทัล ที่มีความเหมาะสม คือ มีความรู้ และมีประสบการณ์เพียงพอ ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีด้านการรักษาความปลอดภัยด้านข้อมูลและเครือข่ายระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Data and Network Securities) และสามารถถ่ายทอดความรู้นั้น ๆ ให้แก่ผู้ใช้งานระบบได้อย่างมีประสิทธิภาพ

๗.๒.๒ การจัดจ้างหน่วยงานภายนอกที่มีความรู้ความชำนาญ และมีประสบการณ์ เพื่อจัดทำโครงการพัฒนาระบบข้อมูลดิจิทัล รวมถึงการบำรุงรักษาระบบงาน (Application Maintenance) ที่ใช้งานอยู่ เนื่องจากหน่วยงานภายนอกจะมีบุคลากรที่มีความชำนาญเป็นพิเศษเฉพาะทาง มีจำนวนเพียงพอ รวมถึงมีเครื่องมือและเทคโนโลยีที่ทันสมัย ทันต่อการพัฒนาระบบฐานข้อมูล มากกว่าบุคคลากรของสำนักงานฯ แต่การว่าจ้างหน่วยงานภายนอกนี้จะมีความเสี่ยงในเรื่องของความรู้ ความเข้าใจในระบบงานของสำนักงานฯ การคัดเลือก ผู้รับจ้างอาจต้องคัดเลือก โดยพิจารณาจากความรู้ความสามารถและประสบการณ์มากกว่าด้านราคา และให้ความสำคัญต่อผลสัมฤทธิ์ที่เกิดจากการทำงาน อีกทั้งความคุ้มค่าของการใช้จ่ายงบประมาณด้วย ดังนั้น หน่วยงานภายในสำนักงานฯ ที่เป็นเจ้าของงบประมาณต้องกำกับดูแล ควบคุมอย่าง

ต่อเนื่อง ตั้งแต่เริ่มกระบวนการจนถึงสิ้นสุดกระบวนการ โดยยึดหลักการบริหารกิจการบ้านเมืองที่ดี รักษาประโยชน์ของทางราชการให้มากที่สุด

๗.๒.๓ บุคลากรของสำนักงานฯ อาจจะยังขาดความรู้ความเข้าใจในเรื่องของระบบเทคโนโลยีดิจิทัลในเชิงลึก และมีจำนวนน้อย รวมถึงมีภารกิจอื่นๆ ที่ไม่สามารถให้เวลาได้เต็มเวลา โดยเฉพาะในเรื่องเชิงเทคนิคด้านการพัฒนาโปรแกรมและนวัตกรรมใหม่ๆ ทำให้เกิดช่องว่างในการที่จะประสานงานและรับผิดชอบงานอย่างมีประสิทธิภาพ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยง ในประเด็นนี้สามารถแก้ไขได้โดยการส่งเจ้าหน้าที่เข้ารับการอบรม และทดสอบความรู้ทางเทคโนโลยีดิจทัล (Certified) อย่างต่อเนื่องและเป็นระบบ เพื่อพัฒนาคุณภาพและประสิทธิภาพของบุคคลากร

๗.๒.๔ แผนการบริหารความเสี่ยงด้านบุคลากรนั้น จำเป็นต้องมีการฝึกอบรมเจ้าหน้าที่ในด้านที่เกี่ยวข้องกับระบบฐานข้อมูลดิจิทัล สำหรับบุคลากรใน ๒ ระดับ คือ ระดับผู้ดูแลระบบ (Administration Level) และผู้ใช้งานทั่วไป (User Level)

๗.๒.๔ แผนการบริหารความเสี่ยงด้านบุคลากร จำเป็นต้องมีการแผนการปฏิบัติงานจากภายนอกสถานที่ปฏิบัติราชการ หากเกิดกรณีฉุกเฉินที่ไม่สามารถมาปฏิบัติงาน ณ สถานที่ราชการประจำได้ เช่น กรณีเกิดประกาศภาวะฉุกเฉินห้ามออกนอกสถานที่ จากเหตุโรคระบาด หรือ ภัยพิบัต เช่น ควันพิษ สำหรับบุคลากรใน ๒ ระดับ คือ ระดับผู้ดูแลระบบ (Administration Level) และผู้ใช้งานทั่วไป (User Level)

๗.๒.๕ จัดอบรมและจัดทำคู่มือ หรือประชาสัมพันธ์ในการใช้งานระบบคอมพิวเตอร์และเครือข่ายที่ถูกต้อง รวมถึงข้อควรระวังในการรับส่งแฟ้มข้อมูลต่างๆ จากอุปกรณ์ที่เชื่อมโยงโดยตรงกับคอมพิวเตอร์ เช่น Flash Drive และ External Hard Disk หรือแฟ้มข้อมูลที่มีการส่งผ่านเครือข่าย เช่น การ Share File การรับส่งแฟ้มข้อมูลทาง e-Mail หรือ การ FTP เป็น ซึ่งจะช่วยลดความเสี่ยงจากการติดไวรัส Malware หรือ Trojan ด้วยความไม่รู้ของผู้ใช้

๗.๓ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีดิจิทัล (Hardware and Data Communication Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีทางไซเบอร์จากภายในสำนักงานฯ และมาจากภายนอกสำนักงานฯ โดยผ่านทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

การบริหารจัดการความเสี่ยงด้านอุปกรณ์เทคโนโลยิจิทัล

๗.๓.๑ ความเสี่ยงในด้านการจัดหาอุปกรณ์เทคโนโลยีดิจิทัลให้เหมาะสมกับลักษณะของงานและขององค์กร ซึ่งต้องมีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ รวมถึงการจัดหาและติดตั้งอุปกรณ์ต่างๆ ให้เหมาะสมตามลักษณะของงาน ตามงบประมาณที่ได้รับ รวมถึงการนำมาใช้งานร่วมกันได้อย่างมีประสิทธิภาพ

๗.๓.๒ ความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีดิจิทัล (Maintenance) ซึ่งโอกาสที่จะเกิดความเสี่ยง ๒ ด้าน คือ

๗.๓.๒.๑ ด้านการบำรุงรักษา เพื่อลดความเสี่ยงในการไม่สามารถใช้งานระบบคอมพิวเตอร์ได้เนื่องจากเครื่องเสีย

๑) เพื่อให้สามารถแก้ไขปัญหาเบื้องต้นของเครื่องคอมพิวเตอร์ได้โดย Administrator หรือ User รวมถึงการดูแลอย่างถูกต้องและต่อเนื่อง

๒) การสำรองข้อมูลดิจิทัล (Backup) เป็นประจำอย่างสม่ำเสมอและเก็บไว้ภายในอาคารและต่างอาคารเป็นอย่างน้อย และมีตารางการสำรองข้อมูลอย่างสม่ำเสมอ เช่น ประจำวัน ประจำสัปดาห์ ประจำเดือน และประจำปี เป็นต้น ทั้งนี้ รวมถึงทำการทดสอบการนำกลับมาใช้ใหม่ (Restore) ด้วยตามความจำเป็นและความสำคัญของข้อมูล

๓) มีการตรวจสอบไวรัส จากผู้ผลิต หรือจากศูนย์กลางระบบป้องกันไวรัสของสำนักงานฯ และทำการอัพเดท Signature รวมถึง Version ให้ทันสมัยล่าสุด และมีการตรวจสอบไวรัสอย่างสม่ำเสมอทุกครั้งก่อนการใช้งานเครื่องคอมพิวเตอร์ หรือให้ระบบ Desktop Management ทำการตรวจสอบว่าแต่ละเครื่องที่เข้ามาใช้งานในเครือข่ายได้มีการอัพเดท Virus Signature ให้ทันสมัย ก่อนการอนุญาตให้เข้าใช้งานเครือข่ายหรือไม่ ซึ่งสำนักงานฯ อยู่ระหว่างการติดตั้งระบบ Desktop Management

๔) การติดตั้งระบบรักษาความปลอดภัยเครือข่าย เช่น Firewall, Intrusion Prevention System (IPS), Network Access Control (NAC) และ Radius เป็นต้น

เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าสู่ระบบเทคโนโลยีดิจิทัลของสำนักงานฯ ผ่านทางเครือข่ายอินเทอร์เน็ตได้

๕) มีการตรวจสอบและดูแลเครื่องคอมพิวเตอร์แม่ข่ายเป็นประจำอย่างสม่ำเสมอ เพื่ออุดช่องโหว่ด้านการรักษาความปลอดภัยของระบบปฏิบัติการ (Operating System) หรือระบบรักษาความปลอดภัยของเครื่องแม่ข่าย รวมถึงการติดตั้งระบบป้องกันไวรัสบนเครื่องแม่ข่ายทุกเครื่อง โดยเฉพาะเครื่องที่มีระบบปฏิบัติการ Windows Server

๖) ติดตั้งโปรแกรม เพื่อตรวจสอบให้แน่ใจว่าไม่มีอุปกรณ์ใดในเครือข่ายสำนักงานฯ ได้ส่ง Spam ออกไปยังเครือข่ายอินเทอร์เน็ต โดยเฉพาะจาก SMTP Mail Server ซึ่งมักจะเป็นแหล่งที่ Hacker ชอบใช้ในการส่ง Spam ปัจจุบันสำนักงานฯ ได้ทำการติดตั้ง Symantec Brightmail Gateway เพื่อป้องกันแล้ว แต่ต้องมีการกำหนดตาราง ในการตรวจสอบที่เข้มงวด

๗) ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนทำการ Upload ข้อมูลขึ้น Web Server หรือ FTP Server เช่น Symantec Web Gateway, Symantec Endpoint Protection ที่สำนักงานฯ มีใช้อยู่ ซึ่งจะช่วยลดความเสี่ยงจากการถูก Black List โดย Search Engine หรือ Spamhaus (http://www.spamhaus.org) เป็นต้น

๘) มีการฝึกอบรมผู้ดูแลระบบ (Administrator) และผู้ใช้งานระบบ (User) ให้มีความรู้ความเข้าใจในการบริหารระบบ การใช้งานระบบงาน การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง และ การรักษาความปลอดภัยในการใช้ระบบสารสนเทศและการสื่อสาร เช่น การกำหนดรหัสผู้ใช้ (Username) และการใช้รหัสผ่าน (Password) รวมถึงการทำ User Authorization ผ่านอุปกรณ์ควบคุมการใช้งานเครือข่าย Network Access Control (NAC) และ Radius รวมถึงการควบคุมการเข้าใช้งานระดับ Certificate Authority (CA) ตามความจำเป็นของระบบการรักษาความปลอดภัยที่ตั้งไว้

