ประกาศองค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ
เรื่อง แนวปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ตามที่มีประกาศคณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัล เรื่อง นโยบายเทคโนโลยีดิจิทัล องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ ลงวันที่ ๘ กรกฎาคม ๒๕๖๔ เพื่อเป็นแนวทางการบริหารจัดการเทคโนโลยีดิจิทัล นั้น

เพื่อให้เกิดความชัดเจนในการนำไปปฏิบัติตามประกาศดังกล่าว จึงได้จัดทำแนวปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ และเพิ่มประสิทธิภาพการดำเนินงาน รวมทั้งลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นจากกระบวนการปฏิบัติงาน คณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัล ในการประชุมครั้งที่ ๑/๒๕๖๘ เมื่อวันที่ ๑๖ มกราคม ๒๕๖๘ มีมติเห็นชอบแนวปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามที่เอกสารแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๓๐ เมษายน พ.ศ. ๒๕๖๘

(นายสุวรงค์ วงษ์ศิริ)
รองผู้อำนวยการองค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

NSM
องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ

แนวปฏิบัติ
การบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ

ฉบับปรับปรุง 2568

Information Security Risk Management

National Science Museum Thailand

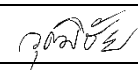
UPDATE 2025

แนวปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

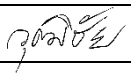
(IT Risk Management)

ประวัติการแก้ไขเอกสาร (Revision History)

ครั้งที่ 1

การลงนามอนุมัติและประกาศใช้งาน			
	ตำแหน่ง	ลงนาม	วันที่
ผู้จัดทำ	นายวุฒิชัย เกตุพรม กองเทคโนโลยีดิจิทัล		1 มี.ค.66
ผู้ทบทวน	ผู้อำนวยการกองเทคโนโลยีดิจิทัล		8 มี.ค.66
ผู้อนุมัติ	ผู้อำนวยการสำนักวิศวกรรมและการผลิตสื่อ		15 มี.ค.66

ครั้งที่ 2

การลงนามอนุมัติและประกาศใช้งาน			
	ตำแหน่ง	ลงนาม	วันที่
ผู้จัดทำ	นักเทคโนโลยีสารสนเทศ		2 มี.ค.67
ผู้ทบทวน	ผู้อำนวนการกองเทคโนโลยีดิจิทัล		23 ก.พ.67
ผู้ทบทวน	ผู้อำนวนการสำนักวิศวกรรมและการผลิตสื่อ		27 ก.พ.67
ผู้ทบทวน	คณะทำงานพัฒนาเทคโนโลยีดิจิทัล	ในการประชุมครั้งที่ 3/67	14 ส.ค.67
ผู้ทบทวน	คณะทำงานพัฒนาเทคโนโลยีดิจิทัล	ในการประชุมครั้งที่ 1/68	10 ม.ค.68
ผู้อนุมัติ	คณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัล	ในการประชุมครั้งที่ 1/68	16 ม.ค.68

ประวัติการแก้ไขเอกสาร			
เวอร์ชั่น	วันที่	รายละเอียด	ผู้ขอแก้ไข
0	15 มี.ค.66	ทั้งหมด	ประกาศใช้ครั้งแรก
1	14 ส.ค.67	ไม่มีแก้ไข	ทบทวน โดยคณะทำงานพัฒนาเทคโนโลยีดิจิทัล ในการประชุมครั้งที่ 3/2567
2	16 ม.ค.68	เพิ่มเติมการกำหนดการวัดติดตามและประเมินผล	กองเทคโนโลยีดิจิทัล

สารบัญ

บทสรุปผู้บริหาร Executive Summary

องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ (อพวช.) มีฐานะเป็นรัฐวิสาหกิจ สังกัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) จัดตั้งขึ้นตามพระราชกฤษฎีกาจัดตั้งองค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ พ.ศ. ๒๕๓๘ โดยมีหน้าที่และความรับผิดชอบ ได้แก่ ดำเนินการส่งเสริม และแสดงกิจกรรมหรือผลงานสิ่งประดิษฐ์ทาง ว และ ท เพื่อให้ความรู้และความบันเทิงแก่ประชาชน ดำเนินการรวบรวมวัตถุ จำแนกประเภทวัตถุ จัดทำบันทึกหลักฐานและสงวนรักษาผลงาน สิ่งประดิษฐ์ทาง ว และ ท เพื่อประโยชน์ในการศึกษา วิจัย และความก้าวหน้าทางวิชาการ ดำเนินการส่งเสริมการวิจัย การให้บริการด้านวิชาการและนิทรรศการทาง ว และ ท แก่หน่วยงานของรัฐและเอกชน จัดนิทรรศการทาง ว และ ท รวมทั้งกิจการอื่นที่เกี่ยวเนื่องกับ ว และ ท เป็นศูนย์รวมทางด้านข้อมูลและวิชาการเกี่ยวกับพิพิธภัณฑ์วิทยาศาสตร์และเทคโนโลยี และให้บริการที่เกี่ยวเนื่องแก่หน่วยงานของรัฐและเอกชนตามความเหมาะสม ร่วมมือกับองค์กรอื่นทั้งในและต่างประเทศ เพื่อประโยชน์ในด้านการพัฒนาพิพิธภัณฑ์วิทยาศาสตร์ และดำเนินกิจกรรมหรือธุรกิจอื่นที่เกี่ยวเนื่องกับกิจการพิพิธภัณฑ์วิทยาศาสตร์

ปัจจุบันการดำเนินงานของ อพวช. กำลังเข้าสู่ยุค digital โดยอาศัยเทคโนโลยีสารสนเทศเป็นตัวขับเคลื่อนและมีบทบาทสำคัญที่ช่วยเสริมสร้างประสิทธิภาพในกระบวนการดำเนินงาน ให้รองรับกลยุทธ์ทางด้านการให้บริการผู้เข้าชม การหารายได้นอกงบประมาณ รวมถึงการบริหารจัดการภายในทั้งตัวชี้วัดด้านการเงิน และตัวชี้วัดที่ไม่ใช่การเงิน อีกทั้งการพัฒนานวัตกรรมกระบวนการดำเนินงานผ่านช่องทางอิเล็กทรอนิกส์ยังเป็นกลไก ในการพัฒนา อพวช. ที่สำคัญ ช่วยเพิ่มศักยภาพ ลดต้นทุน ค่าใช้จ่าย งบประมาณ เพิ่มโอกาสในการแข่งขัน เพื่อสามารถให้บริการผู้เข้าชมได้อย่างสะดวก รวดเร็ว ตอบสนองความต้องการของลูกค้าที่หลากหลายได้อย่างทั่วถึง

การใช้เทคโนโลยีสารสนเทศของ อพวช. จึงนับเป็นโจทย์ที่ท้าทาย ภายใต้บริบทของสภาวะแวดล้อม โครงสร้างพื้นฐานด้านดิจิทัลที่มีการพัฒนาและเปลี่ยนแปลงอย่างรวดเร็ว ตั้งแต่การกำหนดยุทธศาสตร์ในการพัฒนาเทคโนโลยีสารสนเทศเพื่อเป็นตัวขับเคลื่อนกระบวนการดำเนินงาน รวมทั้งการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีที่ อพวช. ต้องปรับตัวให้เท่าทัน และความเสี่ยงในการเผชิญภัยคุกคามทางไซเบอร์ที่นับวันมีแนวโน้มเพิ่มขึ้น มีวิวัฒนาการที่ซับซ้อนขึ้น ส่งผลกระทบที่มีความรุนแรงและ เป็นวงกว้างมากขึ้น ดังเช่น เหตุการณ์ภัยคุกคามทางไซเบอร์ ที่เกิดขึ้นทั่วโลก ไม่ว่าจะกรณีการโจมตีด้วย DDoS จนทำให้ ระบบใช้งานไม่ได้ หรือโปรแกรม Malware ที่เข้าแทรกแซงระบบให้ส่งคำสั่งปลดเงินค่าใช้จ่ายของ อพวช. เป็นต้น

จึงเห็นได้ว่าปัจจุบัน อพวช. กำลังเผชิญกับความเสี่ยง ด้านเทคโนโลยีสารสนเทศในหลายมิติมากขึ้น หาก อพวช. ไม่มีการปรับตัวให้เท่าทันกับการเปลี่ยนแปลง หรือไม่มีการบริหาร จัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เพียงพอ อาจนำไปสู่ความเสี่ยงด้านอื่นที่สำคัญด้วย โดยปัจจุบันความเสี่ยง ด้านเทคโนโลยีสารสนเทศ ไม่เป็นเพียงส่วนหนึ่งของความเสี่ยงด้านปฏิบัติการอีกต่อไป แต่กลายเป็นหนึ่งในความ

เสี่ยงด้านการให้บริการที่สำคัญที่สามารถส่งผลกระทบต่อความเชื่อมั่นของผู้เข้าชม ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กรที่มีต่อการใช้บริการด้านการเบิกจ่ายงบประมาณ การจองเข้าชม และอื่น ๆ ที่หากเกิดเหตุแล้วจะส่งผลต่อภาพลักษณ์และชื่อเสียงของ อพวช. ดังนั้น อพวช. จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบและต่อเนื่อง ซึ่ง อพวช. ตระหนักถึงความสำคัญ และความจำเป็นในการยกระดับความพร้อมรับมือต่อความเสี่ยงที่ อพวช. กำลังเผชิญเพื่อให้ อพวช. มีการกำกับดูแลและบริหารจัดการทรัพยากรเทคโนโลยีสารสนเทศ ทั้งบุคลากร กระบวนการ และ การนำเทคโนโลยีสารสนเทศมาใช้ ภายใต้การบริหารความเสี่ยงอย่างเหมาะสมและเพียงพอรองรับตามระดับความเสี่ยงที่ อพวช. มี โดยเริ่มตั้งแต่คณะกรรมการของ อพวช. และผู้บริหาร อพวช. ที่ให้ความสำคัญในการผลักดันและยกระดับการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศโดยสร้างวัฒนธรรมและพฤติกรรม ร่วมของทุกคนในองค์กรให้ตระหนักถึงความเสี่ยงอย่างรอบด้าน และเป็นรูปธรรม การสร้างธรรมาภิบาลที่ดีในองค์กรโดยมีโครงสร้างและบทบาทหน้าที่ความรับผิดชอบอย่างเหมาะสม การกำหนดกรอบการบริหารความเสี่ยงด้านเทคโนโลยี สารสนเทศที่ชัดเจนเพื่อให้มีการประเมิน และติดตามความเสี่ยง อย่างต่อเนื่อง และเท่าทันกับความเสี่ยงรูปแบบใหม่ที่อาจ เกิดขึ้น การขับเคลื่อนธุรกิจโดยคำนึงถึงการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและปลอดภัย รวมถึงการดูแลให้มีบุคลากรของ อพวช. มีความรู้ความเชี่ยวชาญอย่างเพียงพอ ตลอดจนมีการเสริมสร้างความรู้ความเข้าใจทางด้านเทคโนโลยีดิจิทัล ให้กับพนักงานและลูกจ้างอย่างต่อเนื่อง

อพวช. จึงได้จัดทำประกาศ เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ พร้อมทั้งได้จัดทำแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับประกาศดังกล่าว โดยอ้างอิงมาตรฐานสากลที่ยอมรับโดยทั่วไป โดยมุ่งหวังให้แนวปฏิบัตินี้เกิดประโยชน์ต่อพนักงาน ลูกจ้าง และผู้มีส่วนได้ส่วนเสียของ อพวช. ต่อไป

หลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สรุปหลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีดังนี้

1. การใช้เทคโนโลยีสารสนเทศสอดคล้องกับกลยุทธ์ในการดำเนินกิจการและการเปลี่ยนแปลง

ปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อกระบวนการดำเนินงานของ อพวช. มากขึ้น โดยเป็นโครงสร้างพื้นฐานที่สำคัญที่รองรับกลยุทธ์ในการดำเนินงาน ช่วยเพิ่มประสิทธิภาพ ลดต้นทุนในการดำเนินงาน และเพิ่มศักยภาพในการแข่งขัน ตอบสนองต่อความต้องการของลูกค้าที่ต้องการผลิตภัณฑ์และบริการที่หลากหลายได้อย่างสะดวกและรวดเร็ว นอกจากนี้ อพวช. ยังต้องเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศให้พร้อมรับการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็วเพื่อรองรับการดำเนินงานในอนาคต

2. คณะกรรมการ อพวช. และผู้บริหารมีบทบาทสำคัญในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องมีการกำกับดูแลในระดับองค์กร โดยเป็นความรับผิดชอบของคณะกรรมการของ อพวช. ที่ต้องสนับสนุนและผลักดันให้องค์กรมีกลยุทธ์และนโยบายด้านเทคโนโลยีสารสนเทศที่เพิ่มประสิทธิภาพให้แก่การดำเนินกิจการ ความสามารถในการแข่งขัน มีความมั่นคงปลอดภัยและพร้อมรับมือภัยคุกคามทางเทคโนโลยีและภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมทั้งผลักดันให้ อพวช. มีการสร้างความตระหนักในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness) อย่างต่อเนื่องและมีประสิทธิภาพ

3. ความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงในระดับองค์กร (enterprise wide risk)

