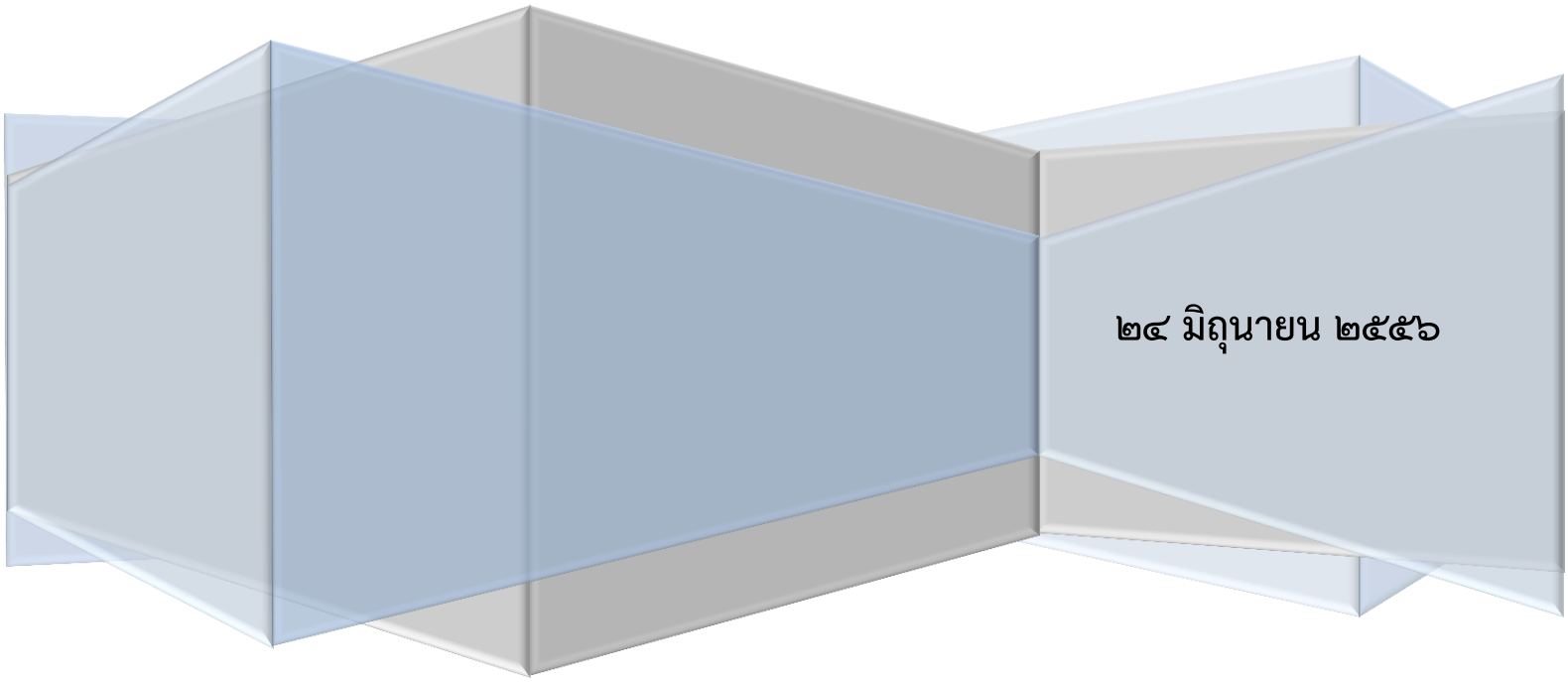
สำนักงานบริหารหนี้สาธารณะ
PUBLIC DEBT MANAGEMENT OFFICE

แผนบริหารความต่อเนื่อง
สำนักงานบริหารหนี้สาธารณะ

Business Continuity Plan : BCP



๒๔ มิถุนายน ๒๕๕๖

สารบัญ

บทที่ ๑
บทนำ

๑.๑ เหตุผลและความจำเป็น

จากการที่ประเทศไทยได้เผชิญกับสถานการณ์อุทกภัยรุนแรง ในปี พ.ศ. ๒๕๕๔ ที่ผ่านมา ปรากฏว่า ระบบและกลไกของรัฐหลายประการมีปัญหาโดยไม่สามารถดำเนินการในสภาวะวิกฤตได้อย่างมีประสิทธิภาพ ส่งผลให้การแก้ไขปัญหาของประชาชนขาดระบบการบริหารจัดการที่ดี ดังนั้น สำนักงาน ก.พ.ร. จึงได้เสนอแนวทางการดำเนินการเตรียมความพร้อมต่อสภาวะวิกฤต และมาตรการที่เกี่ยวข้องต่อคณะรัฐมนตรี และคณะรัฐมนตรีได้มีมติเห็นชอบกรอบแนวตามที่สำนักงาน ก.พ.ร. เสนอ เมื่อวันที่ ๒๔ เมษายน ๒๕๕๕ ซึ่งกำหนดให้ทุกส่วนราชการทั้งระดับกรม จังหวัด สถาบันอุดมศึกษา องค์กรปกครองส่วนท้องถิ่น องค์กรมหาชน และรัฐวิสาหกิจ ดำเนินการเพื่อสร้างความพร้อมให้แก่หน่วยงานเมื่ออยู่ในสภาวะวิกฤต ประกอบด้วย ๔ ขั้นตอน คือ ๑) การสร้างความรู้ความเข้าใจให้กับส่วนราชการ ๒) เตรียมความพร้อมของส่วนราชการ ๓) ซักซ้อมแผนและนำไปปฏิบัติจริง และ ๔) ส่งเสริมให้มีการบริหารจัดการอย่างยั่งยืน ทั้งนี้ เพื่อให้ระบบบริหารจัดการของหน่วยงานของรัฐสามารถตอบสนองต่อปัญหาและแก้ไขความไม่มีประสิทธิภาพของกลไกของรัฐในการให้บริการประชาชนได้อย่างต่อเนื่องไม่สะดุดหยุดลงเมื่อเกิดสถานการณ์วิกฤต ซึ่งเป็นไปตามพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. ๒๕๔๖