๙) การจัดทำคู่มือผู้ดูแลอุปกรณ์เทคโนโลยีดิจิทัล

๑๐) การกำหนดให้ทำการ Logout ออกจากเครือข่าย หรือระบบงาน รวมถึงการปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว ซึ่งอาจทำโดยเจ้าของเครื่องหรือระบบ Network Access Control (NAC) และ Desktop Management ภายในเครือข่าย

๑๑) ตรวจสอบ Availability ของเครื่องคอมพิวเตอร์แม่ข่ายด้วยโปรแกรมตรวจสอบ เช่น Montastic จาก http://www.montastic.com เป็นต้น

๑๒) การจัดให้มีเส้นทางออกสู่เครือข่ายอินเทอร์เน็ต (Gateway) มากกว่า ๑ ทาง

๗.๓.๒.๒ ด้านการรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่าย (Server) ประกอบด้วย

๑) กำหนดขั้นตอนและวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์ และระบบเครือข่าย

๒) ทดสอบระบบปฏิบัติการ (Operating System) เกี่ยวกับการรักษาความปลอดภัย การแก้ไขช่องโหว่ด้วยการ Patch และการตรวจสอบและประเมินประสิทธิภาพการใช้งานอย่างสม่ำเสมอ

๓) ติดตั้งโปรแกรมระบบรักษาความปลอดภัย และระบบป้องกันไวรัส และมีการอัพเดทระบบควบคุมและป้องกันไวรัสจากส่วนกลางอย่างสม่ำเสมอ

๔) มีการวาง Web Server ไว้มากกว่า ๑ ที่ เช่น ที่อาคารสุขประพฤติ และ ที่ผู้ให้บริการเครือข่ายอินเทอร์เน็ต (ISP)

๕) การจัดตั้งศูนย์สำรอง (Backup Site)

๖) การปรับปรุงเครือข่ายหลักภายใน (Backbone Networks) อุปกรณ์ป้องกันการโจมตีเช่น Firewall, IPS/IDS, NAC, Router และ Switch ต่างๆ ใหม่ให้เป็นแบบ Redundancy

๗) การจัดหา Bandwidth Management เพื่อควบคุมการใช้งานเครือข่ายให้มีประสิทธิภาพ เพื่อให้การใช้งานระบบงานของสำนักงานฯ ได้รับ Bandwidth สูงกว่าการใช้งานด้านอื่นๆ

๗.๔ ความเสี่ยงด้านระบบดิจิทัล (Digital System)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของระบบต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งสำนักงานฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

การบริหารจัดการความเสี่ยงด้านระบบดิจิทัล สามารถดำเนินการได้โดยการพัฒนามาตรฐานการใช้งานและการบริการสำหรับระบบดิจิทัล ดังนี้

๗.๔.๑ พัฒนาและปรับปรุงมาตรฐานฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และเครือข่ายให้เป็นฐานข้อมูลกลางของระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา และเป็นไปในทิศทางเดียวกัน

๗.๔.๒ สร้างกลไกการจัดการฐานข้อมูล การจัดระบบสารสนเทศและการสื่อสาร เพื่อการบริหารจัดการของหน่วยงานให้ครอบคลุม ถูกต้อง และทันสมัยมากยิ่งขึ้น

๗.๔.๓ พัฒนาโปรแกรมให้สามารถบริหารจัดการฐานข้อมูลของสำนักงานเลขาธิการวุฒิสภา ให้มีมาตรฐาน และแบ่งสรรการใช้ทรัพยากรฐานข้อมูลจากโปรแกรมร่วมกันได้ ไม่ควรแยกกันทำเพราะจะทำให้ระบบงานที่เกิดขึ้นไม่เป็นในแนวทางเดียวกัน คนละมาตรฐาน ควบคุมได้ยาก และจะทำให้ การทำงานร่วมกัน รวมถึงค่าใช้จ่ายในการบริหารจัดการดูแลระบบจะประสบปัญหาตามมาในอนาคต

๗.๔.๔ พัฒนาโปรแกรมให้สามารถจัดเก็บ รวบรวม ประมวลผลข้อมูล ศึกษา วิเคราะห์เพื่อการนำเสนอและสนับสนุนการบริหารราชการ และพัฒนา ส่งเสริม บำรุงรักษาระบบ และการเผยแพร่ข้อมูลข่าวสารของสำนักงานฯ ได้ในลักษณะของ Web Services เพื่อความสะดวกในการใช้งานและเชื่อมโยงกับฐานข้อมูลอื่นๆ ได้ง่าย

๗.๔.๕ ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำขององค์กรด้านความปลอดภัยในการพัฒนาระบบงาน เช่น OWASP- Top ๑๐ Web Application Security Risks

๗.๔.๖ มีการกำหนดมาตรฐานในการพัฒนา โดยผู้รับจ้างภายนอกให้อยู่ภายใต้ข้อกำหนด เพื่อลดความเสี่ยงอย่างน้อย ดังนี้

๑) การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) level ๒

๒) การออกแบบโดยการอ้างอิงด้วยแผนผังแสดงความสัมพันธ์ระหว่างกลุ่มข้อมูล (Entity) – ER Diagram

๓) การส่งมอบ Source Code ในรูปแบบอุปกรณ์บันทึกอื่น ที่ไม่มีการเข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้

๔) หากมีการพัฒนา Library ด้วยตนเอง ผู้พัฒนาจะต้องส่ง Source Code Library ที่สามารถแก้ไขได้

๕) มีการถ่ายทอดความรู้ เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่ของสำนักงานเลขาธิการวุฒิสภา ทั้งระดับผู้ดูแลระบบและผู้ใช้งาน

๖) มีแผนงานการบำรุงรักษาระบบงานที่รวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัพเดทเมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูลเกิดความเสียหาย เป็นต้น

๗) มีรายงานการบำรุงรักษาทุกด้านตามที่ผู้รับจ้างภายนอกได้ดำเนินการไป

๗.๔.๗ จัดหาลิขสิทธิ์ซอฟต์แวร์ให้ถูกต้องตามจำนวนความต้องการใช้งานจริงๆ โดยทำสัญญา หรือข้อตกลงกับบริษัทเจ้าของลิขสิทธิ์ หรือใช้ซอฟต์แวร์ประเภท Open Source หรืออาจใช้ซอฟต์แวร์ที่ให้บริการการใช้งานโดยไม่เสียค่าใช้จ่าย Software as a Services (SaaS)

ตัวอย่างเช่น ใช้งานโปรแกรมจัดการเอกสารจากเว็บไซต์ www.docs.com แทนโปรแกรม Microsoft Office ที่มีลิขสิทธิ์ เป็นต้น

๗.๕ ความเสี่ยงด้านระบบฐานข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการ ความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร สมาชิกวุฒิสภา กรรมาธิการ ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

การบริหารจัดการความเสี่ยงด้านระบบฐานข้อมูล มีแนวทางดำเนินการ ดังนี้

๗.๕.๑ ฐานข้อมูลของสำนักงานฯ มีความเสี่ยงในด้านความพร้อมใช้งานด้านข้อมูลสารสนเทศและขาดข้อมูลวิชาการเชิงลึกในด้านต่างๆ เพื่อสนับสนุนงานด้านนิติบัญญัติ ซึ่งสำนักงานฯ โดยสำนักเทคโนโลยีสารสนเทศและการสื่อสาร ได้มีการพัฒนาการเชื่อมโยงของข้อมูลนิติบัญญัติในระบบเทคโนโลยีสารสนเทศ เพื่อสนับสนุนการดำเนินงานตามบทบาทใหม่ ซึ่งในงบประมาณปี พ.ศ.๒๕๖๒-๒๕๖๕ สำนักเทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินตามแผนขับเคลื่อนแผนพัฒนา Digital Parliament ของสำนักงานเลขาธิการวุฒิสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ – ๒๕๖๕) เพื่อเตรียมความพร้อมใช้งานด้านข้อมูลดิจิทัล

๗.๕.๒ ฐานข้อมูลของสำนักงานฯ มีความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) และการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลง โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่สำนักงานฯ ไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอ (Access Risk) โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ส่งผลให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์อาจถูกแก้ไขเปลี่ยนแปลงได้ ควรมีการควบคุมการใช้งานร่วมกันระหว่างการเชื่อมต่อเข้าใช้งานเครือข่ายด้วย Network Access Control (NAC) และ Radius

ส่วนการใช้ระบบงานสามารถควบคุม โดยการใช้งานร่วมกันระหว่างระบบบริหาร การใช้งานฐานข้อมูล (Relational Database Management Security) กับระบบ Directory เช่น Active Directory หรือ Lightweight Directory Access Protocol (LDAP) เป็นต้น และการใช้งานระบบต่างๆ ด้วยระบบการบริหารการใช้งานด้วยระบบ Single Sign On (SSO) เพื่อที่จะไม่ต้อง Login หลายๆ ครั้งในการพิสูจน์สิทธิ์ (Authenticate) เพื่อใช้งานระบบใดระบบหนึ่ง สำหรับฐานข้อมูลที่มีความสำคัญควรติดตั้งผ่านทาง Firewall และ Intrusion Prevention System/ Intrusion Detection System (IPS/ IDS) เพื่อปกป้องฐานข้อมูลโดยเฉพาะ และเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประเมินผล และการแสดงผลมีความถูกต้องครบถ้วน

๗.๕.๓ ฐานข้อมูลของสำนักงานฯ มีความเสี่ยงกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการที่ไม่ได้ทำการสำรองข้อมูลและระบบงานคอมพิวเตอร์อย่างสม่ำเสมอ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉินดังกล่าว