เนื่องจากเทคโนโลยีสารสนเทศกลายเป็นโครงสร้างพื้นฐานสำคัญรองรับกระบวนการทางธุรกิจและการปฏิบัติงานด้านต่าง ๆ ของ อพวช. ดังนั้นการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ไม่ได้เป็นความรับผิดชอบอยู่เพียงหน่วยงานด้านเทคโนโลยีสารสนเทศเท่านั้น แต่เป็นเรื่องที่บุคลากรทุกระดับและทุกฝ่ายในองค์กรต้องให้ความตระหนักและมีแนวทาง การบริหารความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศครอบคลุมทั้งในเชิงกลยุทธ์และเชิงปฏิบัติการเพื่อให้มีการป้องกัน ติดตาม และรับมือความเสี่ยงที่อาจเกิดขึ้น ด้วยเหตุนี้ อพวช. จำเป็นต้องมีกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างครอบคลุมทั่วทั้งองค์กรและเหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ โดยครอบคลุมการกำหนดนโยบายและบทบาทหน้าที่ความรับผิดชอบ การพัฒนากระบวนการและเครื่องมือ รวมถึงการพัฒนาความรู้และความเชี่ยวชาญในด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเพียงพอและทั่วถึง

4. มีการกำกับดูแลเป็นไปตามหลัก 3 lines of defence

โครงสร้างการกำกับดูแลการปฏิบัติงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ จำเป็นต้องสอดคล้องตามหลัก 3 lines of defence เพื่อให้สอดคล้องตามหลักการถ่วงดุล (check and balance) และมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจน (segregation of duties) ในการปฏิบัติงาน การบริหารความเสี่ยง การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ

5. การรักษาความมั่นคงปลอดภัยและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศสอดคล้อง กับความเสี่ยงที่เพิ่มขึ้น

ความเสี่ยงที่เกิดจากเทคโนโลยีสารสนเทศหากไม่ได้รับการบริหารจัดการและควบคุมอย่างเพียงพอ อาจทำให้เกิดช่องโหว่ด้านการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบในการให้บริการแก่ธุรกิจและการดำเนินงานของ อพวช. ซึ่งอาจนำไปสู่ความเสี่ยงด้านความน่าเชื่อถือ ชื่อเสียง ภาพลักษณ์ การปฏิบัติ ตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

6. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศอย่างรัดกุมและมีประสิทธิภาพ

ความต้องการของลูกค้าที่ต้องการผลิตภัณฑ์และบริการที่หลากหลาย รวมทั้งการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศที่เป็นไปอย่างรวดเร็ว ทำให้ อพวช.ต้องบริหารจัดการทรัพยากรที่มีอยู่อย่างจำกัดให้มีประสิทธิภาพสูงสุด ดังนั้น หาก อพวช. ไม่สามารถบริหารจัดการโครงการพัฒนาระบบได้อย่างมีประสิทธิภาพ ทำให้ไม่สามารถส่งมอบโครงการได้ ตามเป้าหมายที่กำหนดส่งผลให้เกิดความเสี่ยงที่โครงการด้านเทคโนโลยีสารสนเทศไม่แล้วเสร็จตามกำหนดเวลา โครงการไม่มีคุณภาพ รวมถึงโครงการไม่สอดรับกับกลยุทธ์ทางธุรกิจของ อพวช. นอกจากนี้ในบางกรณีอาจส่งผลให้ อพวช. ไม่สามารถปฏิบัติได้ตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องของผู้กำกับดูแลได้

7. มีการพัฒนาความรู้ความสามารถ (capability) ของบุคลากร

ด้วยวิวัฒนาการของเทคโนโลยีและความเสี่ยงซึ่งมีความซับซ้อนมากขึ้น อพวช. จำเป็นต้องมีการพัฒนาความรู้ด้านเทคโนโลยีอย่างต่อเนื่อง เพื่อเพิ่มมุมมองความรู้และความเชี่ยวชาญของบุคลากรในการระบุประเมิน ควบคุม ติดตาม และรับมือความเสี่ยงจากภัยที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ นอกจากนี้ การดำเนินธุรกิจในยุคดิจิทัล ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศไม่ได้จำกัดอยู่เพียงระดับปฏิบัติการเท่านั้น แต่ยังส่งผลต่อการดำเนินกลยุทธ์ของธุรกิจ ดังนั้นคณะกรรมการ ผู้บริหารระดับสูง และบุคลากรทุกระดับจึงจำเป็นต้องได้รับการพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศและความเสี่ยงต่อธุรกิจรวมถึงติดตามภัยคุกคามทางไซเบอร์ เพื่อให้มีความรู้เท่าทันภัยคุกคามใหม่ ๆ

ความเชื่อมโยงประกาศและแนวปฏิบัติที่เกี่ยวข้อง

1. การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการ อพวช.

วัตถุประสงค์ เพื่อให้คณะกรรมการ อพวช. กำกับดูแลและสนับสนุนให้ อพวช. มีการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศอย่างเพียงพอเหมาะสมและสอดคล้องกับการดำเนินกิจการ

1.1.1 คณะกรรมการ อพวช. ประกอบด้วยกรรมการที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ อย่างน้อย 1 ท่าน เพื่อให้คณะกรรมการ อพวช. สามารถกำหนดทิศทางและกำกับดูแลให้ อพวช. มีการใช้เทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์การดำเนินธุรกิจของ อพวช. มีความรู้เท่าทันความเสี่ยงและพัฒนาการด้านเทคโนโลยีที่เปลี่ยนแปลงไป

1.1.2 ดูแลให้มีการใช้เทคโนโลยีที่สอดรับกับกลยุทธ์ในการดำเนินธุรกิจของสถาบันการเงิน และดูแลให้การใช้เทคโนโลยีของสถาบันการเงินมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและ การเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต

1.1.3 ดูแลให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในฐานะที่เป็นความเสี่ยงที่สำคัญโดยถือเป็น ส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของ อพวช. (Enterprise Risk Management: ERM)

1.1.4 ดูแลให้มีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งรวมถึงนโยบายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยนโยบายดังกล่าวต้องสอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศและความเสี่ยงที่เกี่ยวข้อง รวมทั้งทำหน้าที่ในการอนุมัตินโยบายดังกล่าวด้วย

1.1.5 ดูแลให้มีมาตรฐาน ระเบียบวิธีปฏิบัติ กระบวนการ เครื่องมือ และบุคลากรในการรักษาความมั่นคงปลอดภัย และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายข้อ 1.1.4 รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและ

ประเมินประสิทธิภาพนโยบายดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.1.6 ดูแลให้มีการติดตามตรวจสอบและรายงานต่อคณะกรรมการ อพวช. คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงของ อพวช. อย่างเหมาะสม ในเรื่องที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และการบริหาร ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น ผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของ อพวช. ข้อมูลเกี่ยวกับปัญหาหรือเหตุการณ์ทางด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของ อพวช.

1.1.7 ดูแลและสนับสนุนให้มีการสื่อสารกับบุคลากรของ อพวช. เพื่อให้ตระหนักถึงความสำคัญของความเสี่ยงและ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งเข้าใจการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เพื่อช่วยลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.1.8 คณะกรรมการของ อพวช. ได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศอย่างเพียงพอตามระยะเวลา ที่เหมาะสมเพื่อให้มีความรู้ความเข้าใจด้านเทคโนโลยีสารสนเทศที่เพียงพอต่อการกำกับดูแลและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ อพวช. ให้ทันกับภัยคุกคามใหม่ รวมถึงการพิจารณาเชิงกลยุทธ์ ในการนำเทคโนโลยีมาใช้ในการขับเคลื่อนธุรกิจ

1.2 โครงสร้างองค์กรในการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ เพื่อให้มีโครงสร้างและบทบาทหน้าที่ในการกำกับดูแลการดำเนินงานและการบริหาร ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่เหมาะสมสอดคล้องตามหลัก 3 lines of defence

ภาพที่ 2 โครงสร้างและอำนาจหน้าที่การกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

คณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.2.1 อพวช. มีการตั้งแต่งตั้งคณะทำงานพัฒนาเทคโนโลยีดิจิทัล โดยกำหนดให้มีอำนาจและหน้าที่ในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล และรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ระบบเครือข่ายสื่อสาร ทรัพย์สินด้านเทคโนโลยีสารสนเทศและ

ข้อมูลสารสนเทศ อพวช.ที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึงการถ่วงดุลอำนาจอย่างเป็นอิสระอย่างน้อยครอบคลุม

- **คณะกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ** (เช่น IT Steering Committee หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดกลยุทธ์นโยบาย และแผนงานด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์ของ อพวช. รวมทั้งกำกับดูแลและติดตามการดำเนินงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนี้ อพวช. อาจพิจารณาให้มีคณะกรรมการที่ดูแลงานเฉพาะด้านเพิ่มเติม หากเห็นว่างานดังกล่าวมีนัยสำคัญหรือ มีผลกระทบสูงต่อ อพวช. เช่น คณะกรรมการหรืออนุกรรมการด้านการบริหารความเสี่ยงและควบคุมภายใน โดยมีประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ดิจิทัล) ด้วย เป็นต้น
- **คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ** (เช่น คณะกรรมการบริหารความเสี่ยง คณะกรรมการบริหารความเสี่ยงด้านปฏิบัติการ คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแล ให้มีการกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งกำกับดูแลและติดตามให้เป็นไปตามนโยบายที่กำหนดไว้ โดยมีการเชื่อมโยงกับความเสี่ยงในภาพรวมของ อพวช. (enterprise risk management)
- **คณะกรรมการกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ** (เช่น คณะกรรมการตรวจสอบ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อให้ อพวช. มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเป็นอิสระ ครอบคลุมถึงการปฏิบัติงานและการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ รวมทั้ง การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

โครงสร้างองค์กร

1.2.2 อพวช. มีโครงสร้างองค์กรและหน้าที่ความรับผิดชอบเป็นลายลักษณ์อักษร โดยสอดคล้องตามหลัก การถ่วงดุล (check and balance) และการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจน (segregation of duties) ระหว่างการทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ

1.2.3 อพวช. ดูแลให้มีทรัพยากรเพียงพอที่จะสนับสนุนการปฏิบัติงาน การบริหารความเสี่ยง การกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ สอดคล้องตามปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น จัดให้มีบุคลากรที่มีความรู้ความเชี่ยวชาญและมีเครื่องมือหรือระบบที่ช่วยสนับสนุนการปฏิบัติงาน เป็นต้น

1.2.4 อพวช. พิจารณาจัดให้มีผู้บริหารระดับสูงหรือหัวหน้าสายงานที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) โดยควรมีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และควรเป็นผู้ที่มีความรู้ความสามารถด้านเทคโนโลยีสารสนเทศ และด้านการบริหารจัดการและรับมือกับภัยคุกคามทางไซเบอร์ เช่น ได้รับการรับรองความรู้ความสามารถ ตามมาตรฐานของประเทศ เป็นต้น

1.2.5 หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและผู้ใช้งานระบบเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 1st line of defence) เช่น หน่วยงานด้านเทคโนโลยีสารสนเทศ หน่วยงานอื่นที่เป็นผู้ใช้งานระบบ เป็นต้น

- ***หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ*** มีหน้าที่ปฏิบัติงานตามที่ได้รับมอบหมายรวมทั้งประเมินความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศ จัดให้มีแนวทางการควบคุม ติดตามและรายงานการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยนำเสนอต่อคณะกรรมการที่ได้รับมอบหมายและผู้บริหารระดับสูงที่เกี่ยวข้อง อย่างน้อยครอบคลุม
  - รายงานผลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations) เช่น สถานะความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศ (capacity and system utilization) เหตุการณ์ผิดปกติ และปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem) ระดับการให้บริการงาน ด้านเทคโนโลยีสารสนเทศ (service availability) เป็นต้น
  - รายงานความคืบหน้า ปัญหาและอุปสรรคในการดำเนินโครงการด้านเทคโนโลยีสารสนเทศ ในภาพรวมและรายโครงการที่สำคัญ
  - รายงานการติดตามและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งแนวโน้มความเสี่ยงและภัยคุกคามที่อาจจะเกิดขึ้นและส่งผลกระทบต่อ อพวช.