สำนักงานบริหารหนี้สาธารณะ (สบน.) ได้ศึกษาแนวทางการเตรียมความพร้อมของหน่วยงานต่อสภาวะวิกฤต และวิเคราะห์ความสำคัญของกระบวนงานในภารกิจหลักและภารกิจสนับสนุน รวมทั้ง วิเคราะห์ความเสี่ยงที่อาจจะเกิดขึ้น อันจะส่งผลกระทบต่อการปฏิบัติงานตามพันธกิจหลักขององค์กร โดยใช้หลักเกณฑ์ในการวิเคราะห์ตามแนวทางการบริหารความเสี่ยง ซึ่งเป็นการประเมินความเสี่ยง (Risk Assessment) ของภารกิจขององค์กร โดยวิเคราะห์จากโครงสร้างและลักษณะงานของแต่ละหน่วยงาน รวมทั้ง พิจารณาโอกาสและผลกระทบของเหตุการณ์ พร้อมทั้งความเร่งด่วนของกิจกรรมต่างๆ ที่อาจจะส่งผลกระทบต่อการดำเนินงานของ สบน. โดยผลการประเมินความเสี่ยงปรากฏว่า กระบวนงานในภารกิจหลักที่จะต้องดำเนินการอย่างต่อเนื่องเพื่อมิให้เกิดผลกระทบต่อการดำเนินงานของ สบน. คือ กระบวนงานบริหารการชำระหนี้ (สบช.) รวมทั้ง กระบวนงานสนับสนุน คือ กระบวนการบริหารระบบเทคโนโลยีสารสนเทศ (ศทส.) ที่จะทำให้การปฏิบัติงานในกระบวนงานหลักอื่นๆ ของ สบน. เป็นไปอย่างต่อเนื่อง โดยเฉพาะข้อมูลหนี้สาธารณะ ซึ่งมีความสำคัญและเป็นข้อมูลหลักของการดำเนินงาน ดังนั้น สบน. จึงได้คัดเลือกทั้ง ๒ กระบวนงาน มาจัดทำแผนบริหารความต่อเนื่อง หรือต่อไปนี้จะเรียกว่า “Business Continuity Plan (BCP)” เพื่อให้สำนักบริหารการชำระหนี้ (สบช.) และศูนย์เทคโนโลยีสารสนเทศ (ศทส.) หรือต่อไปนี้จะเรียกว่า “หน่วยงาน” สามารถนำแผนดังกล่าวไปใช้ในการตอบสนองและปฏิบัติงานในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ ทั้งที่เกิดจากภัยธรรมชาติ อุบัติเหตุ หรือการมุ่งร้ายต่อองค์กร เช่น อุทกภัย อัคคีภัย การก่อการประท้วง การก่อการจลาจล การก่อวินาศกรรม เป็นต้น ทั้งนี้ เพื่อมิให้สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินดังกล่าวส่งผลให้หน่วยงานต้องหยุดการดำเนินงาน หรือไม่สามารถให้บริการได้อย่างต่อเนื่อง รวมทั้ง แผนบริหารความต่อเนื่องจะสามารถสนับสนุนให้หน่วยงานรับมือกับเหตุการณ์ฉุกเฉินที่ไม่อาจคาดคิดได้ และยังสามารถทำให้กระบวนการที่สำคัญ (Critical Business Process) กลับมาดำเนินการได้อย่างเป็นปกติ หรือตามระดับการให้บริการที่ได้กำหนดไว้ ซึ่งจะทำให้สามารถลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อหน่วยงานและ สบน. ได้

๑.๒ วัตถุประสงค์ (Objectives)

- เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่องของการปฏิบัติงาน
- เพื่อให้หน่วยงานมีการเตรียมความพร้อมในการรับมือกับสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ ที่อาจเกิดขึ้น
- เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงานหรือการให้บริการ
- เพื่อบรรเทาความเสียหายให้อยู่ในระดับที่ยอมรับได้
- เพื่อให้ประชาชน เจ้าหน้าที่ หน่วยงานรัฐวิสาหกิจ หน่วยงานภาครัฐ และผู้รับบริการ (Customer)/ ผู้มีส่วนได้ส่วนเสีย (Stakeholders) มีความเชื่อมั่นในศักยภาพของหน่วยงาน แม้หน่วยงานต้องเผชิญกับเหตุการณ์ร้ายแรงและส่งผลกระทบจนทำให้การดำเนินงานต้องหยุดชะงัก

๑.๓ สมมติฐานของแผนบริหารความต่อเนื่อง (BCP Assumptions)

เอกสารฉบับนี้ สบน. จัดทำขึ้นภายใต้สมมติฐาน ดังต่อไปนี้

- เหตุการณ์ฉุกเฉินที่เกิดขึ้นในช่วงเวลาสำคัญต่างๆ แต่มิได้ส่งผลกระทบต่อสถานที่ปฏิบัติงานสำรองที่ได้มีการจัดเตรียมไว้
- หน่วยงานเทคโนโลยีสารสนเทศรับผิดชอบในการสำรองระบบสารสนเทศต่างๆ โดยระบบสารสนเทศสำรองมิได้รับผลกระทบจากเหตุการณ์ฉุกเฉินเหมือนกับระบบสารสนเทศหลัก
- “บุคลากร” ที่ถูกระบุในเอกสารฉบับนี้ หมายถึง เจ้าหน้าที่และพนักงานทั้งหมดของหน่วยงาน

๑.๔ ขอบเขตของแผนบริหารความต่อเนื่อง (Scope of BCP)