๗.๕.๔ ฐานข้อมูลของสำนักงานฯ มีความเสี่ยงเกี่ยวกับการที่ไม่ได้จัดให้มีระบบคอมพิวเตอร์ที่ทันสมัย มีการอัพเดทอย่างสม่ำเสมอ เพื่ออุดช่องโหว่อันเกิดจากระบบปฏิบัติการ (Operating System) ระบบจัดการฐานข้อมูล (Database Management) หรือแม้กระทั่งระบบงาน (Application Software) และบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการทำงาน หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานสำคัญทุกด้าน และการจัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอ เพื่อให้มีความรู้ และเชี่ยวชาญในงานที่รับผิดชอบสำหรับการควบคุมการปฏิบัติงาน

๗.๕.๕ ฐานข้อมูลของสำนักงานสำนักงานฯ มีความเสี่ยงเกี่ยวกับการเก็บสำรองระบบงาน และฐานข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) โดยวัตถุประสงค์ของการสำรองข้อมูลที่สำคัญ คือ เพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการบริหารจัดการสำรองข้อมูล และ การกู้คืนข้อมูล ดังนั้น การสำรองข้อมูลและการเตรียมข้อมูลให้พร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan) ของสำนักงานฯ จึงมีวัตถุประสงค์ เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับ การใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและในเวลาที่ต้องการ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ การเก็บรักษา การทดสอบ รวมทั้งการจัดทำและการทดสอบแผนฉุกเฉิน

การสำรองข้อมูลให้มีความพร้อมใช้งานได้ตลอดเวลาและต่อเนื่อง เพื่อป้องกันการสูญหายที่อาจจะเกิดขึ้นได้ ควรมีการสำรองข้อมูลเป็นประจำเป็นรายวันรายสัปดาห์ รายเดือน และรายปี โดยดำเนินการอย่างน้อย ดังนี้

๑) กำหนดสถานที่ในการเก็บรักษาข้อมูลสำรองโดยเฉพาะ

๒) การสำรองข้อมูลโดยการบันทึกไว้ที่ระบบสำรองข้อมูลด้วยเทปแม่เหล็ก

๓) กำหนดการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้ตรวจสอบได้ว่าข้อมูลรวมทั้งโปรแกรมต่างๆ ที่ได้สำรองไว้มีความถูกต้อง ครบถ้วน และใช้งานได้

๔) การกู้ข้อมูลสู่ระบบ มีการกำหนดบุคลากรผู้ที่ได้รับสิทธิ์กู้คืนข้อมูลที่ได้ทำการสำรองไว้

๕) มีระบบการวางแผนจัดศูนย์สำรอง (Backup Site)

๗.๕.๖ มีการบริหารจัดการอุปกรณ์เก็บข้อมูลอื่น ๆ หรือ Cloud Computing เพื่อให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว (หากทำได้) เพื่อลดความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้

๗.๖ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหารองค์กรเนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

การบริหารจัดการความเสี่ยงด้านกลยุทธ์ ดำเนินการโดยการสื่อสารนโยบายและผลักดันให้มีการนำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร และแนวนโยบาย/แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา มาใช้ในหน่วยงานทุกระดับอย่างทั่วถึงและมีการแปลงแผนไปสู่การปฏิบัติอย่างจริงจัง

๗.๗ ความเสี่ยงด้านการเงิน (Financial Risk)

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

การบริหารจัดการความเสี่ยงด้านการเงิน ดำเนินการดังนี้

๗.๗.๑ มีการจัดทำแผนบริหารจัดการการใช้จ่ายงบประมาณที่ได้รับให้ทันการจ่ายเงินงวดในปีนั้นๆ

๗.๗.๒ จัดลำดับความสำคัญของโครงการ รวมถึงระยะเวลาในการจัดหาพัสดุสำหรับโครงการสั้นๆ ให้ทันต่อความต้องการใช้งาน

๗.๗.๓ มีการติดตามงบประมาณรายจ่ายอย่างต่อเนื่อง

๗.๗.๔ มีแผนรองรับกรณีงบประมาณถูกตัด

๗.๘ ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)

หมายถึง ความเสี่ยง เนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

การบริหารจัดการความเสี่ยงด้านการบริหาร ดำเนินการโดย

๗.๘.๑ มีการจัดทำตามแผนขับเคลื่อนแผนพัฒนา Digital Parliament ของสำนักงานเลขาธิการวุฒิสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ – ๒๕๖๕)

๗.๘.๒ มีการแต่งตั้งคณะกรรมการกำหนดแนวนโยบายและแผนที่เกี่ยวข้องกับด้านเทคโนโลยีดิจิทัล มีคณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา ระยะ ๔ ปี (พ.ศ. ๒๕๖๒ –๒๕๖๕) เพื่อสนับสนุนการจัดทำแผนการบริหารจัดการงานให้บริการด้านเทคโนโลยีดิจิทัล ด้านระบบสารสนเทศขององค์กรให้มีมาตรฐานด้านความปลอดภัยของข้อมูลและการบริหารจัดการงานให้บริการด้านระบบสารสนเทศที่มีประสิทธิภาพและประสิทธิผลชัดเจน เป็นไปตามมาตรฐานสากลที่หน่วยงานต่างๆ ทั้งในประเทศและต่างประเทศให้การยอมรับ เช่น มาตรฐานด้าน Service Support และ Service Delivery ตลอดจนการกำหนด SLA (Service Level Agreement) เป็นต้น ซึ่งการบริหารความเสี่ยงที่เกี่ยวข้องกับการควบคุมภายในระดับองค์กร ตามมาตรฐานของ COSO V.๒ ซึ่งมีความสัมพันธ์ กับ COBIT ภายใต้ IT Governance หรือกระบวนการบริหารและการควบคุมสารสนเทศที่ดี และระบบมาตรฐานด้าน ความปลอดภัยของข้อมูล ISO/IEC ๒๗๐๐๑:๒๐๐๕ (Information Security Management System: ISMS)

๗.๘.๓ การบริหารจัดการ ติดตาม ควบคุม กำกับดูแล และให้คำปรึกษา แก้ไขปัญหาระบบต่างๆ

๗.๘.๔ การจัดการประเมินผลแผนขับเคลื่อนแผนพัฒนา Digital Parliament ของสำนักงานเลขาธิการวุฒิสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ – ๒๕๖๕)

๗.๘.๕ การติดตาม ควบคุม กำกับ ดูแล และให้คำปรึกษา แก้ไขปัญหาระบบงานต่างๆ ของสำนักงานฯ ให้สามารถใช้งานได้อย่างมีประสิทธิภาพสูงสุด

๗.๘.๖ การศึกษา วิเคราะห์ข้อมูลที่เกี่ยวข้อง เพื่อการวางแผนและคาดการณ์แนวโน้ม ความต้องการบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๗.๘.๗ การให้บริการฝึกอบรม เพื่อพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสารแก่บุคลากรของสำนักงานฯ

๘. แผนบริหารและประเมินความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล

ตามที่สำนักงานเลขาธิการวุฒิสภาได้มีการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๕๕ – ๒๕๕๙ และแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษา และป้องกันแก้ไขปัญหาอันอาจส่งผลกระทบต่อฐานข้อมูลและระบบสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งระบบเครือข่ายของสำนักงานเลขาธิการวุฒิสภา และได้จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานเลขาธิการวุฒิสภา ปี ๒๕๖๐ – ๒๕๖๒ ซึ่งคณะกรรมการกำหนดแนวนโยบายและแผนที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลได้นำมาศึกษาและระดมความคิดเห็นจากผู้รับผิดชอบในด้านที่เกี่ยวข้อง เพื่อนำมาจัดทำแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล พ.ศ. ๒๕๖๒ - ๒๕๖๕ เพื่อให้กระบวนงานด้านระบบเทคโนโลยีดิจิทัลดำเนินการรองรับภารกิจของหน่วยงานได้ ให้สอดคล้องกับแผนขับเคลื่อนแผนพัฒนา Digital Parliament ของสำนักงานเลขาธิการวุฒิสภา ระยะ ๕ ปี (พ.ศ. ๒๕๖๑ – ๒๕๖๕) โดยได้มีการนำเสนอและรับฟังความคิดเห็นต่อแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล พ.ศ. ๒๕๖๒ - ๒๕๖๕ ให้กับบุคลากรสำนักเทคโนโลยีสารสนเทศและการสื่อสาร และมีการสัมภาษณ์ สอบถามจากเจ้าหน้าที่ผู้เกี่ยวข้อง

จากแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา ส่วนที่ ๖ เรื่อง แนวปฏิบัติการประเมินความเสี่ยง พ.ศ. ๒๕๕๒ ได้กำหนดมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสาร รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ทำให้สามารถระบุความเสี่ยง และควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ ดังนี้

๑) ความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการประเมินความเสี่ยงนั้น ดังนี้

๑.๑) ความเสี่ยงที่เกิดจากการลอบเข้าระบบปฏิบัติการ เพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต

๑.๒) ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๑.๓) ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๑.๔) ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) ระบบสารสนเทศและการสื่อสารที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

๑.๕) ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๒) กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๓) การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