- รายงานผลการประเมินความเสี่ยง การติดตามความเสี่ยง และแนวทางการควบคุมที่เกี่ยวข้อง
- รายงานความคืบหน้าการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง
- รายงานผลการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก

- ***ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ*** มีหน้าที่ปฏิบัติตามนโยบายและระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งมีส่วนร่วมรับผิดชอบในการประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องจากการใช้งานระบบ

1.2.6 **หน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 2nd line of defence)** เช่น หน่วยงานบริหารความเสี่ยง และหน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ เป็นต้น

- **หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง** มีหน้าที่กำหนดกรอบและกระบวนการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ สนับสนุนให้มีการประเมินความเสี่ยงเป็นไปตามกรอบการบริหารความเสี่ยง ที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยงและทบทวนการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ของหน่วยงานที่ทาหน้าที่เป็น 1st line of defence โดยมีการรวบรวมและเชื่อมโยงความเสี่ยงด้านเทคโนโลยีสารสนเทศกับความเสี่ยงด้านอื่นของ อพวช.และเสนอผลการบริหารความเสี่ยงต่อคณะกรรมการที่ทาหน้าที่กำกับดูแลความเสี่ยง
- **หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ** มีหน้าที่กำหนดกระบวนการติดตามดูแล ให้คำปรึกษา สอบทานและรายงานการปฏิบัติ ตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง และนำเสนอต่อคณะกรรมการที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นต้น เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานที่เกี่ยวข้อง
- **หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ (หน่วยงานที่ทำหน้าที่เป็น 3nd line of defence)** ซึ่งอาจเป็นผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้าน

เทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น หน่วยงานตรวจสอบภายใน เป็นต้น

- **หน่วยงานที่ทำหน้าที่ตรวจสอบ** มีหน้าที่ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงของหน่วยงานที่ทำหน้าที่ 1st lineและ 2nd line of defence รวมถึงงานอื่น ๆ ที่เกี่ยวข้อง เช่น การใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ เป็นต้น เพื่อสอบทานให้มั่นใจว่า มีการปฏิบัติที่เป็นไปตามนโยบาย มาตรฐาน และระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศ
- กรณี อพวช. มีข้อจำกัดด้านบุคลากรที่ไม่เพียงพอหรือมีความรู้ความเชี่ยวชาญด้านการตรวจสอบเทคโนโลยีสารสนเทศที่ไม่เพียงพอ อาจพิจารณาว่าจ้างผู้ตรวจสอบภายนอกที่มีความเป็นอิสระ และได้รับมาตรฐานสากลที่ยอมรับโดยทั่วไปในการตรวจสอบเทคโนโลยีสารสนเทศดำเนินการแทนได้
- มีกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมอย่างน้อย ดังนี้
  - **การวางแผนงานและกำหนดขอบเขตการตรวจสอบ** (planning and scoping) ครอบคลุม และสอดคล้องกับความสำคัญและความเสี่ยงของการใช้งานเทคโนโลยีสารสนเทศของ อพวช. และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยแผนงานและขอบเขตการตรวจสอบต้องได้รับความเห็นชอบจากคณะกรรมการตรวจสอบ และมีการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
  - **การตรวจสอบ** (execution) อย่างน้อยปีละ 1 ครั้งตามแผนงานและขอบเขตที่กำหนด และพิจารณาให้มีการตรวจสอบเมื่อมีเหตุการณ์ผิดปกติในงานด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ นอกจากนี้แนวทางการตรวจสอบควรเป็นไปตามมาตรฐานที่ อพวช. กำหนด ซึ่งสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง รวมถึงมาตรฐานสากลที่ยอมรับโดยทั่วไป
  - **การวิเคราะห์** (analysis) นำข้อมูลที่ได้จากการตรวจสอบมาวิเคราะห์เพื่อสรุปผลการตรวจสอบ และอาจพิจารณาการขยายขอบเขตการตรวจสอบเพิ่มเติม หากมีความจำเป็น เช่น พบข้อบ่งชี้ถึงความเสี่ยงที่อาจกระทบต่อ อพวช. อย่างมีนัยสำคัญ
  - **การรายงานและติดตามผลการตรวจสอบ** (reporting and follow up) มีการสรุปผลการตรวจสอบและประเด็นที่ต้องแก้ไขกับผู้บริหารของหน่วยงานผู้รับตรวจและจัดทำรายงานผลการตรวจสอบ เพื่อนำเสนอต่อ

คณะกรรมการตรวจสอบและแจ้งให้ผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบ ตลอดจนจัดเก็บรายงานผลการตรวจสอบไว้ที่ อพวช.พร้อมไว้ สำหรับการตรวจสอบหรือเมื่อร้องขอโดยหน่วยงานที่เกี่ยวข้อง นอกจากนี้ อพวช. ต้องจัดให้มีการติดตามการแก้ไขประเด็นที่ตรวจพบภายในระยะเวลาที่กำหนดและรายงานต่อคณะกรรมการตรวจสอบ

- อพวช. ควรจัดให้มีผู้เชี่ยวชาญภายนอกที่เป็นอิสระทำหน้าที่ประเมินระบบหรือเทคโนโลยีที่มีความสำคัญ ซึ่ง อพวช. เห็นว่ามีความจำเป็นต้องประเมินแต่มีข้อจำกัดหรือผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของ อพวช. ไม่สามารถประเมินได้ เช่น การประเมินระบบที่มีความซับซ้อนหรือมีการใช้เทคโนโลยีใหม่ หรือ การประเมินความสามารถของระบบในการปรับเปลี่ยนเพื่อรองรับการทำธุรกิจของ อพวช. ในอนาคตภายใต้สภาวะการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็ว

1.3 การบริหารจัดการบุคลากร

วัตถุประสงค์ เพื่อให้ อพวช. มีบุคลากรที่มีความรู้และความเชี่ยวชาญเพียงพอในการปฏิบัติงานที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศ โดยบุคลากรทุกระดับมีความตระหนักถึงการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศของ อพวช.

1.3.1 มีกระบวนการบริหารจัดการบุคลากรอย่างเหมาะสม ครอบคลุม การคัดเลือกบุคลากรที่มีความรู้ความสามารถเพียงพอ การว่าจ้างบุคลากรที่เป็นไปตามข้อกำหนดหรือเงื่อนไขด้านความปลอดภัยเทคโนโลยีสารสนเทศ การพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ การเปลี่ยนแปลงหรือสิ้นสุดการว่าจ้างบุคลากร รวมทั้งการดูแลบุคลากรให้เพียงพอกับปริมาณการใช้เทคโนโลยีสารสนเทศ

1.3.2 อพวช.มีกระบวนการบริหารจัดการบุคลากรอย่างเหมาะสมครอบคลุม การคัดเลือกบุคลากรที่มีความรู้ความสามารถเพียงพอ การว่าจ้างบุคลากรที่เป็นไปตามข้อกำหนดหรือเงื่อนไขด้านความปลอดภัยเทคโนโลยีสารสนเทศ การพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ การเปลี่ยนแปลงหรือสิ้นสุดการว่าจ้างบุคลากร รวมทั้งการดูแลบุคลากรให้เพียงพอกับปริมาณการใช้เทคโนโลยีสารสนเทศ อาจพิจารณาการได้รับการรับรองความรู้ความสามารถตามมาตรฐานที่รับรองทั่วไป (certificate) เฉพาะด้านที่เกี่ยวข้องกับงาน

ด้านเทคโนโลยีสนเทศ เพื่อให้ได้บุคลากรที่มีคุณสมบัติเหมาะสม มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

1.3.3 กองทรัพยากรบุคคล ตรวจสอบประวัติของบุคลากรก่อนการว่าจ้างตามความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ เช่น ประวัติการศึกษา ประวัติการทำงาน ประวัติอาชญากรรม เป็นต้น

1.3.4 มีข้อกำหนดหรือเงื่อนไขการว่าจ้างงาน โดยกล่าวถึงบทบาทหน้าที่ความรับผิดชอบการปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ อพวช.เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศของ อพวช.

1.3.5 ให้บุคลากรและผู้ให้บริการภายนอกที่ได้รับการว่าจ้างทำความเข้าใจรับทราบและลงนามยอมรับเงื่อนไขการว่าจ้างงาน นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ อพวช. และข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) ก่อนเริ่มปฏิบัติงาน

1.3.6 กำหนดโปรแกรมการอบรมและพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ (training program) ที่ครอบคลุม การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ให้แก่บุคลากรทุกระดับ โดยมีการวัดประสิทธิผลของหลักสูตรฝึกอบรมที่จัดขึ้น เช่น

- หลักสูตรฝึกอบรมบุคลากรที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (1st line of defence) ให้มีความรู้และความเชี่ยวชาญที่เพียงพอต่อการปฏิบัติงานและการใช้งาน
- หลักสูตรฝึกอบรมบุคลากรที่เกี่ยวข้องกับงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (2ndline of defence) และการตรวจสอบด้านเทคโนโลยีสารสนเทศ (3rd line of defence) ให้มีความรู้และความเชี่ยวชาญเพียงพอที่จะระบุประเมิน และให้ข้อเสนอแนะในการปรับปรุงประสิทธิภาพของการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่หน่วยงานที่ทำหน้าที่ 1st line of defence

1.3.7 กำหนดโปรแกรมในการเสริมสร้างความตระหนัก (awareness program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย เช่น การทดสอบเรื่อง social engineering และ phishing

การซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือ กับการโจมตีทางไซเบอร์ เป็นต้นโดยโปรแกรมดังกล่าวควรครอบคลุมตั้งแต่ระดับคณะกรรมการ ผู้บริหารระดับสูง และบุคลากรทุกระดับ รวมถึงบุคคลภายนอกที่เกี่ยวข้อง รวมทั้งมีการจัดกิจกรรมเสริมสร้างความตระหนักอย่างต่อเนื่อง นอกจากนี้ อพวช. ควรจัดให้มีการประชาสัมพันธ์เพื่อสร้างความรู้หรือสร้างความตระหนักในการใช้งานบริการทางอิเล็กทรอนิกส์อย่างปลอดภัยให้แก่ลูกค้าของ อพวช. ทราบอย่างสม่ำเสมอด้วย

1.3.8 มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงาน เช่น การคืนสินทรัพย์ของ อพวช. การบริหารจัดการสิทธิ์ต้องมีการปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องมีการสื่อสารให้ผู้เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ์ หน้าที่และความรับผิดชอบ เป็นต้น

1.4 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ เพื่อให้ อพวช. มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและสอดคล้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศของ อพวช.

1.4.1 อพวช. กำหนดให้มีนโยบายเป็นลายลักษณ์อักษรและอยู่ใต้กรอบหลักการที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล (confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (integrity) และ ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ อย่างน้อยครอบคลุมนโยบายดังต่อไปนี้

- นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy)
- นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy)
- นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT outsourcing policy)

1.4.2 นโยบายดังกล่าวควรสอดคล้องกับกลยุทธ์ในการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจ นโยบายการบริหารความเสี่ยงของ อพวช. รวมทั้งสอดคล้องกับแนวทางบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัย ตามมาตรฐานสากลหรือมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

1.4.3 นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการของ อพวช. และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งควรจัดให้มีการชี้แจง

และสื่อสารนโยบายให้ผู้เกี่ยวข้อง ได้รับทราบอย่างทั่วถึงและมีการควบคุมดูแลให้มีการปฏิบัติตามนโยบายได้อย่างถูกต้องครบถ้วน

1.4.4 **นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy)** ควรรวมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมอย่างน้อย

- การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)
- การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)
- การควบคุมการเข้าถึง (access control)
- การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)
- การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)
- การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)
- การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (system acquisition and development)
- การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem management)
- การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การบริหารจัดการผู้ให้บริการภายนอก (third party management)

1.4.5 **นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy)** โดยครอบคลุมอย่างน้อย

- โครงสร้างองค์กร บทบาทหน้าที่ของผู้เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- จัดทำหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้

(1) การประเมินความเสี่ยง (risk assessment)

(1.1) การระบุความเสี่ยง (risk identification)

อพวช. ควรจัดให้มีการระบุเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นหรือที่เกิดขึ้นจริง รวมถึงภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง

ๆ ที่ส่งผลกระทบต่อ การดำเนินธุรกิจของ อพวช. โดยเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรระบุอย่างน้อยครอบคลุม

- ผู้กระทำให้เกิดความเสี่ยงและเหตุการณ์ความเสี่ยง เช่น ผู้ไม่ประสงค์ดี ภัยคุกคามหรือช่องโหว่ เป็นต้น
- ประเภทของความเสี่ยง เช่น ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ ความเสี่ยงด้านโปรแกรม ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงด้านการบริหารโครงการ เป็นต้น
- วัน เวลา สถานที่ ช่วงเวลาหรือระยะเวลาที่เกิดเหตุการณ์ผิดปกติหรือความเสี่ยง ด้านเทคโนโลยีสารสนเทศ (ถ้ามี)
- สาเหตุของการเกิดเหตุการณ์ เช่น กระบวนการปฏิบัติงาน ระบบงาน บุคลากร ปัจจัยภายนอก เป็นต้น
- ผลกระทบต่อทรัพย์สินทรัพยากร การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และการดำเนินธุรกิจของ อพวช.

ทั้งนี้ ผู้ที่มีส่วนร่วมในการระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศควรมีความรู้ และความเข้าใจถึงเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ได้ระบุไว้เป็นอย่างดี

(1.2) การวิเคราะห์ความเสี่ยง (risk analysis)

อพวช. ควรจัดให้มีการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อหาแนวทาง ในการจัดการความเสี่ยงที่เหมาะสม โดยควรดำเนินการ ดังนี้

- กำหนดเจ้าของความเสี่ยงด้านเทคโนโลยีสารสนเทศ (risk owner)
- ระบุการควบคุมที่มีอยู่ในปัจจุบัน (existing control)
- พิจารณาและค้นหาสาเหตุและสถานการณ์ที่เป็นไปได้
- วิเคราะห์ผลกระทบที่เกิดขึ้นจากเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(1.3) การประเมินค่าความเสี่ยง (risk evaluation)

อพวช. ควรประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ เพื่อจัดลำดับในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยควรดำเนินการ ดังนี้

- กำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบเช่น ด้านการเงิน ด้านปฏิบัติการ เป็นต้น
- กำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)
- ประเมินค่าโอกาสและผลกระทบของเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- จัดลำดับความเสี่ยงด้านเทคโนโลยีสารสนเทศแสดงในแผนภาพความเสี่ยง ด้านเทคโนโลยีสารสนเทศ

(2) การจัดการความเสี่ยง (risk treatment)

- อพวช. ควรจัดให้มีแนวทางในการจัดการควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)โดยควรครอบคลุมอย่างน้อย ดังนี้
- กำหนดแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการเลือกแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรพิจารณาถึง ความคุ้มค่าและวิธีการที่เหมาะสมสำหรับ อพวช. เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง การลดหรือบรรเทาโอกาสเกิดความเสี่ยง การลดหรือบรรเทาผลกระทบที่เกิดขึ้น การแบ่งหรือโอนความเสี่ยงให้หน่วยงานอื่น การยอมรับความเสี่ยงไว้โดยแจ้งเหตุผลให้ผู้บริหารทราบเพื่อตัดสินใจในการยอมรับความเสี่ยง เป็นต้น
- ระบุรายละเอียดของงานที่ต้องดำเนินการผู้รับผิดชอบ ระยะเวลาที่ใช้ในการดำเนินการ
- ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้
- จัดทำแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดลำดับความสำคัญ ในการดำเนินการ
- นำเสนอและขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