สบน. ได้มีการวิเคราะห์ความเสี่ยง และภัยคุกคามของเหตุการณ์หรือภัยพิบัติทางธรรมชาติที่อาจส่งผลกระทบต่อการปฏิบัติงานและการให้บริการของหน่วยงาน และใช้เกณฑ์ในการวิเคราะห์ตามแนวทางการบริหารความเสี่ยง โดยพิจารณาจากโอกาสและผลกระทบของเหตุการณ์ที่อาจส่งผลกระทบต่อการดำเนินงานของ สบน. โดยได้คัดเลือกเหตุการณ์ความเสี่ยงที่มีระดับความเสี่ยงปานกลางขึ้นไปเพื่อมาจัดทำแผนบริหารความต่อเนื่อง ประกอบด้วยเหตุการณ์ ดังต่อไปนี้

๑. อัคคีภัย
๒. การชุมนุมเรียกร้องทางการเมือง หรือการปิดล้อมสถานที่ปฏิบัติงานของส่วนราชการ
๓. อุทกภัย
๔. ระบบคอมพิวเตอร์ขัดข้อง ข้อมูลสูญหายจากไวรัสและหรือการจารกรรมข้อมูล

๑.๕ การวิเคราะห์ทรัพยากรที่สำคัญ

- สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินมีหลากหลายรูปแบบ ดังนั้น เพื่อให้หน่วยงานมีแนวทางในการบริหารจัดการได้อย่างต่อเนื่อง การจัดหาทรัพยากรที่สำคัญจึงเป็นสิ่งจำเป็นที่ต้องระบุไว้ในแผนบริหารความต่อเนื่อง ซึ่งการจัดเตรียมทรัพยากรที่สำคัญ จะพิจารณาจากผลกระทบใน ๕ ด้าน ดังต่อไปนี้

๑. ผลกระทบด้านอาคาร/สถานที่ปฏิบัติงานหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้สถานที่ปฏิบัติงานหลักได้รับความเสียหาย หรือไม่สามารถใช้สถานที่ปฏิบัติงานหลักได้ และส่งผลให้บุคลากรไม่สามารถเข้าไปปฏิบัติงานได้ชั่วคราวหรือระยะยาว

๒. ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญ หรือไม่สามารถจัดหา/จัดส่งวัสดุอุปกรณ์ที่สำคัญเพื่อใช้ในการปฏิบัติงานได้

๓. ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ระบบงานเทคโนโลยี หรือระบบสารสนเทศ หรือข้อมูลที่สำคัญไม่สามารถนำมาใช้ในการปฏิบัติงานได้ตามปกติ

๔. ผลกระทบด้านบุคลากรหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ

๕. ผลกระทบด้านคู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสียที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย ไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้

- นำผลวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงและภัยคุกคามไประบุไว้ในตารางที่ ๑ ทั้งนี้ความเสี่ยงและภัยคุกคามบางเหตุการณ์อาจส่งผลกระทบต่อทรัพยากรของหน่วยงานได้มากกว่า ๑ ด้าน

ตารางที่ ๑ การประเมินความเสี่ยงและภัยคุกคาม และผลกระทบต่อทรัพยากรสำคัญ

ความเสี่ยงและภัยคุกคาม	ผลกระทบ				
	ด้านอาคาร/สถานที่ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ	ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	ด้านบุคลากรหลัก	ด้านคู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสียที่สำคัญ
๑. อัคคีภัย	✓	✓	✓	✓	
๒. การชุมนุมเรียกร้องทางการเมือง หรือการปิดล้อมส่วนราชการ	✓	✓		✓	✓
๓. อุทกภัย	✓	✓		✓	✓
๔. ระบบคอมพิวเตอร์ขัดข้อง ข้อมูลสูญหายจากไวรัสและหรือการจารกรรมข้อมูล		✓	✓		

อนึ่ง แผนบริหารความต่อเนื่อง (BCP) ฉบับนี้ ไม่รองรับการปฏิบัติงานในกรณีที่มีเหตุขัดข้องอันเกิดขึ้นจากการดำเนินงานปกติ และเหตุขัดข้องดังกล่าวไม่ส่งผลกระทบในระดับสูงต่อการดำเนินงานและการให้บริการของหน่วยงาน เนื่องจากหน่วยงานยังสามารถจัดการหรือปรับปรุงแก้ไขสถานการณ์ได้ภายในระยะเวลาที่เหมาะสม โดยผู้บริหารหน่วยงาน หรือผู้บริหารของแต่ละกลุ่มงานและฝ่ายงานสามารถรับผิดชอบและดำเนินการได้ด้วยตนเอง

๑.๖ การติดตามและรายงานผล

การติดตามและรายงานผลการดำเนินการตามแผนบริหารความต่อเนื่องของ สบน. ให้หัวหน้าคณะบริหารความต่อเนื่องของแต่ละหน่วยงานรายงานผลการดำเนินงานตามแผนดังกล่าวให้ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ และ/หรือผู้บริหารระดับสูงที่กำกับดูแลแต่ละหน่วยงานทราบเป็นระยะๆ อย่างต่อเนื่อง

บทที่ ๒
การศึกษาและทำความเข้าใจองค์กร

๒.๑ การศึกษาและวิเคราะห์ภารกิจขององค์กร

เป็นขั้นตอนการศึกษาและระบุกิจกรรมหรือกระบวนการสำคัญๆ ภายในของ สบน. โดยทำความเข้าใจองค์กร และนำโครงสร้างองค์กรและลักษณะงานตามกฎกระทรวงการแบ่งส่วนราชการสำนักงานบริหารหนี้สาธารณะ กระทรวงการคลังฯ พ.ศ. ๒๕๕๑ มาพิจารณาและสรุปรวมลงในตาราง เพื่อประเมินผลกระทบในขั้นต่อไป ดังปรากฏตามตารางที่ ๒