๓.๑) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

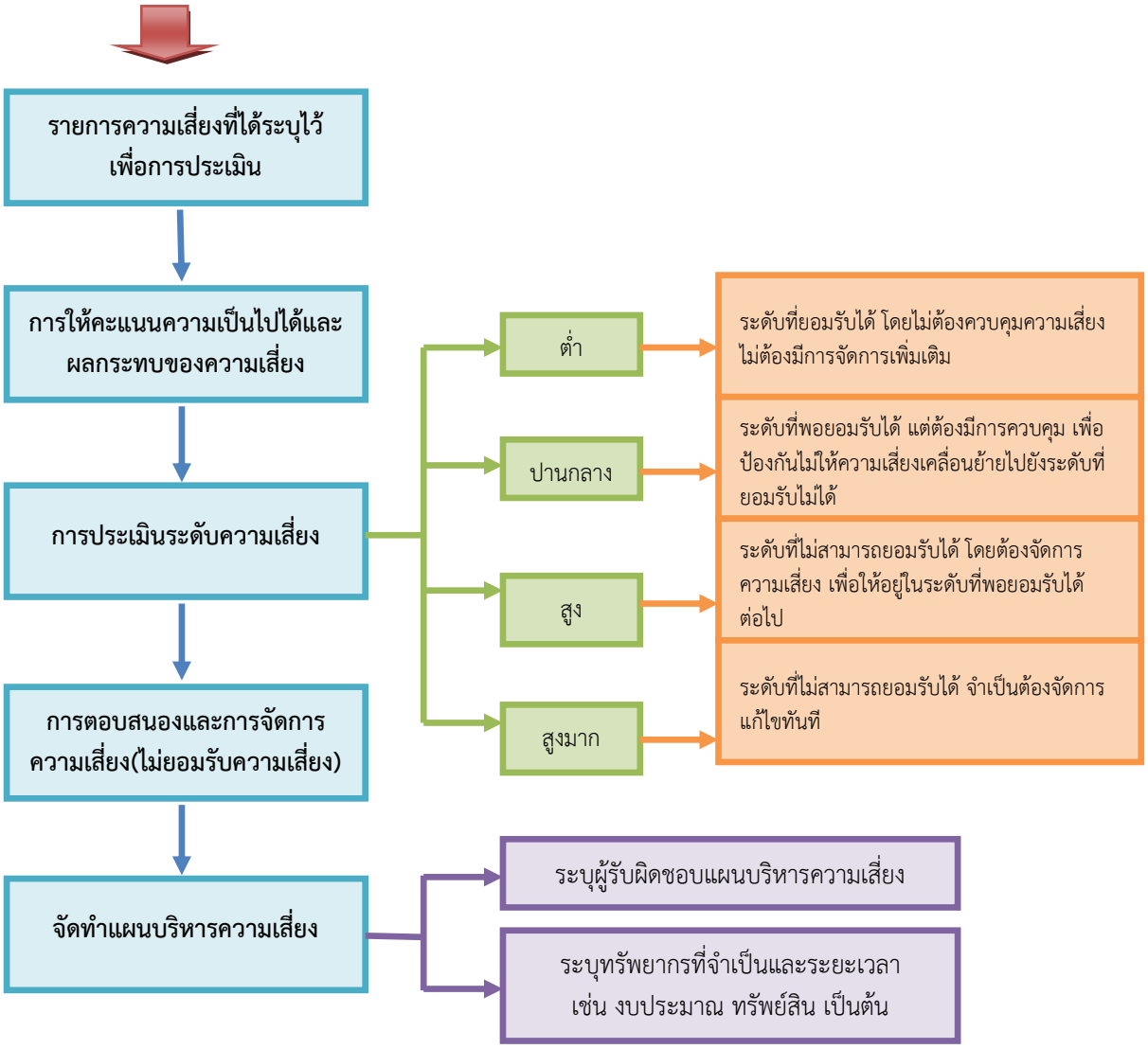
๓.๒) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๓.๓) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๔) ผลการประเมินภาพรวมของความเสี่ยงที่ระบุ ต้องจัดทำเป็นคะแนนโดยมีคะแนนเต็ม ๑๐๐ คะแนน และกำหนดให้มีเกณฑ์ในการพิจารณาว่า ความเสี่ยงที่ระบุนั้นต้องมีการบริหารจัดการลด ความเสี่ยงนั้นหรือไม่ โดยให้เกณฑ์เป็น ๘๐ คะแนนขึ้นไป

๕) ขั้นตอนการประเมินความเสี่ยง มีขั้นตอนตามแผนผัง ดังนี้

ขั้นตอนการประเมินความเสี่ยง



รูปที่ ๑ ขั้นตอนการประเมินความเสี่ยง

ตารางที่ ๑

แผนผังประเมินความเสี่ยงตามแนวทางของ COSO

(Committee of Sponsoring Organization)

ระดับโอกาส (ความเป็นไปได้)

Risk Assessment Matrix			ต่ำมาก/น้อยมาก	ต่ำ/น้อย	ปานกลาง	สูง/บ่อย	สูงมาก/บ่อยมาก
			๑	๒	๓	๔	๕
ผลกระทบ (ความรุนแรง)	สูงมาก/หายนะ	๕	๕	๑๐	๑๕	๒๐	๒๕
	สูง/วิกฤต	๔	๔	๘	๑๒	๑๖	๒๐
	ปานกลาง	๓	๓	๖	๙	๑๒	๑๕
	ต่ำ/น้อย	๒	๒	๔	๖	๘	๑๐
	ไม่เป็นสาระสำคัญ/น้อยมาก	๑	๑	๒	๓	๔	๕

ระดับของความเสี่ยง

ตารางที่ ๒ เกณฑ์การยอมรับความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	แทนด้วยแถบสี	ความหมาย
ต่ำ	๑ - ๓	**เขียว**	ระดับที่ยอมรับได้โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม (Acceptable or Limited Focus)
ปานกลาง	๔ - ๙	**เหลือง**	ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ (Tolerable but caution or Management Discretion/ Medium Risk)
สูง	๑๐ - ๑๖	**ส้ม**	ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป (Intolerable or Attention required/ High Risk)
สูงมาก	๑๗ - ๒๕	**แดง**	ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ทันที (Intolerable or Immediate attention require/ High Risk)

ตารางที่ ๓ ระดับโอกาส (ความเป็นไปได้)

ระดับโอกาส (ความเป็นไปได้)	คำนิยาม
๑	นานๆครั้ง (แทบไม่เกิดขึ้นเลย)
๒	ไม่บ่อย (อาจเกิดขึ้นได้ทุก ๕ ปี)
๓	ปานกลาง (อาจเกิดขึ้นได้ทุกปี)
๔	บ่อย (อาจเกิดขึ้นได้ทุกเดือน)
๕	บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)

ตารางที่ ๔ ผลกระทบ (ความรุนแรง)

ผลกระทบ (ความรุนแรง)	คำนิยาม
๑	กระทบต่อความน่าเชื่อถือขององค์กร/ ความพึงพอใจของผู้ใช้บริการน้อยมาก (แทบไม่มีผลกระทบเลย)
๒	กระทบต่อความน่าเชื่อถือขององค์กร/ ความพึงพอใจของผู้ใช้บริการน้อย (เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ)
๓	กระทบต่อความน่าเชื่อถือขององค์กร/ ความพึงพอใจของผู้ใช้บริการปานกลาง (เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย)
๔	กระทบต่อความน่าเชื่อถือขององค์กร/ ความพึงพอใจของผู้ใช้บริการมาก (ผู้บริหารถูกตำหนิหรือถูกร้องเรียน)
๕	กระทบต่อความน่าเชื่อถือขององค์กร/ ความพึงพอใจของผู้ใช้บริการมากที่สุด (ผู้บริหารถูกลงโทษทางวินัย)

ได้กำหนดความเสี่ยง ปัจจัยเสี่ยง ผลกระทบ ระดับความเสี่ยง มาตรการและแผนปฏิบัติการ ระยะเวลาที่ต้องดำเนินการ และผู้รับผิดชอบไว้ตามรายละเอียดในตารางที่ ๕ ดังนี้

จากการระดมความคิดเห็นจากทุกฝ่ายที่เกี่ยวข้องในการบริหารและประเมินความเสี่ยงของสำนักงานฯ ทำให้ได้ข้อมูลเพื่อนำมาประเมินความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล และจัดทำเป็นตารางประเมินความเสี่ยงของสำนักงานฯ ได้ ดังนี้

ตารางที่ ๕ ผลการประเมินความเสี่ยงของสำนักงานฯ ตามแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล พ.ศ. ๒๕๖๒ – ๒๕๖๕

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
<u>ความเสี่ยงสูงมาก</u>									
ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	๑. เสี่ยงต่อการสูญหายของข้อมูล ๒. เสี่ยงต่อการถูกฟ้องร้องและเสื่อมเสียชื่อเสียงและความน่าเชื่อถือของสำนักงานฯ	๑. การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้นๆ ๒. สำนักงานฯ อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ ๓. ความไม่สะดวกหากไปใช้งานด้วยซอฟต์แวร์ ที่ไม่จำเป็นต้องมีลิขสิทธิ์ (Open Source)	สูงมาก ๕x๕=๒๕	๑. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น ๓. การรณรงค์ขอความร่วมมือเจ้าหน้าที่ในการใช้งานซอฟต์แวร์ที่ถูกกฎหมาย ๒. การทำสัญญา หรือข้อตกลง/สนับสนุนการใช้โปรแกรมที่มีลิขสิทธิ์อย่างถูกต้อง	/ /	/ /	/ / /	๔	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
<u>ความเสี่ยงสูง</u>									
๑. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	๑. ไม่สามารถใช้งานระบบงานของสำนักงานฯ ผ่านเครือข่ายอินทราเน็ต ได้ ๒. ไม่สามารถเชื่อมต่อภายนอกสำนักงานฯผ่านเครือข่ายอินเทอร์เน็ตได้	๑. ขัดขวางการทำงานของเจ้าหน้าที่และผู้บริหารงานสำนักงานฯ ๒. บุคคลภายนอกไม่สามารถเข้าใช้ Web Server หรือค้นหาข้อมูลที่ต้องการได้	สูง ๕x๓=๑๕	๑. ตรวจสอบ Availability ของ Server ด้วยโปรแกรมตรวจสอบ เช่น Montastic จาก http://www.montastic.com เป็นต้น	/	/	/	๓	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
				๒. การจัดทำเส้นทางออกสู่เครือข่ายอินเทอร์เน็ต (Gateway) มากกว่า ๑ ทาง หากสำนักงานฯ มีงบประมาณเพียงพออาจพิจารณาในการจัดทำ Gateway ที่ผู้ให้บริการเครือข่ายอินเทอร์เน็ต (ISP) ต่างออกไป จะทำให้ระบบเครือข่ายอินเทอร์เน็ต มีเสถียรภาพมากขึ้น	/	/	/		
				๓. การวาง Web Server ไว้มากกว่า ๑ ที่ เช่น ที่อาคารสุขประพฤติ หรือที่ ISP	/	/	/		
				๔. การจัดตั้งศูนย์สำรอง (DR Site)	/	/	/		
				๕. การปรับปรุงเครือข่ายหลัก					