- ดำเนินการสื่อสารแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

นอกจากนี้ อพวช. ควรจัดให้มีการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ให้สอดคล้องกับความสำคัญของงานเทคโนโลยีสารสนเทศ แต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

(3) การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

อพวช. ควรกำหนดผู้รับผิดชอบและจัดให้มีกระบวนการในการติดตามดัชนีชี้วัดความเสี่ยง ด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ตามที่กำหนดและทบทวนความเสี่ยง ด้านเทคโนโลยีสารสนเทศ ให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรจัดให้มีการจัดเก็บและบันทึกข้อมูลอย่างเป็นระบบ เพื่อใช้ติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพ ครอบคลุมอย่างน้อย

- การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง ด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง
- ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อจำกัดที่เกิดขึ้น
- ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นกับ อพวช. และองค์กรอื่น
- รายงานความคืบหน้าของแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามรอบที่กำหนด
- ควรจัดให้มีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรครอบคลุมอย่างน้อยดังนี้
- กำหนดแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการเลือกแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมสาหรับ อพวช. เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง การลดหรือบรรเทาโอกาสเกิดความเสี่ยง การลดหรือบรรเทาผลกระทบที่เกิดขึ้น การแบ่งหรือ

โอนความเสี่ยงให้หน่วยงานอื่น การยอมรับความเสี่ยงไว้โดยแจ้งเหตุผลให้ผู้บริหารทราบเพื่อตัดสินใจในการยอมรับความเสี่ยง เป็นต้น

- ระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ ระยะเวลาที่ใช้ในการดำเนินการ
- ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้
- จัดทำแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดลำดับความสำคัญ ในการดำเนินการ
- นำเสนอและขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ดำเนินการสื่อสารแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

นอกจากนี้ อพวช.ควรจัดให้มีการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators)

ให้สอดคล้องกับความสำคัญของงานเทคโนโลยีสารสนเทศ แต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

(3) การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

อพวช. ควรกำหนดผู้รับผิดชอบและจัดให้มีกระบวนการในการติดตามดัชนีชี้วัดความเสี่ยง ด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) ตามที่กำหนดและทบทวนความเสี่ยง ด้านเทคโนโลยีสารสนเทศให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite) โดยควรจัดให้มีการจัดเก็บและบันทึกข้อมูลอย่างเป็นระบบ เพื่อใช้ติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพครอบคลุมอย่างน้อย

- การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง ด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง
- ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อจำกัดที่เกิดขึ้น
- ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นกับ อพวช. และองค์กรอื่น

- รายงานความคืบหน้าของแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามรอบที่กำหนด

(4) การรายงานความเสี่ยง (risk reporting)

อพวช. ควรจัดให้มีกระบวนการนำเสนอผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ พร้อมทั้งรายงานผลการประเมินและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยเชื่อมโยง กับความเสี่ยงในระดับองค์กร รวมทั้งรายงานแนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นต่อคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายในของ อพวช. และคณะกรรมการ อพวช. อย่างน้อยไตรมาสละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่า อพวช. มีการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศที่เหมาะสมและต่อเนื่อง โดยการรายงานควรครอบคลุมอย่างน้อย

- สถานะและผลลัพธ์การดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศประจำปี
- ผลการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร
- รายงานดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ และรายงานสรุปเหตุการณ์ผิดปกติ
- แนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นกับ อพวช.
- ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง

ทั้งนี้ อพวช. ควรจัดให้มีการทบทวนหลักเกณฑ์ ระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.4.6 **นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT outsourcing policy)** โดยครอบคลุมอย่างน้อย

- หลักเกณฑ์การแบ่งประเภทของการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ
- แนวทางการบริหารจัดการความเสี่ยง แนวทางการคัดเลือกผู้ให้บริการ และแนวทางการประเมินประสิทธิภาพของผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ
- แนวทางการรักษาความมั่นคงปลอดภัยของระบบงานและข้อมูล

- การรายงานผลการประเมินความเสี่ยงและประสิทธิภาพการดำเนินงานของผู้ให้บริการภายนอก ด้านงานเทคโนโลยีสารสนเทศ
- การตรวจสอบผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ
- การคุ้มครองผู้ใช้บริการของ อพวช. จากการใช้บริการผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ

2. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

2.1 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

วัตถุประสงค์ เพื่อให้ อพวช.มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างครบถ้วนและควบคุม ดูแลทรัพย์สินด้านเทคโนโลยีสารสนเทศให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

2.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ครอบคลุม การจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน

2.1.2 จัดให้มีหน่วยงานผู้รับผิดชอบในการจัดทำปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ และบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมทั้งวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support) จากผู้ผลิตได้อย่างเหมาะสมทันการณ์

2.1.3 มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT inventory list) ของฮาร์ดแวร์ (hardware) และซอฟต์แวร์ (software) ที่รองรับระบบเทคโนโลยีสารสนเทศของ อพวช. อย่างครบถ้วนและเป็นลายลักษณ์อักษร โดยครอบคลุมอย่างน้อย ดังนี้

- ชื่อเครื่องแม่ข่าย
- ชื่อระบบปฏิบัติการ (operating system) และเวอร์ชัน
- ชื่อระบบงาน (application) และเวอร์ชัน
- ประเภทของอุปกรณ์ ยี่ห้อ รายละเอียดทางเทคนิค (specification)
- หมายเลขอ้างอิงของฮาร์ดแวร์ (serial number) และหมายเลขอ้างอิงของซอฟต์แวร์ (software license)
- สถานที่ตั้ง

- วันที่เริ่มติดตั้ง
- รายละเอียดผู้ให้บริการหรือผู้บำรุงรักษา
- วันที่บำรุงรักษาล่าสุด
- วันสิ้นสุดการใช้งานตามสัญญา (warranty) และวันสิ้นสุดการรับประกันการใช้งาน (support contract)
- วันสิ้นสุดการให้บริการจากผู้ผลิต (end of support)

2.1.4 มีการปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการตรวจสอบทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับทะเบียนรายการอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

2.1.5 มีกระบวนการในการยกเลิกและเรียกคืนทรัพย์สิน (return asset) เมื่อสิ้นสุดการใช้งาน ครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายใน อพวช. และกรณีที่ผู้ให้บริการภายนอกมีการใช้งานทรัพย์สินของ อพวช. ทันทีที่มีการยกเลิกสัญญาจ้างด้วย

2.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

วัตถุประสงค์ เพื่อให้ อพวช.มีการรักษาความมั่นคงปลอดภัยและความลับของข้อมูล ครอบคลุมการรับส่งข้อมูล ผ่านเครือข่ายสื่อสาร การจัดเก็บหรือใช้งานบนระบบและสื่อบันทึกข้อมูลต่างๆ

การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

2.2.1 กำหนดให้มีเจ้าของข้อมูล (Information Owner) รับผิดชอบในการกำหนดผู้ใช้งาน สิทธิการเข้าถึงและการใช้งานข้อมูลอย่างปลอดภัย

2.2.2 กำหนดหลักเกณฑ์การจัดชั้นความลับของข้อมูล (information classification) โดยควรระบุชั้นความลับของข้อมูล (labeling) อย่างชัดเจน

2.2.3 กำหนดแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลที่สอดคล้องตามชั้นความลับครอบคลุม

- ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint)
- ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit)
- ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest)

2.2.4 กำหนดแนวทางการควบคุมดูแลรักษาความปลอดภัยสื่อบันทึกข้อมูลระหว่างขนส่ง เพื่อให้มีการควบคุมการเข้าถึงสื่อที่มีข้อมูลสำคัญในระหว่างการขนส่ง

2.2.5 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการทำลายข้อมูล (information disposal) ครอบคลุมขอบเขตหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการทำลายข้อมูลให้

สอดคล้องกับระดับความสำคัญ ของข้อมูล โดยมีกระบวนการควบคุมการทำลายข้อมูลที่ครอบคลุมการอนุมัติจากหน่วยงานเจ้าของข้อมูลก่อนดำเนินการ การควบคุมการทำลายในลักษณะ dual control การสอบทานการปฏิบัติงานโดยหัวหน้างาน รวมทั้งจัดให้มีการจัดทำทะเบียนการทาลายข้อมูลสำคัญ โดยระบุผู้รับผิดชอบในการทำลายข้อมูล วันที่ เวลา ชนิดของสื่อบันทึกข้อมูล serial number และวิธีการที่ใช้ทำลายข้อมูล

การบริหารจัดการการเข้ารหัสข้อมูล (cryptography)

2.2.6 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูลครอบคลุมขอบเขตหน้าที่ ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการเข้ารหัสข้อมูลที่สอดคล้องตามระดับความสำคัญของข้อมูล

2.2.7 กำหนดให้มีการเข้ารหัสข้อมูลสำคัญและช่องทางการสื่อสารที่ใช้รับส่งข้อมูลสำคัญกับภายนอก

2.2.8 วิธีการเข้ารหัสข้อมูล ควรใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล เช่น การเข้ารหัสข้อมูลแบบสมมาตร (เช่น AES) การเข้ารหัสข้อมูลแบบอสมมาตร (เช่น public key cryptography) เป็นต้น

2.2.9 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management) ควรกำหนดกระบวนการที่มีความรัดกุมปลอดภัยครอบคลุมตั้งแต่การสร้างและติดตั้งการจัดเก็บและการยกเลิกกุญแจเข้ารหัสข้อมูล

2.3 การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์ เพื่อให้ อพวช. มีการบริหารจัดการข้อมูลของผู้ใช้งานให้มีประสิทธิภาพเป็นไปตามหลักความจำเป็นของการใช้งานและสอดคล้องกับหลักการแบ่งแยกงานด้านเทคโนโลยีสารสนเทศที่ดี โดยสามารถ ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2.3.1 แนวทางการควบคุมการเข้าถึงให้ อพวช. ปฏิบัติตามแนวปฏิบัติที่ดีสาหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices)

2.4 การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

2.4.1 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

วัตถุประสงค์ เพื่อให้ อพวช. มีการบริหารจัดการการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศสอดคล้องตามมาตรฐานสากล โดยมีการควบคุมที่รัดกุมปลอดภัยเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างครบถ้วนถูกต้อง

2.4.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร เพื่อควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศให้มีความรัดกุมเพียงพอ

2.4.1.2 กำหนดบทบาทหน้าที่และความรับผิดชอบของผู้บริหารที่ได้รับมอบหมายหรือคณะกรรมการบริหารจัดการการเปลี่ยนแปลง (Change Advisory Board:CAB) ซึ่งควรประกอบด้วยผู้บริหารจากหน่วยงานเทคโนโลยีสารสนเทศและหน่วยงานผู้ใช้งานเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อทำหน้าที่ประเมินผลกระทบและพิจารณาเหตุผลความจำเป็นก่อนอนุมัติให้ดำเนินการเปลี่ยนแปลงระบบ ป้องกันการแก้ไขเปลี่ยนแปลง โดยไม่ได้รับอนุญาตและไม่ให้เกิดผลกระทบที่อาจเกิดกับระบบที่เกี่ยวข้อง โดยครอบคลุมอย่างน้อยดังนี้

- ผลการประเมินความเสี่ยงและผลกระทบของการเปลี่ยนแปลง โดยมีหน่วยงานเจ้าของระบบและผู้มีหน้าที่เกี่ยวข้องทำการประเมินองค์ประกอบที่เกี่ยวข้อง ได้แก่ ระบบโครงสร้างพื้นฐานเครือข่ายสื่อสารและการเชื่อมต่อกับระบบอื่น เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้น ไม่กระทบต่อการรักษา ความปลอดภัย ความถูกต้องเชื่อถือได้ ความพร้อมใช้ของระบบ
- ผลการทดสอบ เพื่อให้มั่นใจว่าระบบได้ผ่านการทดสอบอย่างครบถ้วนเหมาะสมตามมาตรฐานและระเบียบวิธีปฏิบัติของ อพวช.
- ข้อจำกัดหรือปัญหาต่าง ๆ ที่พบในระหว่างการทดสอบได้รับการแก้ไขอย่างเหมาะสม
- แผนย้อนกลับ กรณีที่ทำการเปลี่ยนแปลงไม่สำเร็จ เพื่อรองรับปัญหาขัดข้อง ระหว่างการเปลี่ยนแปลง
- ตารางเวลาการเปลี่ยนแปลงในภาพรวม change calendar เพื่อบริหารทรัพยากรและลดความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้น

2.4.1.3 ผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการการเปลี่ยนแปลงควรมีการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ผู้มีสิทธิ์ร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น

2.4.1.4 มีหลักเกณฑ์ในการจัดประเภทการเปลี่ยนแปลงระบบตามความเสี่ยงและความสำคัญที่ชัดเจน เช่น การเปลี่ยนแปลงมาตรฐานที่ได้รับอนุมัติเป็นการทั่วไป standard change การเปลี่ยนแปลงที่ต้องขออนุมัติตามกระบวนการปกติ normal change และการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน emergency change โดย อพวช. ควรกำหนดกระบวนการและขั้นตอนในการจัดการการเปลี่ยนแปลงตามแต่ละประเภทอย่างเหมาะสม

2.4.1.5 กรณีการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน ควรมีกระบวนการในการพิจารณาความเสี่ยง และผลกระทบ รวมถึงขออนุมัติจากผู้บริหารที่ได้รับมอบหมายให้สามารถตัดสินใจได้กรณีเร่งด่วน โดยภายหลังดำเนินการให้มีการรายงานผู้บริหารที่เกี่ยวข้องได้รับทราบโดยเร็ว