ตารางที่ ๒ การกำหนดกระบวนการจากคำบรรยายลักษณะงาน (Functional Description)

หน่วยงาน	กิจกรรม/กระบวนการ
๑. กลุ่มพัฒนาระบบบริหาร	๑. เสนอแนะให้คำปรึกษาแก่ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะเกี่ยวกับยุทธศาสตร์การพัฒนาระบบราชการภายในสำนักงาน
	๒. ติดตาม ประเมินผล และจัดทำรายงานเกี่ยวกับการพัฒนาระบบราชการในสำนักงาน
	๓. ประสานและดำเนินการเกี่ยวกับการพัฒนาระบบราชการร่วมกับหน่วยงานกลางต่างๆ และหน่วยงานในสังกัดสำนักงาน
๒. กลุ่มตรวจสอบภายใน	๑. ดำเนินการเกี่ยวกับการตรวจสอบด้านการบริหาร การเงิน และการบัญชีของสำนักงาน
	๒. ให้ข้อเสนอแนะ เพื่อปรับปรุงการปฏิบัติงานของส่วนราชการให้ดีขึ้น ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบ
๓. กลุ่มกฎหมาย	๑. เสนอแนะความเห็น และให้คำปรึกษาข้อหารือทางกฎหมาย กฎ ระเบียบ และข้อบังคับที่เกี่ยวข้อง
	๒. ดำเนินการเกี่ยวกับกฎหมาย ระเบียบ มติคณะรัฐมนตรี และประกาศที่เกี่ยวข้องกับการบริหารหนี้สาธารณะ รวมทั้งศึกษา พิจารณา ปรับปรุง และพัฒนากฎหมายและระเบียบที่เกี่ยวข้องให้มีประสิทธิภาพและสอดคล้องกับนโยบายและแผนเกี่ยวกับหนี้สาธารณะของประเทศ
	๓. ดำเนินการเกี่ยวกับงานนิติกรรมและสัญญา ตลอดจนยกร่างสัญญาที่เกี่ยวข้องกับการบริหารหนี้สาธารณะ งานเกี่ยวกับความรับผิดทางแพ่งและอาญา งานคดีปกครอง และงานคดีอื่นที่อยู่ในอำนาจหน้าที่ของสำนักงาน
๔. สำนักงานเลขานุการกรม	๑. ปฏิบัติงานสารบรรณของสำนักงาน
	๒. ดำเนินการเกี่ยวกับการช่วยอำนวยการ และงานเลขานุการของสำนักงาน
	๓. ประชาสัมพันธ์และเผยแพร่กิจกรรม ความรู้ ความก้าวหน้า และผลงานของสำนักงาน
	๔. ดำเนินการเกี่ยวกับงานการเงิน การบัญชี การงบประมาณ การพัสดุ อาคารสถานที่ และยานพาหนะของสำนักงาน
	๕. จัดระบบงานและบริหารงานบุคคลของสำนักงาน
๕. ศูนย์เทคโนโลยีสารสนเทศ	๑. จัดทำแผนแม่บทและแผนปฏิบัติการด้านเทคโนโลยีสารสนเทศของสำนักงานให้สอดคล้องกับนโยบายเทคโนโลยีสารสนเทศของกระทรวงการคลัง
	๒. วางแผน พัฒนา และจัดให้มีการนำระบบเทคโนโลยีสารสนเทศสมัยใหม่เพื่อนำมาใช้ในการบริหารการปฏิบัติงานภายในสำนักงานและให้บริการประชาชน
	๓. วิเคราะห์ ประมวลผล ปรับปรุง ตรวจสอบ และเผยแพร่ข้อมูลหนี้สาธารณะและข้อมูลของสำนักงาน
	๔. กำกับดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศของสำนักงาน