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
				ภายใน (Backbone Networks) อุปกรณ์ป้องกันการโจมตีเช่น Firewall, IPS/ IDS, NAC, Router และ Switch ต่างๆ ใหม่ให้เป็นแบบ Redundancy	/	/	/		
				๖. การจัดหา Bandwidth Management เพื่อควบคุมการใช้งานเครือข่ายให้มีประสิทธิภาพ เพื่อให้การใช้งานระบบงานของสำนักงานฯ ได้รับ Bandwidth สูงกว่าการใช้งานด้านอื่นๆ	/	/	/		
๒. ความเสี่ยงจากการการติดไวรัสคอมพิวเตอร์หรือ Malware	๑. เสี่ยงต่อการถูกทำลาย โปรแกรมหรือข้อมูล ๒. เสี่ยงต่อการไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ	๑. ใช้คอมพิวเตอร์ไม่ได้ ๒. ใช้ระบบงานไม่ได้ ๓. ข้อมูลที่สำคัญสูญหาย	สูง ๕x๓=๑๕	๑. ใช้ระบบป้องกันไวรัสกับเครื่องแม่ข่ายที่ต้องเสียค่าใช้จ่าย Protection ที่สำนักงานฯ ใช้อยู่ที่สามารถควบคุมการโจมตีและการบุกรุกเครือข่ายจากสาเหตุต่างๆ เช่น การระบาดของ Virus และ Worm, การโจมตีเพื่อห้ามการบริการ (Denial of Server-DoS) การบุกรุกแบบ Vulnerability Exploit,	/	/	/	๓	ทุกสำนัก

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
	๓. เสี่ยงต่อการถูกขโมยข้อมูลที่สำคัญ			Network Reconnaissance และเทคนิคการหลบซ่อนการโจมตีแบบ Traffic Normalization, IP Defragmentation, TCP Reassemble ได้ ๒. อัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ ๓. มีการสำรองข้อมูลที่เครื่องลูกข่ายที่จำเป็นไว้อย่างสม่ำเสมอ	/ /	/ /	/ /		
๓. ความเสี่ยงจากช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๑. เสี่ยงต่อการถูกขโมยข้อมูล ๒. เสี่ยงต่อการทำความเสียหายแก่โปรแกรม ๓. เสี่ยงต่อการใช้ช่องโหว่ของโปรแกรม หรือการซ่อน Script ไว้ในโปรแกรมเพื่อวัตถุประสงค์แอบแฝง	๑. ลดความน่าเชื่อถือต่อสำนักงานฯ หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ ๒. กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อสำนักงานฯ เป็นอย่างยิ่ง	สูง ๕x๓=๑๕	๑. ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top ๑๐ Web Application Security Risks เพื่อลดความเสี่ยง ๒. มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ	/ /	/ /	/ /	๔	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร หรือสำนักอื่นๆที่พัฒนาระบบงานขึ้นใช้เอง

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
๔. ความเสี่ยงจากการถูก Black List โดย Search Engine หรือ Spamhaus (http://www.spamhaus.org)	๑. ผู้ใช้งานที่ต้องการข้อมูลของสำนักงานฯ หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน Web Server ได้ ๒. ไม่สามารถใช้งานเครือข่ายหรือ e-mail ได้	๑. ลดความน่าเชื่อถือต่อสำนักงานฯ หรือข้อมูลของสำนักงานฯ ๒. สำนักงานฯ อาจถูกฟ้องร้อง โดยผู้มีส่วนได้ส่วนเสีย	สูง ๕x๓=๑๕	๑. ติดตั้งโปรแกรม เพื่อตรวจสอบให้แน่ใจว่าไม่มีอุปกรณ์ใดในเครือข่ายสำนักงานฯ ได้ส่ง Spam ออกไปยังเครือข่ายอินเทอร์เน็ตโดยเฉพาะจาก SMTP Mail Server ซึ่งมักจะเป็นแหล่งที่ Hacker ชอบใช้ในการส่ง Spam ปัจจุบันสำนักงานฯ ได้ทำการติดตั้ง Symantec Brightmail Gateway เพื่อป้องกันแล้ว แต่ต้องมีตารางในการตรวจสอบที่เข้มงวด	/	/	/	๒ และ ๓	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
				๒. ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนการอัพโหลดข้อมูลขึ้น Web Server หรือ FTP Server เช่น Symantec Web Gateway Symantec Endpoint Protection ที่สำนักงานฯ มีใช้อยู่เป็นต้น	/	/	/		
				๓. มีการอัพเดทตัวโปรแกรมและ Signature อย่างสม่ำเสมอ และการทำการบำรุงรักษา	/	/	/		

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
				(Maintenance) ทั้งฮาร์ดแวร์และซอฟต์แวร์ พร้อมทั้ง Update Licenses					
๕. ความเสี่ยงจากการใช้โปรแกรมที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	๑. เสี่ยงต่อการถูกขโมยข้อมูล ๒. เสี่ยงต่อการทำความเสียหายแก่โปรแกรม ๓. ไม่สามารถแก้ไขข้อบกพร่องได้เอง ๔. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว ๕. เสียค่าใช้จ่ายสูง	๑. ลดความน่าเชื่อถือต่อสำนักงานฯ หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ ๒. กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อสำนักงานฯ เป็นอย่างยิ่ง ๓. จัดหางบประมาณ เพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลพร้อมกับการทำการบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องที่ต้องมีการอัพเดทอยู่เสมอ	สูง ๓x๔=๑๒	๑. การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level ๒ ๒. การออกแบบโดยการอ้างอิงด้วย แผนผังแสดงความสัมพันธ์ระหว่างกลุ่มข้อมูล (Entity) – ER Diagram ๓. ให้มีการส่งมอบ Source Code ในรูปแบบ DVD ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้ ๔. หากมีการพัฒนา Library ด้วยตนเอง ต้องส่ง Source Code Library ที่สามารถแก้ไขได้ ๕. มีการถ่ายทอดความรู้เทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่	/ / / / /	/ / / / /	/ / / / /	๔	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร หรือสำนักอื่นๆ ที่พัฒนาระบบงานขึ้นใช้เอง

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
				๖. มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม	/	/	/		
				๗. มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึง การแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัพเดท เมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น	/	/	/		
๖. ความเสี่ยงจากการเกิดอัคคีภัย	๑. การถูกทำลายทรัพย์สิน ระบบคอมพิวเตอร์และเครือข่าย ๒. การถูกทำลายข้อมูล	๑. เสียงบประมาณในการจัดหาระบบทดแทน ๒. การไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทน	สูง ๒x๕=๑๐	๑. ติดตั้งระบบตรวจจับควันที่สามารถตรวจจับควันได้ก่อนล่วงหน้า (Very Early Smoke Detection Apparatus- VESDA) ๒. ติดตั้งระบบแจ้งเตือนไฟไหม้	/ /	/ /	/ /	๑	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักบริหารงานกลาง

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
	๓. การบาดเจ็บหรือเสียชีวิตของเจ้าหน้าที่หรือลูกจ้างภายในอาคาร			๓. ติดตั้งระบบดับเพลิงแบบ Aerosol ซึ่งปัจจุบันสำนักงานฯ ได้มีการติดตั้งระบบนี้ใช้งานอยู่ในศูนย์สารสนเทศทั้ง ๓ ระบบข้างต้นแล้ว	/	/	/		
				๔. จัดตั้งศูนย์สำรองในกรณีที่เกิดอัคคีภัยขึ้น	/	/	/		
				๕. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	/	/	/		
๗. ความเสี่ยงจากข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk	๑. ข้อมูลที่อยู่ในชั้นความลับ รั่วไหลทำให้เสียหายต่อความน่าเชื่อถือของสำนักงานฯ ๒. ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	สูง ๒x๕=๑๐	มีการบริหารจัดการ ต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว หากทำได้	/	/	/	๕	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
<u>ความเสี่ยงปานกลาง</u>									
๑. ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	๑. ไม่สามารถใช้งานเครื่องแม่ข่ายและเครือข่ายได้ ๒. ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่าย ทั้งส่วนระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (RDBMS) อันเนื่องมาจากเครื่องไม่ได้ถูกทำการ Shutdown อย่างเหมาะสม	๑. ข้อมูลเสียหาย ๒. ระบบปฏิบัติการ โปรแกรม หรือ ฐานข้อมูลเสียหาย ต้องมีการติดตั้งใหม่ ๓. เสียเวลาการใช้งาน ๓ ถึง ๖ ชั่วโมงเป็นอย่างน้อย	ปานกลาง ๒x๔=๘	๑. ติดตั้งระบบ UPS ที่สามารถสำรองไฟฟ้าเพียงพอสำหรับเครื่องแม่ข่าย และระบบเครือข่าย และสามารถทำการ Shutdown เครื่องแม่ข่ายทั้งหมดกรณีไฟฟ้าดับเกินกว่าที่UPSจะสามารถจ่ายไฟได้ ๒. วางแผนจัดการยุบรวมเครื่องแม่ข่ายต่างๆ ที่กระจัดกระจายเป็นจำนวนมาก และมีหลายระบบปฏิบัติการให้เป็นในที่มีระบบสำรอง (Redundancy) โดยใช้เทคโนโลยี Virtualization มาบริหารจัดการ ๓. วางแผนการจัดหาและติดตั้งเครื่องกำเนิดไฟฟ้า (Electrical Generator) สำหรับศูนย์สารสนเทศอาคารรัฐสภาใหม่	/ / /	/ / /	/ / /	๑	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักบริหารงานกลาง

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
๒. ความเสี่ยงจากการเกิดอุทกภัย	ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์	เสียงบประมาณในการซ่อมแซมหรือจัดหาใหม่ทดแทน	ปานกลาง ๒x๓=๖	๑. ติดตั้งเครื่องตรวจจับระดับน้ำรั่วไหลพื้นที่ที่มีความไวต่อน้ำ (โครงการก่อสร้างรัฐสภาแห่งใหม่) ๒. มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ (โครงการก่อสร้างรัฐสภาแห่งใหม่)	/ /	/ /	/ /	๑	-สำนักเทคโนโลยีสารสนเทศและการสื่อสาร -สำนักบริหารงานกลาง
๓. ความเสี่ยงจากแมลง หรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์ หรือสายไฟฟ้า/สายสัญญาณ	เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน	ปานกลาง ๓x๒=๖	๑. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack ๒. ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	/ /	/ /	/ /	๑	-สำนักเทคโนโลยีสารสนเทศและการสื่อสาร -สำนักบริหารงานกลาง