2.4.1.6 คำขอการเปลี่ยนแปลง (change request) ควรได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เพื่อให้มั่นใจได้ว่าการขอเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมจากหน่วยงานเจ้าของระบบ

2.4.1.7 มีระบบหรือทะเบียนในการจัดเก็บคำขอเปลี่ยนแปลงและเอกสารรายละเอียดที่เกี่ยวข้องเพื่อใช้ควบคุม การปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการ และสามารถใช้ในการติดตามและสอบทานการปฏิบัติงานได้

2.4.1.8 มีการจัดเก็บการเปลี่ยนแปลงของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ version control เช่น การนำระบบขึ้นใช้งานจริง การตั้งค่าระบบ การติดตั้งบนระบบที่ให้บริการจริง เป็นต้น เพื่อควบคุมความเสี่ยงในการเปลี่ยนแปลงและลดข้อผิดพลาดที่อาจเกิดขึ้น

2.4.1.9 มีการประเมินผลกระทบหรือทำการทดสอบบนระบบที่มีสภาพแวดล้อมใกล้เคียงกับระบบที่ให้บริการจริง ก่อนนำไปตั้งค่าบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

2.4.2 การบริหารจัดการการตั้งค่าระบบ (system configuration management)

วัตถุประสงค์ เพื่อให้ อพวช. มีกระบวนการควบคุมการเปลี่ยนแปลงการตั้งค่าระบบที่มีความรัดกุมปลอดภัย และเป็นไปตามมาตรฐาน

2.4.2.1 จัดทำเอกสาร minimum baseline standard เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ อย่างเป็นลายลักษณ์อักษร โดยมีการทบทวน ปรับปรุงเอกสารให้เป็นปัจจุบันอย่างสม่ำเสมอ

2.4.2.2 การเปลี่ยนแปลงการตั้งค่าบนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง ที่ อพวช. กำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.4.2.3 มีการจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบของทุกอุปกรณ์ ระบบและระบบงาน (system configuration version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.4.2.4 มีการสอบทานการตั้งค่าจากหน่วยงานที่มีหน้าที่ควบคุมดูแลความปลอดภัยหรือความเสี่ยงด้านเทคโนโลยีอย่างสม่ำเสมอ เพื่อให้สอดคล้องตามมาตรฐานของ อพวช.

2.4.2.5 กรณีมีความจำเป็นต้องตั้งค่าที่ไม่เป็นไปตามเอกสาร minimum baseline standard ควรผ่านกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

2.4.3 การบริหารจัดการ patch (patch management)

วัตถุประสงค์ เพื่อให้ อพวช. มีการบริหารจัดการ patch โดยมีการควบคุมที่รัดกุมปลอดภัย และติดตั้งได้อย่างเหมาะสมทันการณ์

2.4.3.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในกระบวนการบริหารจัดการ patch ที่ครอบคลุม การตรวจสอบความถูกต้องของ patch และการประเมินความเสี่ยงและความจาเป็นในการติดตั้ง patch ใหม่จากผู้ผลิตอย่างเหมาะสมทันการณ์

2.4.3.2 มีการจัดเก็บการเปลี่ยนแปลงการติดตั้งของทุกอุปกรณ์ ระบบและระบบงาน (patch version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.4.3.3 มีกระบวนการทดสอบ patch ที่ออกใหม่ทุกครั้งก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

2.4.3.4 การติดตั้ง patch บนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ อพวช. กำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.4.3.5 มีการทบทวนและปรับปรุงกระบวนการบริหารจัดการ patch อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่า อพวช. สามารถทดสอบและติดตั้ง patch ด้านการรักษาความปลอดภัย ได้ทันต่อสถานการณ์ที่เปลี่ยนไปและสามารถรองรับความเสี่ยงที่เพิ่มขึ้นได้อย่างรวดเร็ว

2.4.4 การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)

วัตถุประสงค์ เพื่อให้ อพวช. มีข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัย สามารถใช้ติดตาม ตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน รวมทั้งใช้เป็นหลักฐานการทางธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด

2.4.4.1 มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารที่สำคัญด้วย วิธีการที่ปลอดภัย โดยมีรายละเอียดที่ครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุ ตัวบุคคลผู้กระทำได้ และจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด

- บันทึกร่องรอยกิจกรรมการทำธุรกรรม (transaction log)
- บันทึกการเข้าถึง (access log)
- บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยต้องครอบคลุม
  - การเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูล และการเปลี่ยนแปลงแก้ไขข้อมูล (update/ insert/ delete) ในตารางที่สำคัญ
  - การเปลี่ยนแปลงการตั้งค่าความปลอดภัยของระบบ
  - การเข้าถึง object ที่สำคัญของระบบ

2.4.4.2 มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสาร

2.4.4.3 ข้อมูลการบันทึกเหตุการณ์ของอุปกรณ์สำคัญ ควรจัดเก็บไว้ที่เครื่องแม่ข่ายที่แยกเฉพาะ อย่างน้อยครอบคลุม access log และ activity log โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

2.4.4.4 มีการสอบทานบันทึกการเข้าถึง (access Log) และบันทึกการดำเนินงาน (activity log) ของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีสิทธิ์สูงอย่างสม่ำเสมอ เช่น system administrator หรือ system operator เป็นต้น เพื่อให้มั่นใจได้ว่าผู้ปฏิบัติงานเข้าถึงและปฏิบัติงานตามขอบเขตหน้าที่ที่ได้รับมอบหมาย

2.4.5 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

วัตถุประสงค์ เพื่อให้ อพวช. สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอรองรับ ต่อการดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

2.4.5.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติเรื่องการบริหารจัดการขีดความสามารถของระบบ เพื่อประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึง ระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ

2.4.5.2 มีการประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศเพื่อวางแผนรองรับการใช้งานในอนาคต (capacity planning) โดยครอบคลุมทั้งระบบหลักและระบบสำรอง

2.4.5.3 มีกระบวนการหรือเครื่องมือในการติดตามประสิทธิภาพและความเพียงพอของการใช้ทรัพยากร ด้านเทคโนโลยีสารสนเทศของระบบ เพื่อบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างทันท่วงที และสามารถตอบสนองความต้องการในการดำเนินงานของ อพวช.อย่างต่อเนื่อง

2.4.5.4 มีการกำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (threshold และ trigger) ในระดับต่าง ๆ เพื่อให้มีการแจ้งเตือนผู้เกี่ยวข้องอย่างทันท่วงที และสามารถวิเคราะห์ปัญหาและแนวทางการรับมือที่เหมาะสม รวมถึงการประสานงานกับหน่วยงานทั้งภายในและภายนอกกรณีเกิดเหตุขัดข้อง

2.4.5.5 จัดทำรายงานความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศนำเสนอต่อคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายในที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อม และความเพียงพอของระบบในการรองรับการให้บริการของ อพวช. ได้อย่างต่อเนื่อง รวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการณ์

2.4.6 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring)

วัตถุประสงค์ เพื่อให้ อพวช. สามารถตรวจจับป้องกันและรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงที โดยมีกระบวนการติดตามดูแลความมั่นคงปลอดภัยของระบบ รวมถึงเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง

2.4.6.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มี การติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง

2.4.6.2 กำหนดกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยของระบบ ที่สำคัญอย่างทันท่วงที ครอบคลุมระบบงานและระบบเครือข่ายสื่อสารทั้งในเชิง physical และ logical เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม

2.4.6.3 มีกระบวนการหรือเครื่องมือในการรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ มีการวิเคราะห์และจัดการข้อมูล ภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุม ลักษณะการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้น เพื่อนำมาใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์

2.4.6.4 กำหนดให้มีผู้รับผิดชอบในการประสานงานแลกเปลี่ยนข้อมูลภัยคุกคามระหว่าง อพวช. และหน่วยงาน ที่เกี่ยวข้อง รวมทั้งมีกระบวนการและช่องทางในการรายงาน แลกเปลี่ยน ติดตาม เพื่อป้องกันรับมือและแก้ไขภัยคุกคาม

2.4.6.5 ในกรณีที่พบภัยคุกคามที่ส่งผลกระทบอย่างมีนัยสำคัญ อพวช. ควรจัดให้มีการรายงานผู้บริหารหรือคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายใน รวมทั้งมีการรายงานหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมทั้งจัดให้มีกระบวนการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) โดยผู้ที่มีความเชี่ยวชาญ เพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่และป้องกันความเสี่ยงที่อาจเกิดขึ้นอีก

2.4.7 การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Test)

วัตถุประสงค์ เพื่อให้ อพวช. ได้รับทราบถึงช่องโหว่ด้านการรักษาความปลอดภัยของระบบ และสามารถดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้อย่างทันการณ์

2.4.7.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ

การบริหารจัดการช่องโหว่ (Vulnerability Management)

2.4.7.2 มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment) โดย อพวช. ควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ให้ครอบคลุมทุกระบบงานอย่างสม่ำเสมอตามระดับความเสี่ยง สำหรับระบบบงานสำคัญควรจัดทำอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.4.7.3 มีการรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไข และนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

การทดสอบเจาะระบบ (Penetration Test)

2.4.7.4 มีการทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่มีความอิสระครอบคลุมระบบงานและระบบเครือข่ายกับระบบที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) อย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.4.7.5 มีการรายงานผลการทดสอบเจาะระบบไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไข และนำเสนอความคืบหน้าการดำเนินการต่อคณะคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายในหรือผู้บริหารที่ได้รับมอบหมาย

2.4.7.6 มีกระบวนการรวบรวมและวิเคราะห์ช่องโหว่ทางด้านเทคนิคที่ตรวจพบ เพื่อกำหนดเป็นมาตรการรักษาความมั่นคงปลอดภัยของระบบงานที่จะมีการพัฒนาในอนาคต

2.4.8 การสำรองข้อมูล (Data Backup)

วัตถุประสงค์ เพื่อให้มั่นใจว่า อพวช. มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีระบบและข้อมูลหลัก เกิดเหตุขัดข้องหรือได้รับความเสียหายจนไม่สามารถใช้งานได้ตามปกติ

2.4.8.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการสำรองข้อมูล เพื่อให้มีข้อมูลสำรองพร้อมใช้และมีความปลอดภัย โดยควรครอบคลุมอย่างน้อย

- วิธีการ เทคโนโลยีและรอบระยะเวลาที่ใช้ในการสำรองข้อมูล โดยควรสอดคล้องกับเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) ที่กำหนด
- รอบระยะเวลาและวิธีการทดสอบความพร้อมใช้ของข้อมูลสำรอง

2.4.8.2 มีกระบวนการสำรองทั้งระบบ (full backup) ทุกครั้งภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ และระบบงาน เพื่อให้ระบบสำรองมีความเป็นปัจจุบัน

2.4.8.3 มีระบบหรือทะเบียนควบคุมการจัดเก็บและเรียกใช้งานสื่อบันทึกข้อมูลตามประเภทของสื่อที่จัดเก็บ โดยมีการระบุข้อมูล ชื่อ วันที่ และช่วงเวลาที่จัดเก็บ ที่สามารถติดตามตรวจสอบได้

2.4.8.4 มีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอก อพวช. ปฏิบัติงานหลัก โดยมีการรักษาสภาพแวดล้อมและการควบคุมความปลอดภัยในการเข้าถึงข้อมูลที่จัดเก็บไว้ เทียบเคียง กับศูนย์คอมพิวเตอร์หลัก

2.4.8.5 จัดให้มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งาน และปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติของ อพวช.