	๕. เป็นศูนย์กลางการพัฒนาบุคลากรของสำนักงานให้มีความรู้ความเข้าใจด้านเทคโนโลยีสารสนเทศ
หน่วยงาน	**กิจกรรม/กระบวนการ**
๖. สำนักงานจัดการหนี้ ๑	๑. ดำเนินการเกี่ยวกับการกู้เงิน การค้ำประกัน และการให้กู้ต่อสำหรับโครงการเงินกู้ในประเทศและต่างประเทศ
	๒. ดำเนินการเกี่ยวกับการบริหารหนี้สาธารณะและความเสี่ยงจากเงินกู้ในประเทศและต่างประเทศ
	๓. กำหนดแผนและกลยุทธ์ในการระดมเงิน การก่อหนี้ และการให้กู้ต่อ
	๔. กำหนดหลักเกณฑ์การก่อหนี้และการให้กู้ต่อ
	๕. ติดตามและประเมินภาวะตลาดเงินทุนในประเทศและต่างประเทศ รวมทั้งฐานะการเงินการคลัง
	๖. ดำเนินการเกี่ยวกับการซื้อคืนหรือไถ่ถอนตราสารหนี้
	๗. ให้คำปรึกษาและคำแนะนำในการบริหารหนี้สาธารณะแก่หน่วยงานที่อยู่ในความรับผิดชอบ
	๘. ประสานงานกับหน่วยงานที่เกี่ยวข้องในการจัดทำแผนการระดมเงิน แผนการกู้เงินเพื่อพัฒนาตลาดตราสารหนี้ และแผนการบริหารหนี้สาธารณะ
	๙. กำหนดแผนและกลยุทธ์ในการระดมเงินและการดำเนินการกู้เพื่อบริหารเงินคงคลัง
๗. สำนักงานจัดการหนี้ ๒	๑. ดำเนินการเกี่ยวกับการกู้เงิน การค้ำประกัน และการให้กู้ต่อสำหรับโครงการเงินกู้ในประเทศและต่างประเทศ
	๒. ดำเนินการเกี่ยวกับการบริหารหนี้สาธารณะและความเสี่ยงจากเงินกู้ในประเทศและต่างประเทศ
	๓. กำหนดแผนและกลยุทธ์ในการระดมเงิน การก่อหนี้ และการให้กู้ต่อ
	๔. กำหนดหลักเกณฑ์การก่อหนี้และการให้กู้ต่อ
	๕. ติดตามและประเมินภาวะตลาดเงินทุนในประเทศและต่างประเทศ รวมทั้งฐานะการเงินการคลังของรัฐวิสาหกิจ
	๖. ดำเนินการเกี่ยวกับการซื้อคืนหรือไถ่ถอนตราสารหนี้
	๗. ให้คำปรึกษาและคำแนะนำในการบริหารและจัดการหนี้สาธารณะแก่รัฐวิสาหกิจ
	๘. ประสานงานกับหน่วยงานที่เกี่ยวข้องในการจัดทำแผนการระดมเงิน และแผนการบริหารหนี้สาธารณะของรัฐวิสาหกิจ
๘. สำนักนโยบายและแผน	๑. ติดตามและประเมินผลเกี่ยวกับสถานะหนี้สาธารณะและหนี้ของประเทศในภาพรวม
	๒. เสนอแนะกรอบนโยบายและแนวทางการบริหารหนี้สาธารณะและการบริหารความเสี่ยงของหนี้สาธารณะ
	๓. ดำเนินการเกี่ยวกับการจัดทำแผนการบริหารหนี้สาธารณะประจำปีงบประมาณ และจัดทำรายงานการกู้เงินและการค้ำประกัน รวมทั้งรายงานสถานะหนี้สาธารณะและผลการดำเนินงานต่างๆ เพื่อเสนอต่อรัฐบาลและรัฐสภา และเผยแพร่ต่อสาธารณชน
	๔. จัดทำหลักเกณฑ์การค้ำประกันและการให้กู้ต่อ รวมทั้งแนวทางการประเมินระดับความน่าเชื่อถือของหน่วยงานในกำกับดูแลของรัฐ องค์กรปกครองส่วนท้องถิ่น และรัฐวิสาหกิจ ตลอดจนกำหนดค่าธรรมเนียมในการค้ำประกันและการให้กู้ต่อ
	๕. ประสานกับรัฐบาลต่างประเทศ สถาบันการเงินระหว่างประเทศ สถาบันจัดอันดับความน่าเชื่อถือ สถาบันการเงิน และนักลงทุน เพื่อจัดหาแหล่งเงินกู้
๙. สำนักบริหารการชำระหนี้	๑. วิเคราะห์ภาระหนี้ของรัฐบาลเพื่อจัดทำคำขอตั้งงบประมาณรายจ่ายเพื่อชำระหนี้ของรัฐบาล
	๒. ศึกษาวิเคราะห์เกี่ยวกับการทำธุรกรรมทางการเงินและข้อมูลที่เกี่ยวข้อง เพื่อให้การบริหารงบชำระหนี้ของรัฐบาลเกิดประโยชน์สูงสุด
	๓. กำหนดกลยุทธ์และแนวทางการบริหารงบชำระหนี้ของรัฐบาล รวมทั้งดำเนินการชำระหนี้

หน่วยงาน	กิจกรรม/กระบวนการ
	๔. กำกับและติดตามการชำระเงินที่ให้กู้ต่อและการจัดเก็บค่าธรรมเนียมการค้ำประกันและการให้กู้ต่อ
	๕. บริหารจัดการการชำระเงินที่ให้กู้ต่อ บริหารจัดการเงินกู้ที่เป็นเงินนอกงบประมาณและกองทุนที่มิได้กำหนดให้เป็นหน้าที่ของส่วนราชการใดโดยเฉพาะตามที่ได้รับมอบหมาย
	๖. ประสานกับหน่วยงานที่เกี่ยวข้องเกี่ยวกับการบริหารงบชำระหนี้ของรัฐบาล และการบริหารจัดการตาม ข้อ ๕
๑๐. สำนักบริหารการระดมทุนโครงการลงทุนภาครัฐ	๑. พิจารณาความเหมาะสมของการระดมทุนสำหรับโครงการลงทุนของภาครัฐโดยศึกษาและวิเคราะห์รายละเอียดเกี่ยวกับความเป็นไปได้ของโครงการ รวมทั้งศึกษาเพื่อกำหนดแนวทางการระดมทุนในโครงการลงทุนของภาครัฐ
	๒. ศึกษา เสนอแนะ หรือจัดทำแผนการบริหารจัดการด้านการเงินสำหรับโครงการลงทุนของภาครัฐที่เป็นการก่อหนี้สาธารณะ
	๓. ให้คำปรึกษาหรือคำแนะนำเกี่ยวกับการระดมเงินทุนหรือจัดหาแหล่งเงินทุน สำหรับโครงการลงทุนของภาครัฐ
	๔. เร่งรัดและติดตามการดำเนินงานของหน่วยงานที่รับผิดชอบโครงการลงทุนของภาครัฐที่เป็นการก่อหนี้สาธารณะให้เป็นไปตามเป้าหมายและแผนงานที่กำหนด
	๕. ดำเนินการร่วมกับหน่วยงานที่เกี่ยวข้องในการพิจารณาความเหมาะสมและจัดลำดับความสำคัญของโครงการลงทุนภาครัฐ และแผนการใช้จ่ายเงินของโครงการลงทุนของภาครัฐตามแผนการบริหารหนี้สาธารณะประจำปีงบประมาณ
	๖. บริหารศูนย์ข้อมูลที่ปรึกษาที่จัดตั้งตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการพัสดุ รวมทั้งส่งเสริมและพัฒนากิจการที่ปรึกษาไทยให้เป็นศูนย์ข้อมูลที่ปรึกษาในระดับภูมิภาค
๑๑. สำนักพัฒนาตลาดตราสารหนี้	๑. กำหนดนโยบายและแนวทางในการกู้เงินเพื่อปรับโครงสร้างหนี้และพัฒนาตลาดตราสารหนี้ และกำหนดแผนและกลยุทธ์ในการพัฒนาตลาดตราสารหนี้ในประเทศ แผนการออกตราสารหนี้แผนการซื้อคืนหรือไถ่ถอนตราสารหนี้
	๒. กำหนดกลยุทธ์ในการบริหารและจัดการกองทุนบริหารเงินกู้เพื่อการปรับโครงสร้างหนี้สาธารณะและพัฒนาตลาดตราสารหนี้ในประเทศ
	๓. ศึกษาและวิเคราะห์ภาวะตลาดตราสารหนี้ เครื่องมือทางการเงินต่าง ๆ และสถานะเศรษฐกิจการเงินการคลังของประเทศในภาพรวม เพื่อใช้เป็นข้อมูลในการพัฒนาตลาดตราสารหนี้รวมทั้งความเหมาะสมในการกู้เงินที่เอื้อต่อการพัฒนาตลาดตราสารหนี้
	๔. ศึกษา วิจัย และพัฒนาตราสารหนี้และการนำเครื่องมือทางการเงินมาใช้ เพื่อให้การระดมทุนของภาครัฐเป็นไปอย่างมีประสิทธิภาพ
	๕. ประสานงานกับหน่วยงานที่เกี่ยวข้องกับการพัฒนาตราสารหนี้และการพัฒนาตลาดพันธบัตรเอเชีย