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
๔. ความเสี่ยงจากการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย หรือเครื่องลูกข่ายและอุปกรณ์ต่อพ่วง ๔.๑ เครื่องแม่ข่าย	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญ	๑. เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง ๒. เสียเวลาในการกู้ระบบ ๓. เสียภาพลักษณ์ของสำนักงานฯ	ปานกลาง ๒x๓=๖	๑. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า-ออก ห้องคอมพิวเตอร์แม่ข่าย	/	/	/	๑	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
				๒. ตู้ Rack ที่ติดตั้งอุปกรณ์ เช่น เครื่องแม่ข่าย (Server) อุปกรณ์จัดเก็บข้อมูล (Disk Array) และอุปกรณ์เครือข่ายต้องมีการล็อคด้วยกุญแจตลอดเวลา	/	/	/		
				๓. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน การนำติดตัวไปด้วยตลอดเวลา หรือติดตั้งอุปกรณ์ล็อค	/	/	/		

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
				เช่น Kensington Lock เป็นต้น เพื่อป้องกันการสูญหาย					
๔.๒ เครื่องลูกข่ายและ อุปกรณ์ต่อพ่วง	เสี่ยงต่อการสูญหายของอุปกรณ์และข้อมูลที่มีความสำคัญ	๑. เสียงบประมาณในการจัดหาอุปกรณ์ทดแทน ๒. เสียภาพลักษณ์ของสำนักงานฯ	ปานกลาง ๒x๓=๖	๑. ควบคุมการเข้าออกอาคาร ๒. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์เข้า-ออกอาคารตลอดเวลา ๓. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ๆ มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	/ / /	/ / /	/ / /	๑	-สำนักบริหารงานกลาง
๕. ความเสี่ยงจากการไม่ทำการสำรองข้อมูล หรือทำการสำรองข้อมูลแต่ขาดการอัพเดท	๑. เสี่ยงต่อการสูญหายของข้อมูลในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานได้ตามปกติ ๒. เสี่ยงต่อการมีข้อมูลที่ไม่ถูกต้องกับความเป็นจริง	๑. เสียค่าใช้จ่ายในการกู้คืนข้อมูล หรือการจัดทำขึ้นมาใหม่ ๒. ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้งานได้เนื่องจากขาดความมั่นใจในข้อมูล	ปานกลาง ๒x๓=๖	๑. มีการบริหารจัดการในการทำการสำรองข้อมูล (Backup) เป็นประจำอย่างสม่ำเสมอ ๒. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore) เพื่อความแน่ใจในข้อมูลที่เก็บไว้ ปัจจุบัน การจัดเก็บสำรองข้อมูลของสำนักงานฯ ที่มีอุปกรณ์และระบบบริหารจัดการสำรองข้อมูลโดยอัตโนมัติ มีเฉพาะระบบเครื่อง	/ /	/ /	/ /	๕	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
				ในโครงการเพิ่มประสิทธิภาพการบริหารราชการของสำนักงานเลขาธิการวุฒิสภา ระยะที่ ๑ และโครงการจัดตั้งห้องสมุดอิเล็กทรอนิกส์ ๓. การจัดการเชื่อมโยงเครื่องแม่ข่ายอื่นเข้าสู่ระบบการสำรองข้อมูลโดยอัตโนมัติ	/	/	/		
๖. ความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์จากภายนอก	เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	๑. ทำให้ระบบเครื่องแม่ข่าย หรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย ๒. ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพบน Web Site ของสำนักงานฯ ๓. ถูกโจรกรรมข้อมูลที่เป็นความลับของสำนักงานฯ	ปานกลาง ๑x๕=๕	๑. ติดตั้งระบบป้องกัน และเตือนภัย Anti Spam, Antivirus, Malware, Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้นๆ อยู่เป็นประจำเพื่อที่จะสามารถแก้ไขได้ทันเมื่อถูกโจมตี ๒. หมั่นตรวจสอบ Policy และ Log ของ Firewall IPS/ IDS อย่างสม่ำเสมอ ๓. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตามลำดับเมื่อเกิด	/ / /	/ / /	/ / /	๓	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
				เหตุการณ์ขึ้นจริงจะได้พร้อมที่จะรับกับสถานการณ์ได้โดยไม่สับสน ๔. ติดตั้ง Firewall และ IDS/ IPS เพื่อป้องกันฐานข้อมูลที่มีความสำคัญโดยเฉพาะ	/	/	/		
๗. ความเสี่ยงจากการโจมตีทางไซเบอร์สำนักงานฯ ไม่ให้สามารถให้บริการได้ (Denial of Service-DoS) ๗.๑ จากภายนอก	เสี่ยงต่อการถูกโจมตีได้จากภายนอก โดยโจมตีทั้งเครื่องแม่ข่ายและ/หรือเครือข่าย ในทุกรูปแบบ ซึ่งจะมีการพัฒนาวิธีการอยู่ตลอดเวลา	ไม่สามารถใช้งานเครือข่ายได้ หรือใช้ได้แต่ช้ามาก	ปานกลาง ๑x๕=๕	๑. ติดตั้งระบบป้องกัน และเตือนภัย Spam, Virus, Malware, Trojan และมีเจ้าหน้าที่คอยดูแลตรวจสอบและอัพเดทฐานข้อมูลของอุปกรณ์นั้นๆ อยู่เป็นประจำ เพื่อลดหรือสามารถแก้ไขได้ทันเมื่อถูกโจมตี	/	/	/	๓	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
				๒. หมั่นตรวจสอบ Policy และ Log ของ Firewall และ IPS/ IDS อย่างสม่ำเสมอ	/	/	/	๓	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
				๓. จัดทำแผนหรือขั้นตอนปฏิบัติที่จำเป็นตาม ลำดับเมื่อเกิดเหตุการณ์ขึ้นจริงจะได้พร้อมที่จะรับกับสถานการณ์ได้โดยไม่สับสน	/	/	/		
๗.๒ จากภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆ โดยเฉพาะประเภท Trojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายในทั้งที่ไม่ได้ตั้งใจและตั้งใจ	ไม่สามารถใช้งานเครือข่ายได้ หรือใช้ได้แต่ช้ามาก	ปานกลาง ๑x๕=๕	๑. มีมาตรการ และกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรมต่างๆ ลงบนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายอินทราเน็ตของสำนักงานฯ	/	/	/		
				๒. การควบคุมด้วยระบบ Desktop Management	/	/	/		

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
๘. ความเสี่ยงจากการระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหาย	๑. เสี่ยงต่อการไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ ๒. เสี่ยงต่อความเสียหายของข้อมูล และการกู้คืนข้อมูล	การใช้งานระบบงานไม่สามารถใช้ได้ตามปกติ	ปานกลาง ๑x๕=๕	๑. การป้องกันระบบเครื่องแม่ข่ายฐานข้อมูลหลักเสียหายด้วยการเพิ่มประสิทธิภาพ การทำงานในแบบ Hot Standby หรือ Clustering ทุกส่วนของเครื่องแม่ข่ายฐานข้อมูลหลัก	/	/	/	๕	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
				๒. การจัดเก็บฐานข้อมูลสำรอง (Backup) และที่พร้อมใช้งานได้ โดยอาจประสานงานกับบริษัทผู้ให้บริการในลักษณะ Application Service Provider หรือหน่วยงานอื่น ในความตกลงที่จะใช้เครื่องของหน่วยงานอื่น เพื่อใช้งานทดแทนในกรณีที่เกิดความเสียหายต่อเครื่องแม่ข่ายฐานข้อมูลหลักของสำนักงานฯ	/	/	/		
				๓. จัดทำระบบเว็บไซต์สำรอง (Backup Site)	/	/	/		

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
๙. ความเสี่ยงจากการใช้ Wireless เข้าเครือข่ายอินทราเน็ต	เสี่ยงต่อผู้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลเข้าใช้เครือข่ายอินทราเน็ต ผ่านทาง WiFi	ข้อมูลที่เป็นความลับถูกนำออกเผยแพร่หรือนำไปใช้ประโยชน์ อันจะนำมาซึ่งการขาดความเชื่อถือในการจัดเก็บข้อมูลของสำนักงานฯ	ปานกลาง ๑x๕=๕	๑. ควบคุมการเข้าใช้เครือข่ายด้วย NAC, Radius และ Directory เช่น AD หรือ LDAP ร่วมกันในการควบคุมการเข้าใช้งานเครือข่าย ซึ่งในปัจจุบันสำนักงานฯ ได้เริ่มมีการนำระบบดังกล่าวเข้ามาติดตั้งใช้งานอยู่ ๒. เพิ่มความปลอดภัยในการใช้งานเพิ่มขึ้นโดยติดตั้งระบบยืนยันตน (Authentication)	/ /	/ /	/ /	๓	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
๑๐. ความเสี่ยงจากการที่เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	๑. เสี่ยงต่อการใช้ Resources ของสำนักงานฯ ในทางที่ผิด หรือเปล่าประโยชน์ เช่น การฟังวิทยุหรือดูโทรทัศน์ออนไลน์ การโหลด Bit Torrent การดู	๑. สูญเสีย Bandwidth ในเครือข่ายทำให้สำนักงานฯ ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี ๒. สำนักงานฯ อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	ปานกลาง ๒x๒=๔	๑. บริหารจัดการด้วยข้อแนะนำ Ten Ways to Protect Your Network From Insider Threats {ก.๘} (www.enterprisenetworkingplanet.com) เพื่อลดความเสี่ยง ๒. บริหารจัดการในการกำหนด Policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น	/ /	/ /	/ /	๒	ทุกสำนัก