2.4.9 การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)

วัตถุประสงค์ เพื่อให้อุปกรณ์ที่ใช้ปฏิบัติงานมีความปลอดภัยและไม่เป็นช่องทางที่ทำให้ข้อมูลสำคัญ ของ อพวช. รั่วไหลหรือมีการเข้าใช้งานโดยไม่ได้รับอนุญาต

2.4.9.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงานเป็นลายลักษณ์อักษร ทั้งอุปกรณ์ของ อพวช. และอุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD) เช่น personal computer, notebook, tablet, smartphone, removable media เป็นต้น เพื่อให้ อพวช. มีแนวทางที่ใช้ในการควบคุมความเสี่ยงจากการใช้งานอุปกรณ์ดังกล่าว

2.4.9.2 กำหนด Security Baseline สำหรับอุปกรณ์ที่ใช้ปฏิบัติงานของ อพวช. เพื่อป้องกันความเสี่ยงที่อุปกรณ์เหล่านั้นอาจเป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญตามระดับความเสี่ยงที่เหมาะสม โดยอย่างน้อยครอบคลุม ดังนี้

- ติดตั้งระบบปฏิบัติการและโปรแกรมพื้นฐานที่ใช้ในการปฏิบัติงานบนเครื่องคอมพิวเตอร์ (personal computer, notebook) โดยมีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้ผู้ใช้งานสามารถติดตั้งโปรแกรมอื่น ๆ นอกเหนือจาก อพวช. กำหนด
- ติดตั้งโปรแกรมรักษาความปลอดภัย เช่น anti-Virus/ anti-malware, Host-based Intrusion Prevention System (HIPS)

เป็นต้น โดยมีการปรับปรุงประสิทธิภาพของการป้องกันโปรแกรมไม่ประสงค์ดี (malware) ให้เพียงพอและเป็นปัจจุบัน เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ๆ

- ควบคุมไม่ให้มีการจัดเก็บข้อมูลที่มีระดับชั้นความลับสูงสุดในเครื่องคอมพิวเตอร์ของผู้ใช้งาน แต่หาก มีความจำเป็นต้องจัดเก็บ ต้องมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ เช่น มีการเข้ารหัส เป็นต้น
- มีกระบวนการหรือเครื่องมือในการตรวจจับ (detect) คัดกรอง (filter) สกัดกั้น (block) เพื่อป้องกันข้อมูลสำคัญรั่วไหล (Data Leakage Prevention : DLP)
- จำกัดการเข้าถึง shared drive หรือ shared folder ตามความจำเป็นในการใช้งานเท่านั้น
- การควบคุมการใช้งานอินเตอร์เน็ต โดย อพวช. ควรมีเครื่องมือในการควบคุมให้อุปกรณ์ที่สามารถเชื่อมต่ออินเตอร์เน็ตเข้าถึงเฉพาะเว็บไซต์ที่ได้รับอนุญาตเท่านั้น รวมถึงมีการจำกัดการดาวน์โหลดหรืออัพโหลดข้อมูลจากอินเตอร์เน็ต
- การควบคุมการใช้สื่อบันทึกข้อมูลพกพา (removable media) เช่น กำหนดแนวทางการอนุญาต ให้ใช้งาน Universal Serial Bus (USB) หรือ external hard disk เป็นต้น
- การควบคุมการใช้ Email เช่น กำหนดแนวทางการใช้งาน Email เป็นต้น

2.4.9.3 มีกระบวนการบริหารจัดการอุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD) ตั้งแต่การลงทะเบียน การต่ออายุ และการยกเลิกการใช้งาน BYOD อย่างน้อยครอบคลุมดังนี้

- หลักเกณฑ์การอนุญาตให้ใช้งาน BYOD
- การควบคุมการใช้ BYOD ในการเข้าถึงระบบเครือข่ายสื่อสาร ระบบงานและข้อมูล ของ อพวช.
- มีกระบวนการตรวจสอบ วิเคราะห์ และติดตามความเสี่ยงของอุปกรณ์ที่นำมาใช้งานใน อพวช.
- กำหนดรหัสผ่านเพื่อใช้ในการล็อคหรือปลดล็อคในการเข้าถึงอุปกรณ์ส่วนตัว

- กรณีเครื่องคอมพิวเตอร์ (personal computer, notebook) ต้องติดตั้ง anti-virus/ anti-malware หรือโปรแกรมตามที่ อพวช. กำหนด
- ไม่อนุญาตให้อุปกรณ์โทรศัพท์เคลื่อนที่ (tablet, smartphone) ที่ถูกปรับแต่ง (rooted หรือ jailbroken) ลงทะเบียนใช้งาน BYOD
- ใช้วิธีการพิสูจน์ตัวตนอุปกรณ์ที่เชื่อถือได้ขององค์กร เช่น trusted root certification authorities, digital certificate เป็นต้น

2.5 การจัดหาและการพัฒนาระบบ (System Acquisition and Development)

วัตถุประสงค์ เพื่อให้มั่นใจได้ว่ากระบวนการจัดหาและการพัฒนาระบบ มีการควบคุมการรักษาความปลอดภัยอย่างรัดกุมและสอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล

2.5.1 การจัดหาระบบ (System Acquisition)

2.5.1.1 มีหลักเกณฑ์การพิจารณาคัดเลือกระบบและผู้ให้บริการ เพื่อใช้เป็นแนวทางในการปฏิบัติงาน ซึ่งควรครอบคลุมอย่างน้อย ดังนี้

- รายละเอียดทั่วไป เช่น หมายเลขอ้างอิงของซอฟต์แวร์ (software license) ฟังก์ชันการทำงาน ประสิทธิภาพของระบบ เป็นต้น
- ความมั่นคงปลอดภัยของระบบ
- ฐานะการเงิน ชื่อเสียง และความสามารถด้านเทคนิค
- การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับ การยอมรับโดยทั่วไป (certificate)
- การสนับสนุนและการบำรุงรักษาระบบ
- สัญญาและข้อตกลงการรับฝากทรัพย์สิน (escrow agreement) ตามระดับความสำคัญของระบบ
- ความน่าเชื่อถือของระบบและผู้ให้บริการ
- ผลการจัดทำ proof of concept ในกรณีที่เป็นระบบสำคัญ

2.5.1.2 อพวช. ควรควบคุมดูแลผู้ให้บริการปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติการออกแบบและพัฒนาระบบ

2.5.1.3 อพวช. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการตรวจสอบและส่งมอบระบบเทคโนโลยีสารสนเทศ

2.5.2 การพัฒนาระบบเทคโนโลยีสารสนเทศ (System Development)

2.5.2.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างเป็นลายลักษณ์อักษร โดยคำนึงถึงการรักษาความมั่นคงปลอดภัยครอบคลุมกระบวนการตั้งแต่จัดทำความต้องการ (requirement) การออกแบบ การพัฒนา และการทดสอบระบบก่อนใช้งานจริง

2.5.2.2 มีการสร้างความตระหนักและให้ความรู้กับผู้พัฒนาโปรแกรมอย่างสม่ำเสมอเพื่อเสริมสร้างทักษะ ในด้านการออกแบบและพัฒนาโปรแกรมอย่างปลอดภัย (secure software development)

2.5.2.3 กำหนดให้หน่วยงานธุรกิจที่เกี่ยวข้องสอบทานความถูกต้องครบถ้วนตามความต้องการของหน่วยงานธุรกิจ (business requirement) โดยครอบคลุมการรักษาความปลอดภัยตามนโยบายหรือมาตรฐานที่ อพวช. กำหนด (security requirement) และ sign off ก่อนเริ่มออกแบบระบบการออกแบบระบบ

2.5.2.4 จัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมการรักษา ความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่ อพวช. กำหนด (security specification) รวมทั้งจัดให้มี การสอบทานความถูกต้องครบถ้วนและ sign off จากผู้ที่เกี่ยวข้องก่อนเริ่มพัฒนาระบบ

2.5.2.5 จัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชันและเงื่อนไขต่าง ๆ ด้านประสิทธิภาพ ตามความต้องการของหน่วยงานที่เกี่ยวข้อง รวมถึงการควบคุมความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่ อพวช. กำหนด เพื่อเป็นแนวทางการพัฒนาระบบและสอบทานผลการทดสอบก่อนที่จะออกใช้งานจริง (exit criteria)

การพัฒนาระบบ

2.5.2.6 มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) การทดสอบ (testing) และระบบที่ให้บริการจริง (production) ออกจากกัน เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นจากการนำระบบขึ้นใช้งานจริง

2.5.2.7 มีการควบคุมเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้มีความปลอดภัยเพียงพอ ตามระดับความเสี่ยงเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2.5.2.8 มีกระบวนการหรือเครื่องมือในการควบคุมเวอร์ชันของคำสั่งในการเขียนโปรแกรม (source code version control)

2.5.2.9 มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (development tools) และเครื่องมือแปลโปรแกรม (compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรม โดยไม่ได้รับอนุญาต

การทดสอบระบบ

2.5.2.10 บทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบควรเป็นไปตามหลักการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงาน ได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ควรแยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น

2.5.2.11 มีการทดสอบบนสภาพแวดล้อมใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงของการเปลี่ยนแปลงบนระบบที่ให้บริการจริง

2.5.2.12 การทดสอบระบบที่ได้รับการพัฒนาหรือเปลี่ยนแปลง ควรครอบคลุม

- unit test
- system and integration test
- user acceptance test
- performance test
- security test ตาม security specification

ทั้งนี้ อพวช. ควรจัดให้มีกระบวนการและเอกสารการ sign off ผลการทดสอบระบบจากฝ่ายงานที่เกี่ยวข้อง ที่ผ่านตาม exit criteria อย่างครบถ้วน ก่อนนำระบบขึ้นใช้งานจริง

2.5.2.13 มีกระบวนการสอบทาน test scenario หรือ test case เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอ

2.5.2.14 การพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการ การทำธุรกรรมทางอิเล็กทรอนิกส์ หรือระบบที่มีการเชื่อมโยงกับระบบอื่นจำนวนมาก อพวช. ควรจัดให้มีการทดสอบประสิทธิภาพ (performance test) เพื่อให้มั่นใจได้ว่าระบบมีเสถียรภาพเพียงพอในการรองรับการใช้งานจำนวนมาก

2.5.2.15 มีการทดสอบระบบรักษาความปลอดภัยควรครอบคลุมการประเมินช่องโหว่ (vulnerability assessment) ของระบบงาน และกรณีเป็นระบบที่เชื่อมต่อกับภายนอก ควรมีการทำทดสอบเจาะระบบ (penetration test) เพื่อให้

สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขได้ก่อนเริ่มให้บริการจริง

2.5.2.16 มีการสอบทานคำสั่งในการเขียนโปรแกรม (source code review) อย่างเป็นอิสระ ทุกครั้งที่ อพวช. มีการพัฒนาหรือเปลี่ยนแปลงระบบในส่วนที่เป็นการทำธุรกรรมด้านการเงิน การจัดซื้อจัดจ้าง เป็นต้น เพื่อระบุช่องโหว่ด้านความมั่นคงปลอดภัย

2.5.2.17 มีแนวทางการควบคุมการรักษาความปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ เช่น data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูลสำคัญดังกล่าว

2.5.2.18 มีกระบวนการในการจัดการข้อผิดพลาดหรือข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ เพื่อพิจารณาแนวทางปรับปรุงหรือลดความเสี่ยงหรือผลกระทบของข้อผิดพลาดหรือข้อบกพร่อง ที่มีต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ

2.5.2.19 มีการจัดทำคู่มือและอบรมผู้ใช้งานระบบ เพื่อให้มีความเข้าใจฟังก์ชันการทำงานและมีการใช้งานระบบ อย่างปลอดภัย รวมถึงจัดให้มีคู่มือการดูแลระบบและอบรมผู้ดูแลระบบ เพื่อสามารถตรวจสอบและ จัดการแก้ไขปัญหาได้

2.5.2.20 หลังจากนำระบบขึ้นใช้งานจริง อพวช. ควรพิจารณาจัดให้มีการทดสอบจริงในวงจำกัด (pilot test) สำหรับฟังก์ชันการทำงานที่สำคัญ รวมทั้งจัดให้มีการติดตามการใช้งานระบบหลังจากให้บริการจริงอย่างใกล้ชิด ตามระยะเวลาที่เหมาะสม เพื่อให้มั่นใจต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ

การนำระบบขึ้นใช้งานจริง (system deployment)

2.5.2.21 การนำระบบขึ้นใช้งานจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ อพวช. กำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

2.5.2.22 มีการจัดเก็บการเปลี่ยนแปลง (version control) ของระบบงานขึ้นใช้งานจริงทั้งหมด โดยมีการรักษา ความปลอดภัยที่รัดกุมเพียงพอ

2.5.2.23 ระบบงานสำรองควรปรับปรุงให้มีความเป็นปัจจุบัน เพื่อให้มีความพร้อมใช้งานเมื่อเกิดเหตุฉุกเฉิน

2.6 การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management)

2.6.1 การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident Management)

วัตถุประสงค์ เพื่อให้ อพวช. มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์อย่างเหมาะสมทันการณ์ ให้สามารถจัดการแก้ไข ปัญหาให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจของ อพวช.

2.6.1.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมตั้งแต่กระบวนการหรือเครื่องมือในการบันทึกเหตุการณ์ผิดปกติ การกำหนดประเภท การจัดระดับความรุนแรง การวิเคราะห์หาสาเหตุ การดำเนินการแก้ไข การติดตามแก้ไข การรายงานเหตุการณ์ผิดปกติ

2.6.1.2 กำหนดหลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติ (escalation) และรายงานความคืบหน้าเหตุการณ์ผิดปกติ ให้ผู้เกี่ยวข้อง ผู้บริหารระดับสูง คณะกรรมการที่เกี่ยวข้องได้รับทราบ ให้สอดคล้องกับระดับความรุนแรงของเหตุการณ์ผิดปกติ

2.6.1.3 การจัดระดับความรุนแรงของปัญหา ควรพิจารณาอย่างน้อยให้ครอบคลุมผลกระทบต่อการให้บริการ ผลกระทบต่อผู้ใช้งาน โดยกรอบระยะเวลาในการแก้ไขเหตุการณ์ผิดปกติควรคำนึงถึงเป้าหมายระยะเวลา ในการกู้คืนระบบ (Recovery Time Objective: RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption: MTPD) เพื่อที่จะสามารถตัดสินใจใช้ แผนสำรองอย่างเหมาะสมทันการณ์

2.6.1.4 จัดให้มีศูนย์รับแจ้งเหตุการณ์ผิดปกติ โดยทำหน้าที่ในการบันทึกและแก้ไขในเบื้องต้น หรือส่งต่อเหตุการณ์ผิดปกติ ไปยังหน่วยงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

2.6.1.5 จัดทำแผนการรับมือกับเหตุการณ์ผิดปกติ (incident response plan) ตามความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์ โดยอย่างน้อยแผนควร ระบุกระบวนการรับมือและช่องทางประสานงานจากผู้เชี่ยวชาญทั้งภายใน

และภายนอก และมีแนวทาง การตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบ

2.6.1.6 จัดทำรายงานเหตุการณ์ผิดปกติ เสนอต่อคณะอนุกรรมการความเสี่ยงและควบคุมภายใน และผู้บริหารระดับสูงที่ได้รับมอบหมาย โดยครอบคลุม วัน เวลา เหตุการณ์ ความเสียหาย การวิเคราะห์สาเหตุที่แท้จริง การวิเคราะห์ผลกระทบ การแก้ไขปัญหาและแนวทางหรือแผนดำเนินการเพื่อป้องกันเหตุการณ์ผิดปกติในอนาคต และในกรณีที่เป็นความเสียหายส่งผลกระทบต่อชื่อเสียงและการดำเนินธุรกิจของ อพวช. อย่างมีนัยสำคัญให้รายงานต่อคณะกรรมการของ อพวช. ทราบด้วย