หมายเหตุ : กิจกรรม/กระบวนงานที่กำหนดเป็นไปตามอำนาจหน้าที่ที่ปรากฏตามกฎกระทรวงการแบ่งส่วนราชการสำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง พ.ศ. ๒๕๕๑

๒.๒ การประเมินความเสี่ยงและภัยคุกคาม

ปัจจุบัน สบน. มีพื้นที่สำหรับการปฏิบัติงาน ๒ แห่ง คือ ชั้น ๔ อาคารสำนักงานเศรษฐกิจการคลัง กระทรวงการคลัง และชั้น ๓๒ อาคารทิปโก้ ถนนพระราม ๖ ซึ่ง สบน. ได้มีการวิเคราะห์ความเสี่ยง และภัยคุกคามของเหตุการณ์หรือภัยพิบัติทางธรรมชาติที่มีโอกาสเกิดขึ้นและส่งผลกระทบต่อการปฏิบัติงานในพื้นที่ และได้มีการกำหนดเกณฑ์ในการวิเคราะห์ตามแนวทางการบริหารความเสี่ยง โดยพิจารณาจากโอกาสและผลกระทบของเหตุการณ์ที่อาจส่งผลกระทบต่อการดำเนินงานของ สบน. ดังต่อไปนี้

๑. โอกาสในการเกิด

โอกาสในการเกิด	เกณฑ์ในการให้คะแนน
สูง	๕
ค่อนข้างสูง	๔
ปานกลาง	๓
ค่อนข้างต่ำ	๒
ต่ำ	๑

๒. ผลกระทบต่อการดำเนินงานตามพันธกิจ

ผลกระทบ	เกณฑ์ในการให้คะแนน
สูง	๕
ค่อนข้างสูง	๔
ปานกลาง	๓
ค่อนข้างต่ำ	๒
ต่ำ	๑

โดยการวิเคราะห์ความเสี่ยงของเหตุการณ์ต่างๆ จะพิจารณาจากสถานที่ตั้งของหน่วยงาน โอกาส และผลกระทบของเหตุการณ์ที่เกิดขึ้นกับหน่วยงาน โดยมีรายละเอียด ดังต่อไปนี้

เหตุการณ์	โอกาส	ผลกระทบ	ระดับความเสี่ยง (โอกาส x ผลกระทบ)	การจัดระดับ
แผ่นดินไหว	๑	๓	๓	X
อุทกภัย	๑	๕	๕	O
วาตภัย	๑	๑	๑	-
อัคคีภัย	๓	๕	๑๕	✔
ระบบคอมพิวเตอร์ขัดข้อง ข้อมูลสูญหายจากไวรัสและหรือการจารกรรมข้อมูล	๑	๕	๕	O
การชุมนุมเรียกร้องทางการเมือง หรือการปิดล้อมส่วนราชการ	๓	๓	๙	O

<u>การวิเคราะห์ระดับของความเสี่ยง</u>

โอกาสในการเกิดเหตุการณ์						
	5	o	✔	✔	✔	✔
	4	o	o	o	✔	✔
	3	x	x	o	o	✔
	2	-	x	x	o	o
	1	-	-	x	x	o
		1	2	3	4	5
		ผลกระทบ				

โดยที่

✔	มีความเสี่ยงสูงมาก
o	มีความเสี่ยงสูง
x	มีความเสี่ยงปานกลาง
-	มีความเสี่ยงต่ำ

และได้คัดเลือกเหตุการณ์ความเสี่ยงที่มีระดับความเสี่ยงปานกลางขึ้นไปเพื่อมาจัดทำแผนบริหารความต่อเนื่องตามหลักเกณฑ์ที่ได้มีการวิเคราะห์ในข้อ ๑.๕ การวิเคราะห์ทรัพยากรที่สำคัญ

๒.๓ การประเมินผลกระทบต่อกระบวนการดำเนินงาน

การประเมินผลกระทบต่อกระบวนการดำเนินงาน หรือการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) ได้กำหนดระดับผลกระทบออกเป็น ๕ ระดับ โดยมีหลักเกณฑ์ในการพิจารณาระดับผลกระทบดังต่อไปนี้