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
	เว็บไซต์ที่ลามก อนาจาร ผิดศีลธรรม เป็นต้น ๒. การใช้ Resource ของสำนักงานฯ ทำผิดกฎหมาย เช่น การ ดาวน์โหลดโปรแกรม หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น			๓. บริหารจัดการในการกำหนด Policy ของอุปกรณ์ Bandwidth Managent เพื่อกำจัดหรือปิดกั้นการใช้ resources ในทางที่ผิด ๔. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ต่างๆ ของสำนักงานฯ ไปใช้ในทางที่ผิด รวมถึงการบันทึกการใช้งานและรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา	/ /	/ /	/ /		
<u>ความเสี่ยงต่ำ</u>									
๑. ความเสี่ยงจากวินาศภัย/ การก่อการร้าย	เสี่ยงต่อการสูญหายและถูกทำลายของอุปกรณ์ และข้อมูลที่เป็นส่วนสำคัญขององค์กร	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	ต่ำ ๑x๓=๓	๑. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน ๒. จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไรและจะใช้เครื่องทดแทนจากที่ใดเพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง ๓. จัดทำระบบเว็บไซต์สำรอง (Backup Site)	/ / /	/ / /	/ / /	๑	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
๒. ความเสี่ยงจากความชื้น อุณหภูมิ	เครื่องมีประสิทธิภาพ (Performance) และ ความเชื่อถือได้ (Stability) ลดลง และเครื่องอาจหยุดทำงานได้	อายุของเครื่องและอุปกรณ์สั้นลง ทำให้สิ้นเปลืองงบประมาณในการจัดการซ่อมแซมหรือจัดหาทดแทน	ต่ำ ๒x๑=๒	๑. บำรุงรักษาระบบปรับอากาศชนิด Precision ที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้นให้อยู่ในสภาวะที่เหมาะสมและสามารถทำงานสลับกันได้ ซึ่งปัจจุบันสำนักงานฯ ได้ติดตั้งระบบนี้ ที่ศูนย์สารสนเทศชั้น ๑๓ อาคารสุขประพฤติแล้ว	/	/	/	๓ ๗ และ ๘	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร ทุกสำนัก
				๒. สำนักงานฯ ควรมีการวางแผนในการจัดทำระบบที่เหมาะสมสำหรับศูนย์สารสนเทศอาคารรัฐสภาแห่งใหม่ด้วย โดยประสานงานกับผู้ออกแบบ และสอดคล้องกับนโยบายของสำนักงานฯ เพื่อลดความเสี่ยงด้านการบริหารจัดการและความเสี่ยงด้านการเงิน เนื่องจากต้องใช้งบประมาณสูงและอาจมีข้อจำกัดหลายๆ ด้าน	/	/	/		

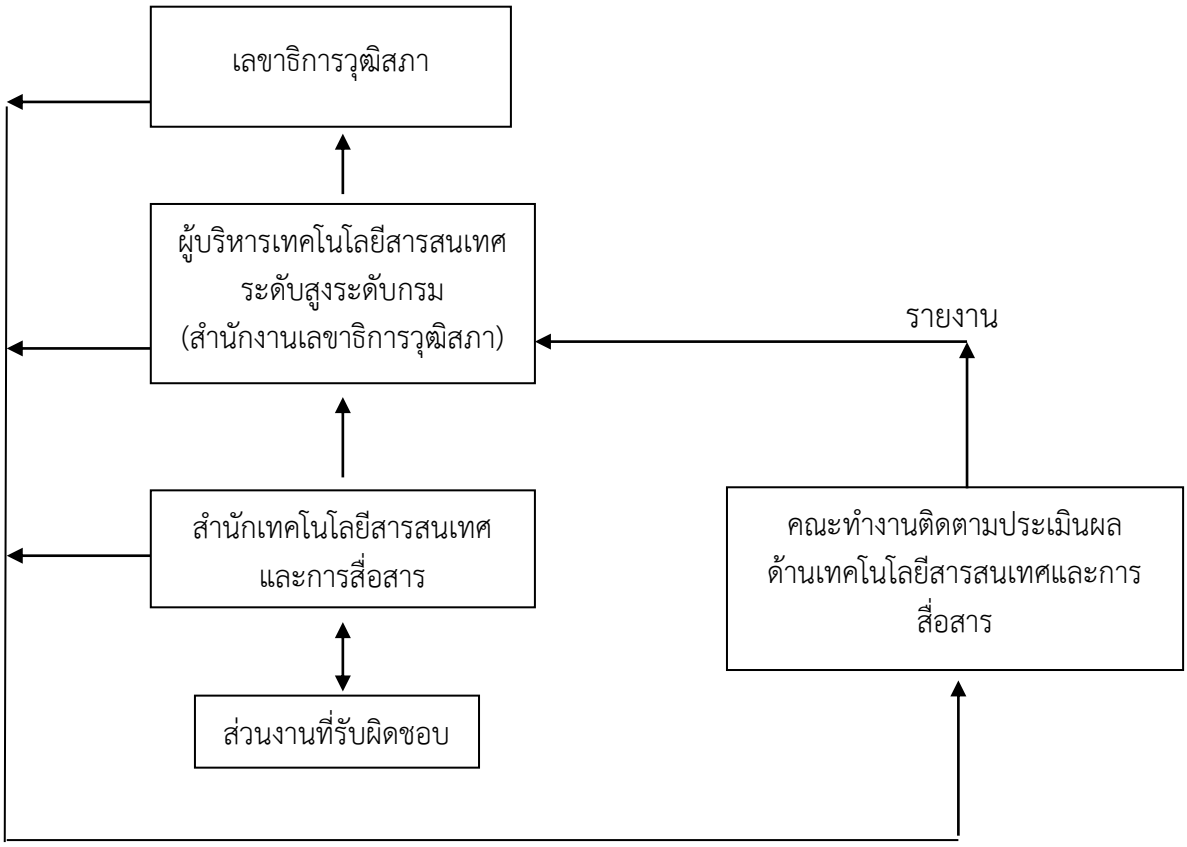
ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
๓. ความเสี่ยงจากแผ่นดินไหว	ความเสียหายด้านโครงสร้างอาจทำลายระบบเครื่องและข้อมูล	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	ต่ำ ๑x๑=๑	๑. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน	/	/	/	๑	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
				๒. จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไรและจะใช้เครื่องทดแทนจากที่ใดเพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง	/	/	/		
				๓. จัดทำระบบเว็บไซต์สำรอง (Backup Site)	/	/	/		
๔. ความเสี่ยงจากการประกาศภาวะฉุกเฉิน (เช่นกรณีเกิดโรคระบาดหรือควัญพิษ) ทำให้บุคลากรไม่สามารถมาปฏิบัติงาน ณ สถานที่ราชการประจำได้	เสี่ยงต่อการกระบวนการปฏิบัติงานรองรับการเชื่อมโยงเครือข่ายของระบบสารสนเทศขององค์กร	ไม่สามารถใช้ระบบงานหรือข้อมูลได้เป็นปกติ	ต่ำ ๑x๑=๑	๑. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน	/	/	/	๑	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
				๒. จัดทำแผนสำรองฉุกเฉิน เพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไรและจะใช้เครื่องทดแทนจากที่ใดเพื่อสามารถจะใช้งานได้อย่างต่อเนื่อง	/	/	/		
				๓. จัดทำระบบเว็บไซต์สำรอง (Backup Site)	/	/	/		

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	มาตรการ/แผนปฏิบัติการ	ระยะ / เวลา (ปีงบประมาณ พ.ศ.)			ประเภทความเสี่ยง	ผู้รับผิดชอบ
					๒๕๖๓	๒๕๖๔	๒๕๖๕		
๕. ความเสี่ยงจากการโจรกรรมฐานข้อมูล	ข้อมูลที่สำคัญรั่วไหลสู่ภายนอกหรือสาธารณะ	๑. เสียชื่อเสียงและความน่าเชื่อถือที่มีต่อสำนักงานฯ ๒. การสูญหายหรือถูกทำลายของข้อมูล	ต่ำ ๑x๑=๑	๑. มีการบริหารจัดการด้านการป้องกันข้อมูล	/	/	/	๕	สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
				๒. มีการบริหารจัดการด้านการเข้าถึงข้อมูล (Access) ตามความสำคัญของข้อมูลโดยสามารถทำงานร่วมกับ Network Access Control (NAC) Radius, Active Directory (AD) หรือ Lightweight Directory Access Protocol (LDAP) Server และ Syslog ได้	/	/	/		
				๓. มีการบริหารสื่อจัดเก็บข้อมูล เช่น Hard Disk ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์ หรือสื่อเก็บข้อมูลนั้นๆทิ้งแล้ว หากทำได้	/	/	/		

๙. การบริหารจัดการและการติดตามประเมินผลแผนบริหารความเสี่ยงระบบเทคโนโลยีดิจิทัล ของ พ.ศ. ๒๕๖๒-๒๕๖๕

สำนักงานเลขาธิการวุฒิสภา ควรกำหนดโครงสร้างการบริหารจัดการและแนวทางการติดตามประเมินผล เพื่อเป็นเครื่องวัดความสำเร็จของแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๓ - ๒๕๖๕ ดังนี้

โครงสร้างการบริหารจัดการ แต่งตั้งคณะทำงานติดตามประเมินผลแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทำการวิเคราะห์และวางระบบติดตามประเมินผล และรายงานผลการทำงานต่อที่ปรึกษาด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเลขาธิการวุฒิสภา



รูปที่ ๒ ผังโครงสร้างการบริหารจัดการและติดตามประเมินผล แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล

<u>ตัวอย่าง</u> แบบรายงานติดตามประเมินผล
แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีดิจิทัล
ปี .....

ความเสี่ยง	ผลกระทบ	มาตรการ/ แผนปฏิบัติการ	ผลการดำเนินงาน	ระยะเวลาในการดำเนินการ	ผู้รับผิดชอบ/ ผู้ดำเนินงาน
๑.....					
๒.....					
๓.....					
๔.....					

ภาคผนวก ก

บันทึกการประชุมระดมสมองเพื่อจัดทำแผนบริหารความเสี่ยง

ของระบบด้านเทคโนโลยีดิจิทัล

วันที่ ๑ เมษายน พ.ศ. ๒๕๖๓ เวลา ๑๓.๓๐-๑๕.๓๐ น.