2.6.1.7 ในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียงของสถาบันการเงิน รวมถึงกรณีเทคโนโลยีสารสนเทศที่สำคัญของ อพวช. ถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่สถาบันการเงินต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดของ อพวช. ทราบ โดยให้ อพวช. รายงานปัญหาหรือเหตุการณ์ดังกล่าวมายังฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ อพวช.ทันทีเมื่อเกิดหรือรับรู้ปัญหาหรือเหตุการณ์นั้น โดยจะแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

2.6.1.8 มีกระบวนการบริหารภาวะวิกฤต (crisis management) เพื่อรองรับกรณีเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศเพิ่มระดับความรุนแรงหรือมีความยืดเยื้อ

- อพวช. จัดให้มีคณะกรรมการบริหารภาวะวิกฤติ (crisis management committee) โดยประกอบด้วยผู้บริหารระดับสูง (C-level) จากฝ่ายงานต่าง ๆ เพื่อให้สามารถพิจารณาประเมินสถานการณ์ได้ อย่างครอบคลุม และตัดสินใจแก้ไขสถานการณ์ได้อย่างรวดเร็วทันการณ์ บรรเทาผลกระทบหรือ ความเสียหายและสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ตลอดจนการกำกับดูแลการดำเนินการต่าง ๆ จนสถานการณ์กลับสู่ภาวะปกติ
- จัดตั้งศูนย์บัญชาการ กาหนดขั้นตอนการสั่งการและการตัดสินใจที่ชัดเจน
- กำหนดทีมงานรับผิดชอบดำเนินการด้านต่าง ๆ ได้แก่ ด้านสถานที่ ด้านบุคลากร ด้านเทคโนโลยีสารสนเทศ ด้านความปลอดภัย ด้าน

สื่อสารองค์กร เป็นต้น ในการประเมินลักษณะและผลกระทบ ของความเสียหายที่เกิดขึ้น พิจารณาแนวทางบรรเทาผลกระทบและแนวทางรองรับธุรกิจอย่างต่อเนื่อง ซึ่งครอบคลุมการกู้คืนระบบ เพื่อนำเสนอต่อคณะกรรมการบริหารภาวะวิกฤต ในการพิจารณาตัดสินใจดำเนินการใช้แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP)

2.6.2 การบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ (IT Problem Management)

วัตถุประสงค์ เพื่อให้ อพวช. มีกระบวนการติดตามหาสาเหตุที่แท้จริง ให้มีแนวทางป้องกันไม่ให้เกิด เหตุการณ์ผิดปกติซ้ำในอนาคต

2.6.2.1 มีมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ เพื่อให้มีการนำเหตุการณ์ผิดปกติที่ยังไม่ทราบสาเหตุที่แท้จริง (unknown root cause) เหตุการณ์ผิดปกติที่เกิดขึ้นซ้ำ (repeated incident) มาวิเคราะห์และพิจารณาแนวทางแก้ไขปัญหาจากสาเหตุที่แท้จริง (root cause)

2.6.2.2 มีกระบวนการหรือเครื่องมือในการบันทึกปัญหา หลักเกณฑ์ในการจัดประเภทปัญหา การจัดลำดับความสำคัญ วิเคราะห์ และจัดให้มีการติดตามการแก้ไขปัญหาเพื่อให้ปัญหาได้รับการแก้ไข

2.6.2.3 มีกระบวนการหรือเครื่องมือบันทึกปัญหาที่เคยเกิดขึ้น เพื่อให้เป็นแหล่งข้อมูลความรู้ให้สามารถสืบค้นเหตุการณ์ปัญหาและแนวทางการแก้ไขปัญหาได้ในภายหลังอย่างรวดเร็วและมีประสิทธิภาพ

2.7 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์ เพื่อให้ อพวช. มีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเกิดหยุดชะงักหรือเกิดความเสียหาย โดยที่ธุรกิจดำเนินการต่อไปได้อย่างต่อเนื่องและสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้

นโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

2.7.1 กำหนดนโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยคำนึงความสอดคล้องกับนโยบาย การบริหารความต่อเนื่องของธุรกิจและนโยบายการบริหารความเสี่ยงของ อพวช.

2.7.2 นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการของ อพวช. และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนฯ

เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบาย การบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการดาเนินธุรกิจหรือทรัพยากรหรือโครงสร้างระบบ IT เป็นต้น

2.7.3 นโยบายการจัดทาแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมอย่างน้อย

- บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการ ผู้บริหารระดับสูง และผู้เกี่ยวข้อง
- การประเมินความเสี่ยง
- การวิเคราะห์ผลกระทบทางธุรกิจและกาหนดเป้าหมายในการกู้คืนระบบเทคโนโลยีสารสนเทศ
- การจัดระดับความสำคัญของระบบงาน
- การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

2.7.4 มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยต้องได้รับการอนุมัติจากคณะกรรมการของ อพวช. โดยจัดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.7.5 จัดให้มีคณะทางานหรือหน่วยงานที่รับผิดชอบในการจัดทาแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศไว้ อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น

2.7.6 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ เหตุการณ์ความเสียหายต่าง ๆ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจของ อพวช. เช่น ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการเงิน ความเสี่ยงด้านการดำเนินการ และความเสี่ยงด้านกฎหมายและข้อกำหนดผูกพันธ์องค์กร

2.7.7 กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมการดำเนินการ ดังนี้

(1) การประเมินความเสี่ยง (risk analysis) เพื่อให้ อพวช. สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการอย่างเหมาะสมเพียงพอดังนี้

- ระบุเหตุการณ์ความเสี่ยง (risk scenarios) ที่อาจทำให้กระบวนการและระบบเทคโนโลยีสารสนเทศหยุดชะงัก ทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ เป็นต้น
- ประเมินความเสี่ยงโดยพิจารณาการควบคุมที่มีอยู่ รวมถึงผลกระทบและโอกาสที่จะเกิดขึ้น พร้อมทั้งกำหนดกระบวนการและทรัพยากรที่จะใช้ในการควบคุมความเสี่ยง
- จัดทำแผนในการจัดการความเสี่ยง เพื่อปรับปรุงกระบวนการและจัดเตรียมทรัพยากรที่จำเป็น ในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

(2) การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) เพื่อให้ทราบถึงความสำคัญของระบบเทคโนโลยีสารสนเทศที่มีผลต่อการดำเนินธุรกิจของ อพวช. รวมถึงผลกระทบจากการหยุดชะงักและความเชื่อมโยงของการให้บริการกับระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการดังนี้

- ระบุระบบเทคโนโลยีสารสนเทศทั้งหมดของ อพวช. และทรัพยากรที่มีการเชื่อมโยงพึ่งพาระหว่างกัน (dependency)
- วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของเทคโนโลยีสารสนเทศ โดยคำนึงถึงเป้าหมายระยะเวลาสูงสุดที่ยอมให้การให้บริการหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD)
- กำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO)

(3) การจัดลำดับความสำคัญของระบบงาน โดยคำนึงถึงทรัพยากร ระยะเวลาในการกู้คืนระบบ เป้าหมายของระบบงานและข้อมูลที่ควรกู้ได้ภายหลังเกิดการหยุดชะงัก และทรัพยากรทางเทคโนโลยีสารสนเทศขั้นต่ำที่จำเป็นต้องใช้ในการกู้คืนระบบ ทั้งนี้ อพวช. ควรพิจารณาให้ระบบการชำระเงินหรือระบบที่มีผลกระทบกับระบบ อพวช. เป็นวงกว้างเป็นระบบที่มีความสำคัญสูงสุด

(4) การกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ อพวช. ต้องมีการกำหนดกลยุทธ์แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและแนวทางจัดเตรียม

ทรัพยากรระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามการจัดลำดับความสำคัญของระบบงาน โดยพิจารณาอย่างน้อยครอบคลุม

- เป้าหมายระยะเวลาที่ได้จากการวิเคราะห์ผลกระทบการให้บริการ
- ปัจจัยสำคัญที่สนับสนุนให้แผนเป็นไปตามกลยุทธ์ เช่น เทคโนโลยีในการสำรองและกู้คืนข้อมูล ความพร้อมใช้ของสถานที่ปฏิบัติงานสำรอง เป็นต้น เพื่อให้ อพวช. มีทิศทางในการพัฒนาแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่บรรลุเป้าหมายที่กำหนดไว้
- ทรัพยากรและงบประมาณ เพื่อจัดเตรียมระบบเทคโนโลยีสารสนเทศให้สอดคล้องตามแผนกลยุทธ์และกิจกรรมที่ต้องดำเนินการทั้งหมด

(5) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรมีการระบุกระบวนการและขั้นตอนสนับสนุนการปฏิบัติที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ รวมทั้งมีความยืดหยุ่นในการตอบสนองต่อเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น อย่างน้อยครอบคลุม

- ชื่อแผน วัตถุประสงค์ ขอบเขต และความสัมพันธ์กับแผนอื่น ๆ ที่เกี่ยวข้อง
- ผังโครงสร้างของการบังคับบัญชาในการดำเนินงานตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบ และผู้ปฏิบัติที่ทำหน้าที่แทนในกรณีที่ผู้ปฏิบัติหน้าที่ไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึก การเปลี่ยนแปลงของแผน
- รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม แผนภาพระบบเครือข่ายสื่อสาร เป็นต้น
- ขั้นตอนในการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ การตอบสนองต่อเหตุการณ์ฉุกเฉินและแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบ
- ขั้นตอนในการดำเนินการกู้คืนระบบ โดยควรระบุรายละเอียดอย่างชัดเจนและเพียงพอ เพื่อให้สามารถใช้เป็น checklist ควบคุมไม่ให้มีการข้ามหรือละเลยขั้นตอนที่กำหนดไว้ ทั้งนี้ อพวช. ควรจัดทำเอกสารหรือคู่มือประกอบการกู้คืนในแต่ละระบบ ในกรณีที่มีการปรับปรุง หรือเพิ่มเติมขั้นตอนนอกเหนือจากที่ระบุในแผนขณะปฏิบัติงานจริง อพวช.

ควรมีกระบวนการรายงานและขออนุมัติจากผู้บริหารตามที่กำหนดในโครงสร้างการบังคับบัญชา พร้อมทั้งนำขั้นตอนดังกล่าวมาปรับปรุงแผนให้เป็นปัจจุบัน

- ขั้นตอนในการกลับคืนสู่ภาวะปกติ (return to normal) และการประกาศยกเลิกแผนฉุกเฉิน ด้านเทคโนโลยีสารสนเทศ
- แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ พร้อมเอกสารประกอบการทำงานภายใต้แผนฉุกเฉิน ด้านเทคโนโลยีสารสนเทศ ควรจัดเก็บไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้ในสถานที่ปฏิบัติงานหลักและสำรอง

(6) การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ อพวช. ต้องจัดให้มีการสื่อสารแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และจัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้อง

- ในการสื่อสารแผนฯ ต้องมีการระบุแนวทางสื่อสารที่ชัดเจนให้บุคลากรทุกคนที่มีส่วนเกี่ยวข้องได้รับทราบถึงรายละเอียดในการจัดทาแผน ขั้นตอนการดำเนินงานตามแผน
- จัดให้มีการฝึกอบรมแก่บุคลากรผู้มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยควรครอบคลุม วัตถุประสงค์ของแผน ขั้นตอนการปฏิบัติงานตามแผน การประสานงานและการสื่อสารกันระหว่างกลุ่ม ขั้นตอนในการรายงาน ระบบรักษาความปลอดภัย กระบวนการเฉพาะของแต่ละกลุ่มดำเนินงาน และความรับผิดชอบของแต่ละบุคคล เป็นต้น

(7) การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

- จัดให้มีแผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปี โดยมีรายละเอียด อย่างน้อยครอบคลุมสถานการณ์จำลอง รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้อง ทั้งนี้แผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปีในภาพรวมควรได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย
- จัดให้มีการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศทั้งในระดับหน่วยงานและระดับองค์กร อย่างน้อยปีละ 1 ครั้ง โดยเฉพาะระบบงาน

หรือข้อมูลที่มีผลกระทบต่อการให้บริการลูกค้าหรือ ต่อ อพวช. ทั้งระบบ

- กรณีระบบงานมีการเชื่อมโยงเครือข่ายสื่อสารหรือใช้บริการจากหน่วยงานภายนอก อพวช. ควรมี การทดสอบแผนฉุกเฉินร่วมกับหน่วยงานภายนอกที่เกี่ยวข้องด้วย เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศของ อพวช. มีความพร้อมใช้งานร่วมกับระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก
- มีการรายงานผลการทดสอบต่อคณะกรรมการของ อพวช. โดยมีรายละเอียดอย่างน้อยครอบคลุม วัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ระยะเวลาที่ใช้ในการกู้คืนระบบเทียบกับเป้าหมายที่กำหนด ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข
- อพวช. ควรจัดให้มีการทบทวนและปรับปรุงแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อย ปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงบุคลากร ที่มีหน้าที่รับผิดชอบในการดำเนินงานตามแผน การเปลี่ยนสภาพแวดล้อมของระบบเทคโนโลยีสารสนเทศ เป็นต้น เพื่อให้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเป็นปัจจุบัน
- อพวช. อาจจัดให้มีการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศโดยหน่วยงานภายนอกหรือภายในที่มีความเป็นอิสระ เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผนให้สามารถใช้งานได้จริง

2.8 การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

วัตถุประสงค์ เพื่อให้ อพวช. มีแนวทางการบริหารจัดการผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจที่มี การเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของ อพวช. หรือสามารถเข้าถึงข้อมูลสำคัญหรือลูกค้าของ อพวช.