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
สูงมาก	• เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับสูงมาก • ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงมากกว่า ร้อยละ ๕๐ • เกิดการสูญเสียชีวิต และ/หรือภัยคุกคามต่อสาธารณชน • ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับประเทศและนานาชาติ
สูง	• เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับสูง • ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงร้อยละ ๒๐-๕๐ • เกิดการบาดเจ็บต่อผู้รับบริการ/บุคคล/กลุ่มคน • ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับประเทศ
ปานกลาง	• เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับปานกลาง • ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงร้อยละ ๑๐-๒๕ • ต้องมีการรักษาพยาบาล • ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับท้องถิ่น
ต่ำ	• เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับต่ำ • ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงร้อยละ ๕-๑๐ • ต้องมีการปฐมพยาบาล • ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับท้องถิ่น
ไม่เป็นสาระสำคัญ	• ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงมากกว่าร้อยละ ๕

ทั้งนี้ นอกจากการประเมินผลกระทบแล้ว หน่วยงานต้องประเมินระดับผลกระทบในแต่ละช่วงระยะเวลาของการหยุดชะงักที่ไม่สามารถปฏิบัติงานได้ด้วย ซึ่งแบ่งออกเป็น ๖ ช่วงระยะเวลา คือ ๑) ๐-๒ ชั่วโมง ๒) ๒-๔ ชั่วโมง ๓) ๑ ชั่วโมง ๔) ๑ สัปดาห์ ๕) ๒ สัปดาห์ ๖) ๑ เดือน และต้องนำผลกระทบที่ได้มีการกำหนดไว้ในตารางที่ ๒ มาประเมินกระบวนการที่สำคัญและระบุระดับผลกระทบ และนำไปจัดทำเป็นข้อมูลผลกระทบตามช่วงเวลาของการหยุดชะงัก ดังปรากฏตามตารางที่ ๓

ตารางที่ ๓ ผลกระทบตามช่วงเวลาของการหยุดชะงัก

๓.๑ กลุ่มพัฒนาระบบบริหาร

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. เสนอแนะให้คำปรึกษาแก่ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะเกี่ยวกับยุทธศาสตร์การพัฒนาระบบราชการภายในสำนักงาน	ต่ำ				✓	✓	✓
๒. ติดตาม ประเมินผล และจัดทำรายงานเกี่ยวกับการพัฒนาระบบราชการในสำนักงาน	ต่ำ				✓	✓	✓
๓. ประสานและดำเนินการเกี่ยวกับการพัฒนาระบบราชการร่วมกับหน่วยงานกลางต่างๆ และหน่วยงานในสังกัดสำนักงาน	ต่ำ				✓	✓	✓

๓.๒ กลุ่มตรวจสอบภายใน

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. ดำเนินการเกี่ยวกับการตรวจสอบด้านการบริหารการเงินและการบัญชีของสำนักงาน	ต่ำ			✓	✓	✓	✓
๒. ให้ข้อเสนอแนะ เพื่อปรับปรุงการปฏิบัติงานของส่วนราชการให้ดีขึ้น ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุมและการกำกับดูแลอย่างเป็นระบบ	ต่ำ				✓	✓	✓

๓.๓ กลุ่มกฎหมาย

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. เสนอแนะความเห็น และให้คำปรึกษาข้อหารือทางกฎหมาย กฎ ระเบียบ และข้อบังคับที่เกี่ยวข้อง	ต่ำ			✓	✓	✓	✓
๒. ดำเนินการเกี่ยวกับกฎหมาย ระเบียบ มติคณะรัฐมนตรี และประกาศที่เกี่ยวข้องกับการบริหารหนี้สาธารณะ รวมทั้งศึกษา พิจารณา ปรับปรุง และพัฒนากฎหมายและระเบียบที่เกี่ยวข้องให้มีประสิทธิภาพและสอดคล้องกับนโยบายและแผนเกี่ยวกับหนี้สาธารณะของประเทศ	ต่ำ				✓	✓	✓

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๓. ดำเนินการเกี่ยวกับงานนิติกรรมและสัญญา ตลอดจนยกร่างสัญญาที่เกี่ยวข้องกับการบริหารหนี้สาธารณะ งานเกี่ยวกับความรับผิดทางแพ่งและอาญา งานคดีปกครอง และงานคดีอื่นที่อยู่ในอำนาจหน้าที่ของสำนักงาน	ต่ำ			✓	✓	✓	✓

๓.๔ สำนักงานเลขานุการกรม

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. ปฏิบัติงานสารบรรณของสำนักงาน	ต่ำ		✓	✓	✓	✓	✓
๒. ดำเนินการเกี่ยวกับการช่วยอำนวยการ และงานเลขานุการของสำนักงาน	ต่ำ			✓	✓	✓	✓
๓. ประชาสัมพันธ์และเผยแพร่กิจกรรม ความรู้ ความก้าวหน้า และผลงานของสำนักงาน	ต่ำ			✓	✓	✓	✓
๔. ดำเนินการเกี่ยวกับงานการเงิน การบัญชี การงบประมาณ การพัสดุ อาคารสถานที่ และยานพาหนะของสำนักงาน	ต่ำ		✓	✓	✓	✓	✓
๕. จัดระบบงานและบริหารงานบุคคลของสำนักงาน	ต่ำ			✓	✓	✓	✓

๓.๕ ศูนย์เทคโนโลยีสารสนเทศ

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. จัดทำแผนแม่บทและแผนปฏิบัติการด้านเทคโนโลยีสารสนเทศของสำนักงานให้สอดคล้องกับนโยบายเทคโนโลยีสารสนเทศของกระทรวงการคลัง	ต่ำ						✓
๒. วางแผน พัฒนา และจัดให้มีการนำระบบเทคโนโลยีสารสนเทศสมัยใหม่เพื่อนำมาใช้ในการบริหารการปฏิบัติงานภายในสำนักงานและให้บริการประชาชน	ต่ำ					✓	✓
๓. วิเคราะห์ ประมวลผล ปรับปรุง ตรวจสอบ และเผยแพร่ข้อมูลหนี้สาธารณะและข้อมูลของสำนักงาน	สูง			✓	✓	✓	✓
๔. กำกับดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศของสำนักงาน	ปานกลาง			✓	✓	✓	✓
๕. เป็นศูนย์กลางการพัฒนาบุคลากรของสำนักงานให้มีความรู้ความเข้าใจด้านเทคโนโลยีสารสนเทศ	ต่ำ					✓	✓