ณ ห้องประชุม สำนักเทคโนโลยีสารสนเศและการสื่อสาร

สำนักงานเลขาธิการวุฒิสภา อาคารสุขประพฤติ

ผู้เข้าประชุม

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

๑) นายนรมิตร คุณโลกยะ	ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร
๒) นายชัยวุฒิ พุฒพิสุทธิ์	ผู้บังคับบัญชากลุ่มงานวิทยาการคอมพิวเตอร์
๓) นางสาวจิรพรรณ แกล้วทนงค์	ผู้บังคับบัญชากลุ่มงานบริการระบบคอมพิวเตอร์
๔) นางทุติยาพร ทวนทอง	ผู้บังคับบัญชากลุ่มงานพัฒนาระบบงานคอมพิวเตอร์
๕) นายสมชาย ชัยเชษฐ์ดำรงกุล	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
๖) นางสาวสุดารัตน์ ใจอุดม	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
๗) นายประจักษ์ สมลา	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
๘) นายประจักษ์ เพ็ญเลี้ยง	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
๙) นางสาวพัทธกานต์ วุฒิอัครวัฒน์	นักวิชาการคอมพิวเตอร์ชำนาญการ
๑๐) นางสาวเบญจมาศ สำเนียงสูง	เจ้าพนักงานธุรการชำนาญงาน

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร ได้มีการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ประจำปี พ.ศ. ๒๕๖๒ – ๒๕๖๕ และประกาศใช้ในสำนักงานเลขาธิการวุฒิสภา ซึ่งเป็นการพิจารณาความเสี่ยงในทุกๆ ด้าน เช่น ระบบไฟฟ้า ภัยพิบัติ รวมไปถึงด้านเทคโนโลยี เช่น การสำรองข้อมูล เพื่อรองรับ สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) มีการกำหนดตัวชี้วัดของหน่วยงานว่าหน่วยงานจะต้องมีการจัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งแผนนี้จะเน้นความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยเฉพาะ สำหรับขั้นตอนการดำเนินงานในการจัดทำแผน เริ่มจาก

หน่วยงานจัดตั้งคณะทำงาน ทำการทบทวนแผนเดิมหรือจัดทำแผนใหม่ และมีการประกาศใช้แผนที่พัฒนาขึ้น

อย่างไรก็ตาม แผนที่พัฒนาขึ้นนี้ มีการจำแนกกิจกรรมในแต่ละปี มีการกำหนดชื่อบุคคลากรที่จะรับผิดชอบแต่ละกิจกรรมชัดเจน และมีระยะเวลากำกับกิจกรรม ซึ่งสำนักงานฯ จะเลือกซักซ้อมในสถานการณ์ที่มักเกิดขึ้นจริง เช่น กรณีไฟดับ หรือเครือข่ายขัดข้อง ทั้งนี้ หน่วยงานได้มีการติดตามการดำเนินการตามมาตรการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ประจำปี ๒๕๖๒ และได้มีการทบทวนการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา ประจำปี พ.ศ. ๒๕๖๓ – ๒๕๖๕ ได้มีปัจจัยในการพิจารณาเพิ่มเติมในการทบทวนแผนฯ ดังนี้

๑. สำนักงานเลขาธิการวุฒิสภา ได้มีการประกาศใช้ วิสัยทัศน์ และ พันธกิจ ตามแผนปฏิบัติราชการสำนักงานเลขาธิการวุฒิสภา พ.ศ. ๒๕๖๓ – ๒๕๖๕ ที่เกี่ยวข้องด้านเทคโนโลยีดิจิทัลของสำนักงานเลขาธิการวุฒิสภา

๒. สำนักงาน ก.พ. ได้มีหนังสือ ที่ นร ๑๐๑๓/ว ๓ เรื่องแนวทางการบริหารจัดการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐ ลงวันที่ ๓๐ มีนาคม ๒๕๖๓ ซึ่งคณะรัฐมนตรีได้มีมติเห็นชอบ เมื่อวันที่ ๒๖ พฤศจิกายน ๒๕๖๒ ในแนวทางการบริหารจัดการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐ (Government Chief Information Officer Management Guideline) เพื่อปรับปรุงบทบาทหน้าที่ความรับผิดชอบของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐ (Government Chief Information Officer : GCIO) ให้รองรับภารกิจในการปรับเปลี่ยนหน่วยงานภาครัฐเป็นรัฐบาลดิจิทัลและให้ส่วนราชการที่มีฐานะเป็นกรม กำหนดให้มีผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer : DCIO) ประจำหน่วยงาน ซึ่งสำนักงานเลขาธิการวุฒิสภามีฐานะเป็นส่วนราชการระดับกรมจึงต้องโดยเปลี่ยนจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer : DCIO

๓. จากเหตุการโรคระบาดจากเชื้อไวรัสโครน่า (COVID - 19) จัดอยู่ในความเสี่ยงความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) ความเสี่ยงด้านบุคลากร (Human Risk) จากการประกาศภาวะฉุกเฉิน (เช่นกรณี เกิดโรคระบาด หรือควัญพิษ) ส่งผลต่อบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสารมาปฏิบัติงาน ณ สถานที่ราชการประจำได้

ผู้เข้าประชุมเห็นชอบให้มีการทบทวนและจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ประจำปี พ.ศ. ๒๕๖๓ – ๒๕๖๕ ได้ร่วมกันระดมความคิดเห็นเพื่อกำหนดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่อาจเกิดขึ้น และทำการประเมินความเสี่ยง ความเป็นไปได้

ที่จะเกิด ความเสี่ยงและความรุนแรงของผลกระทบ โดยยึดตามแนวการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ประจำปี พ.ศ. ๒๕๖๒ – ๒๕๖๕ มีเกณฑ์การกำหนดระดับคะแนนของความเป็นไปได้ และความรุนแรงของผลกระทบ ดังนี้

Risk Assessment Matrix			ระดับโอกาส (ความเป็นไปได้)				
			ต่ำมาก/ น้อยมาก	ต่ำ/น้อย	ปาน กลาง	สูง/บ่อย	สูงมาก/ บ่อยมาก
			๑	๒	๓	๔	๕
ผลกระทบ (ความรุนแรง)	สูงมาก/หายนะ	๕	๕	๑๐	๑๕	๒๐	๒๕
	สูง/วิกฤต	๔	๔	๘	๑๒	๑๖	๒๐
	ปานกลาง	๓	๓	๖	๙	๑๒	๑๕
	ต่ำ/น้อย	๒	๒	๔	๖	๘	๑๐
	ไม่เป็นสาระสำคัญ/ น้อยมาก	๑	๑	๒	๓	๔	๕

ผลสรุปจากการระดมสมอง เพื่อกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เทคโนโลยีดิจิทัล ความเสี่ยงการโจมตีทางไซเบอร์ รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบ มีดังนี้

ประเภทความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
ลิขสิทธิ์ซอฟต์แวร์	๕	๕	๒๕
การเชื่อมต่อระบบอินเทอร์เน็ต/ อินทราเน็ตขัดข้อง	๕	๓	๑๕
ไวรัสคอมพิวเตอร์/ Malware	๕	๓	๑๕
ช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	๓	๕	๑๕
ความเสี่ยงจากการถูก Black List จาก Search Engine/ Spamhause	๓	๕	๑๕
การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง	๓	๔	๑๒
ความเสี่ยงจากอัคคีภัย	๒	๕	๑๐

ประเภทความเสี่ยง	ความน่าจะเป็นที่จะเกิด	ผลกระทบ	คะแนน
ระบบกระแสไฟฟ้าขัดข้อง	๒	๔	๘
ความเสี่ยงจากอุทกภัย	๒	๓	๖
ความเสี่ยงจากแมลง/สัตว์กัดแทะ	๓	๒	๖
การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย /อุปกรณ์	๒	๓	๖
การไม่สำรองข้อมูล/ การสำรองข้อมูลขาดการอัพเดท	๒	๓	๖
การบุกรุกโจมตีทางไซเบอร์จากภายนอก	๑	๕	๕
การโจมตีทางไซเบอร์ภายในหน่วยงานไม่ให้สามารถให้บริการได้ (Denial of Service-DoS)	๑	๕	๕
ระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักเสียหาย	๑	๕	๕
ความเสี่ยงจากการใช้ Wireless เข้าเครือข่ายอินทราเน็ต	๑	๕	๕
เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	๒	๒	๔
ความเสี่ยงจากไฟกระชากจากปลั๊กพ่วง	๒	๒	๔
วินาศภัย/ การก่อการร้าย	๑	๓	๓
ความเสี่ยงจากความชื้น อุณหภูมิ	๒	๑	๒
ความเสี่ยงจากการประกาศภาวะฉุกเฉิน (จากโรคระบาด/ควันพิษ)	๑	๑	๑
ความเสี่ยงจากแผ่นดินไหว	๑	๑	๑
การโจรกรรมฐานข้อมูล	๑	๑	๑

จากนั้น ที่ประชุมร่วมกันกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีผลคะแนนสูงสุด ๖ อันดับแรก ได้ข้อสรุป ดังนี้

๑) ลิขสิทธิ์ซอฟต์แวร์

<u>แนวทางปฏิบัติ</u>

- การทำสัญญา ข้อตกลงกับบริษัท โดยจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น

- สนับสนุนการใช้ SaaS (Software as a Service) เช่น www.docs.com แทนโปรแกรมลิขสิทธิ์ Microsoft Office

๒) การเชื่อมต่อระบบอินเทอร์เน็ต/ อินทราเน็ตขัดข้อง

<u>แนวทางปฏิบัติ</u>

- ทดสอบด้วยการถอดสัญญาณหลักออกแล้วดูผลว่าทำงานได้อัตโนมัติหรือไม่
- ตรวจสอบ Availability ด้วยเว็บไซต์ Montastic

๓) ไวรัสคอมพิวเตอร์/ Malware

<u>แนวทางปฏิบัติ</u>

- อัพเดทข้อมูลไวรัสเสมอ

๔) ช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร

<u>แนวทางปฏิบัติ</u>

- ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตาม OWASP Top Ten Web Application Security Risks

๕) ความเสี่ยงจากการถูก Black List จาก Search Engine/ Spamhause

<u>แนวทางปฏิบัติ</u>

- ติดตั้งโปรแกรม เพื่อตรวจสอบว่าเครื่อง Mail Server ของสำนักงานฯ ไม่ได้ส่ง Spam

๖) การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง

<u>แนวทางปฏิบัติ</u> กำหนดให้ Outsourcer ส่งข้อมูลต่อไปนี้ ภายหลังการพัฒนาระบบ

- การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level ๒
- มีการจัดทำ ER Diagram
- Source Code บรรจุใน CD ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้
- ถ้ามีการพัฒนา Library ด้วยตนเอง ต้องส่งพร้อม Source Code Library ที่สามารถแก้ไขได้
- มีการถ่ายทอดความรู้ และเทคโนโลยีในการพัฒนาระบบให้กับเจ้าหน้าที่ของสำนักงานฯ
- มีแผนการบำรุงรักษาระบบ