2.8.1 กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการผู้ให้บริการภายนอก เพื่อควบคุมให้มีการรักษาความมั่นคงปลอดภัยทรัพย์สินของ อพวช. โดยอย่างน้อยครอบคลุม

- ก่อนใช้บริการ อพวช. ดำเนินการระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลหรือระบบเทคโนโลยีสารสนเทศที่ผู้ให้บริการภายนอกสามารถเข้าถึง โดยอย่างน้อยควรพิจารณา ขอบเขต เหตุผลและความจำเป็นในการเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศ ข้อจำกัดหรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ
- ข้อกำหนดในการรักษาความมั่นคงปลอดภัยของหน่วยงานภายนอก รวมถึง sub-contract ต้องปฏิบัติ โดยควรสอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยที่ อพวช. กำหนด
- ข้อตกลงการไม่เปิดเผยข้อมูล (non disclosure agreement)
- สัญญาการให้บริการและเงื่อนไขระหว่าง อพวช. และผู้ให้บริการภายนอก สอดคล้องตามนโยบาย การรักษาความมั่นคงปลอดภัยที่ อพวช. กำหนด เช่น ความรับผิดชอบต่อการรั่วไหลของข้อมูลอันเนื่องมาจากการนำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงในการให้บริการ เป็นต้น
- มีกระบวนการติดตาม ประเมิน ทบทวน และรายงานผลการปฏิบัติงานของหน่วยงานภายนอก

2.8.2 ในกรณีที่ อพวช. ใช้บริการเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing) ให้ อพวช. ปฏิบัติตามข้อกำหนดว่าด้วยเรื่องการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT outsourcing)

3. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management)

วัตถุประสงค์ เพื่อให้ อพวช. มีการบริหารจัดการความเสี่ยงของการดำเนินโครงการด้านเทคโนโลยีสารสนเทศ อย่างมีประสิทธิภาพและไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนกลยุทธ์ทางธุรกิจ

3.1 กำหนดกรอบการบริหารจัดการโครงการ (project management framework) ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางดำเนินโครงการจัดหาหรือพัฒนาระบบเทคโนโลยีสารสนเทศ โดยควรครอบคลุมดังนี้

3.1.1 โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจนเพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด

- คณะกรรมการกำกับดูแลโครงการ มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแล ให้โครงการสำเร็จเป็นไปตามเป้าหมายที่กำหนด มีการติดตามความคืบหน้า ปัญหาและ อุปสรรคของโครงการ เพื่อให้คำแนะนำและพิจารณาตัดสินใจการดำเนินงานที่สำคัญ โดยควรประกอบด้วยผู้บริหารจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง และเจ้าของโครงการหรือผู้สนับสนุนโครงการ (project owner/ project sponsor) มีส่วนร่วมในการตัดสินใจ รวมทั้งคณะกรรมการกำกับดูแลโครงการควรมีการประชุมอย่างสม่ำเสมอ เพื่อควบคุมดูแลโครงการที่สำคัญให้เป็นไปตามแผนงานที่กำหนด
- หน่วยงานหรือทีมงานดูแลภาพรวมโครงการ (project management office) มีบทบาทหน้าที่และความรับผิดชอบในการกำหนดรูปแบบ กระบวนการและเครื่องมือ ที่เป็นมาตรฐานในการบริหารจัดการและติดตามโครงการ รวมทั้งติดตาม รายงานภาพรวมโครงการสำคัญของ อพวช. ให้กับคณะกรรมการของ อพวช. และผู้บริหารระดับสูงที่เกี่ยวข้องได้รับทราบ เพื่อติดตามและสนับสนุนให้บริหารจัดการโครงการสำเร็จลุล่วงสอดคล้องกับเป้าหมาย ในระดับกลยุทธ์ของ อพวช. ตามแผนงานที่กำหนด
- ผู้จัดการโครงการ (project manager) มีบทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการโครงการ ครอบคลุม กำหนดแผนงานโครงการ วิเคราะห์ผลกระทบ และจัดให้มีแนวทางรองรับหรือแผนสำรองกรณีโครงการประสบปัญหาหรือล่าช้า รวมทั้งรายงานให้คณะกรรมการกำกับดูแลโครงการพิจารณาตัดสินใจแก้ไขปัญหาได้ทันการณ์ เพื่อให้โครงการสามารถส่งมอบ ได้อย่างถูกต้องครบถ้วนสำเร็จตามแผนงานที่กำหนด โดยผู้จัดการโครงการ ต้องมีความรู้ความสามารถและประสบการณ์ในการบริหารโครงการที่เพียงพอ

3.1.2 แนวทางการบริหารจัดการโครงการ ควรกำหนดครอบคลุมอย่างน้อย ดังนี้

- ระเบียบขั้นตอนการบริหารจัดการโครงการ ครอบคลุมตั้งแต่ ก่อนเริ่มโครงการ การดำเนินการและควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ
- ปัจจัยและเกณฑ์ในการประเมินหรือจัดระดับความสำคัญของโครงการที่ชัดเจน รวมถึงขอบเขตอำนาจหน้าที่ในการอนุมัติและกำกับดูแลโครงการตามระดับความสำคัญของโครงการ

- รูปแบบของเอกสารหรือผลลัพธ์ที่เป็นมาตรฐาน ที่ต้องส่งมอบในแต่ละขั้นตอนอย่างชัดเจน เช่น แผนการดำเนินโครงการ รายงานความคืบหน้า รายงานการปิดโครงการ เป็นต้น

การเริ่มโครงการ

3.2 มีการประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งเลือกใช้เทคโนโลยีที่เหมาะสม ทั้งนี้โครงการต้องมีเป้าหมายที่ชัดเจน (project objective) สอดคล้องกับกลยุทธ์ขององค์กร และคานึงถึงการรักษาความมั่นคงปลอดภัย

3.3 มีแผนการดำเนินโครงการ ที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการอย่างน้อยครอบคลุม

- เป้าหมายโครงการ
- ทรัพยากร (resources) ที่ใช้
- บทบาทหน้าที่ ความรับผิดชอบของทีมงานในการดำเนินโครงการ โดยทีมงานจะต้องมีประสิทธิภาพ และมีความรู้ความเชี่ยวชาญเพียงพอในการดำเนินโครงการ
- ขอบเขตและระยะเวลาของการดำเนินโครงการในแต่ละขั้นตอน
- ผลงานที่จะส่งมอบในแต่ละขั้นตอน
- ข้อกำหนดเงื่อนไขที่เกี่ยวข้องกับโครงการ เช่น ข้อกำหนดของผู้ว่าจ้าง ภาระผูกพัน ข้อจำกัด เป็นต้น

3.4 มีการนำเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อคณะกรรมการของ อพวช. คณะกรรมการ ที่ได้รับมอบหมาย หรือผู้บริหารระดับสูง ตามขอบเขตในการอนุมัติที่กำหนดไว้การดำเนินการและแผนงานโครงการที่เกี่ยวข้อง

3.5 มีการบันทึกและจัดเก็บข้อมูลโครงการของแต่ละโครงการอย่างเพียงพอเพื่อใช้ติดตามดูแลและสามารถตรวจสอบย้อนหลังได้

3.6 มีการประเมินและติดตามการดำเนินโครงการอย่างต่อเนื่องและครอบคลุมขอบเขต ระยะเวลา และทรัพยากรที่วางแผนไว้ ในกรณีที่มีการเปลี่ยนแปลงขอบเขต ระยะเวลาและหรือทรัพยากร หรือยกเลิกโครงการ ควรมีการนำเสนอเพื่อขออนุมัติการเปลี่ยนแปลงหรือยกเลิกแผนงานโครงการที่เกี่ยวข้อง

3.7 มีการรายงานความคืบหน้า ปัญหา อุปสรรคและข้อจำกัดในการดำเนินแผนงานโครงการที่เกี่ยวข้อง ต่อคณะกรรมการกำกับดูแลโครงการหรือผู้บริหารที่ได้รับมอบหมายอย่างเป็นประจำ เพื่อสามารถให้คำแนะนำและแนวทางในการแก้ไขปัญหาที่จะลดความเสี่ยงที่อาจ

เกิดขึ้นอย่างทันท่วงที โดยโครงการที่ส่งผลกระทบต่อธุรกิจของ อพวช. อย่างมีนัยสำคัญควรนำเสนอแก่คณะกรรมการของ อพวช. ด้วย

การปิดโครงการ

3.8 มีการสรุปประโยชน์ที่ได้รับจากโครงการเทียบกับเป้าหมายที่กำหนด

3.9 มีการรวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นสิ่งที่ได้เรียนรู้ (lesson learned) ใช้สำหรับวิเคราะห์ ปรับปรุง และพัฒนากระบวนการหรือเครื่องมือในการบริหารจัดการโครงการต่อไปให้มีประสิทธิภาพมากขึ้น

การสอบทานโครงการ

3.10 มีการสอบทานโครงการที่สำคัญ โดยหน่วยงานอิสระ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของโครงการ นโยบาย มาตรฐาน ระเบียบและวิธีปฏิบัติของ อพวช. รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

4. การกำหนดการวัดติดตามและประเมินผล

1. วัตถุประสงค์

1. เพื่อวัดระดับความรับรู้ของบุคลากรเกี่ยวกับแนวปฏิบัติด้านการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ
2. เพื่อสร้างความเข้าใจและความตระหนักรู้ในเรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศในองค์กร
3. เพื่อประเมินผลของกิจกรรมและมาตรการที่ใช้ในการลดความเสี่ยงและป้องกันภัยคุกคามทางไซเบอร์

2. ผู้รับผิดชอบ

1) กองเทคโนโลยีดิจิทัล

3. ตัวชี้วัด : บุคลากร อพ. รับรู้แนวปฏิบัติ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ไม่ต่ำกว่าร้อยละ 50 ของ จำนวนบุคลากร อพวช. ทั้งหมด

4. วิธีการวัดผล

4.1 การอบรมและทดสอบความเข้าใจ

1) จัดอบรมให้กับบุคลากรในหัวข้อเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2) ทำแบบทดสอบความรู้หลังการอบรม โดยบุคลากรที่ได้คะแนนไม่น้อยกว่า 50% ถือว่าผ่าน

4.2 เกณฑ์แบบสำรวจความเข้าใจ

1) จัดทำแบบสำรวจเกี่ยวกับแนวปฏิบัติด้านการบริหารความเสี่ยง
2) หากบุคลากรตอบคำถามได้ถูกต้องมากกว่าร้อยละ 50 ถือว่ามีความรับรู้แนวปฏิบัติ

5. การประเมินผลการวัด ติดตาม

หมวดหมู่	**จำนวนบุคลากรที่เข้าร่วม**	**ร้อยละของบุคลากรทั้งหมดที่ผ่านการทดสอบ**
อบรมและผ่านการทดสอบแบบประเมิน	[จำนวนบุคลากร อพ. ทั้งหมดที่ลงทะเบียนเข้าอบรม]	[ระบุร้อยละ 60]
ทำแบบทดสอบความรู้หลังผ่านการอบรมและติดตาม เพื่อวัดระดับความรู้	[บุคลากร อพ. ที่ผ่านการอบรม]	[ระบุร้อยละ 60]
สรุปรวม	[จำนวนบุคลากรทั้งหมดที่เข้าร่วมทั้ง 2 กิจกรรม]	[ระบุร้อยละ 50]

6. แผนการวิเคราะห์ผลและข้อเสนอแนะ

6.1 [ตัวอย่าง วิเคราะห์ผลการวัด: เช่น หากบุคลากรผ่านตัวชี้วัดน้อยกว่า 50% ควรมีมาตรการเพิ่มเติม]

6.2 [ตัวอย่าง ข้อเสนอแนะเพื่อปรับปรุง เช่น การเพิ่มกิจกรรมอบรม การใช้มาตรการจูงใจ]

7. แผนการสรุปผลและแนวทางปรับปรุงในอนาคต

จากผลการวัดพบว่า [ตัวอย่าง สรุปผลการวัด] ซึ่ง [ผ่าน/ไม่ผ่าน] ตามเกณฑ์ที่กำหนด เพื่อให้บรรลุเป้าหมายในอนาคต อพวช. ควรดำเนินการดังนี้:

7.1 ปรับปรุงเนื้อหาและรูปแบบการอบรมให้เข้าใจง่ายและน่าสนใจ

1) เพิ่มกิจกรรมที่ส่งเสริมให้บุคลากรเข้าร่วมมากขึ้น

2) ใช้เทคโนโลยี เช่น e-Learning หรือแคมเปญสร้างความตระหนักรู้เกี่ยวกับความเสี่ยง

5. เอกสารอ้างอิง

- Control Objectives for Information and related Technology 5 for Risk (COBIT 5 for risk) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ISO 27001:2013 Information technology - Security techniques – Information Security Management Systems – Requirement มาตรฐานด้านการจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ISO 27005:2011 Information technology - Security techniques – Information Security Risk Management หลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ISO 31000:2009 Risk Management – Principles and Guideline มาตรฐานการบริหารความเสี่ยง
- ISO 21500:2012 Guidance on Project Management การบริหารจัดการโครงการ

Information Security Risk

National Science Museum Thailand

องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ
กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
39 หมู่ 9 ต.คลองห้า อ.คลองหลวง จ.ปทุมธานี
www.nsm.or.th