๓.๖ สำนักจัดการหนี้ ๑

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. ดำเนินการเกี่ยวกับการกู้เงิน การค้ำประกัน และการให้กู้ต่อสำหรับโครงการเงินกู้ในประเทศและต่างประเทศ	ปานกลาง					✓	✓
๒. ดำเนินการเกี่ยวกับการบริหารหนี้สาธารณะและความเสี่ยงจากเงินกู้ในประเทศและต่างประเทศ	ปานกลาง					✓	✓
๓. กำหนดแผนและกลยุทธ์ในการระดมเงิน การก่อหนี้และการให้กู้ต่อ	ต่ำ				✓	✓	✓
๔. กำหนดหลักเกณฑ์การก่อหนี้และการให้กู้ต่อ	ต่ำ					✓	✓
๕. ติดตามและประเมินภาวะตลาดเงินทุนในประเทศและต่างประเทศ รวมทั้งฐานะการเงินการคลัง	ต่ำ				✓	✓	✓
๖. ดำเนินการเกี่ยวกับการซื้อคืนหรือไถ่ถอนตราสารหนี้	ปานกลาง					✓	✓
๗. ให้คำปรึกษาและคำแนะนำในการบริหารหนี้สาธารณะแก่หน่วยงานที่อยู่ในความรับผิดชอบ	ต่ำ					✓	✓
๘. ประสานงานกับหน่วยงานที่เกี่ยวข้องในการจัดทำแผนการระดมเงิน แผนการกู้เงินเพื่อพัฒนาตลาดตราสารหนี้ และแผนการบริหารหนี้สาธารณะ	ต่ำ				✓	✓	✓
๙. กำหนดแผนและกลยุทธ์ในการระดมเงินและการดำเนินการกู้เพื่อบริหารเงินคงคลัง	ต่ำ				✓	✓	✓

๓.๗ สำนักจัดการหนี้ ๒

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. ดำเนินการเกี่ยวกับการกู้เงิน การค้ำประกัน และการให้กู้ต่อสำหรับโครงการเงินกู้ในประเทศและต่างประเทศ	ปานกลาง				✓	✓	✓
๒. ดำเนินการเกี่ยวกับการบริหารหนี้สาธารณะและความเสี่ยงจากเงินกู้ในประเทศและต่างประเทศ	ปานกลาง				✓	✓	✓
๓. กำหนดแผนและกลยุทธ์ในการระดมเงินการก่อหนี้และการให้กู้ต่อ	ต่ำ				✓	✓	✓
๔. กำหนดหลักเกณฑ์การก่อหนี้และการให้กู้ต่อ	ต่ำ					✓	✓
๕. ติดตามและประเมินภาวะตลาดเงินทุนในประเทศและต่างประเทศ รวมทั้งฐานะการเงินการคลังของรัฐวิสาหกิจ	ต่ำ				✓	✓	✓
๖. ดำเนินการเกี่ยวกับการซื้อคืนหรือไถ่ถอนตราสารหนี้	ปานกลาง					✓	✓
๗. ให้คำปรึกษาและคำแนะนำในการบริหารและจัดการหนี้สาธารณะแก่รัฐวิสาหกิจ	ต่ำ					✓	✓
๘. ประสานงานกับหน่วยงานที่เกี่ยวข้องในการจัดทำแผนการระดมเงิน และแผนการบริหารหนี้สาธารณะของรัฐวิสาหกิจ	ต่ำ				✓	✓	✓

๓.๘ สำนักนโยบายและแผน

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. ติดตามและประเมินผลเกี่ยวกับสถานะหนี้สาธารณะและหนี้ของประเทศในภาพรวม	ต่ำ				✓	✓	✓
๒. เสนอแนะกรอบนโยบายและแนวทางการบริหารหนี้สาธารณะและการบริหารความเสี่ยงของหนี้สาธารณะ	ต่ำ				✓	✓	✓
๓. ดำเนินการเกี่ยวกับการจัดทำแผนการบริหารหนี้สาธารณะประจำปีงบประมาณ และจัดทำรายงานการกู้เงินและการค้ำประกัน รวมทั้งรายงานสถานะหนี้สาธารณะและผลการดำเนินงานต่างๆ เพื่อเสนอต่อรัฐบาลและรัฐสภา และเผยแพร่ต่อสาธารณชน	ปานกลาง					✓	✓
๔. จัดทำหลักเกณฑ์การค้ำประกันและการให้กู้ต่อ รวมทั้งแนวทางการประเมินระดับความน่าเชื่อถือของหน่วยงานในกำกับดูแลของรัฐ องค์กรปกครองส่วนท้องถิ่นและรัฐวิสาหกิจ ตลอดจนกำหนดค่าธรรมเนียมในการค้ำประกันและการให้กู้ต่อ	ต่ำ					✓	✓
๕. ประสานกับรัฐบาลต่างประเทศ สถาบันการเงินระหว่างประเทศ สถาบันจัดอันดับความน่าเชื่อถือสถาบันการเงิน และนักลงทุน เพื่อจัดหาแหล่งเงินกู้	ปานกลาง					✓	✓

๓.๙ สำนักบริหารการชำระหนี้

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. วิเคราะห์ภาระหนี้ของรัฐบาล เพื่อจัดทำคำขอตั้งงบประมาณรายจ่ายเพื่อชำระหนี้ของรัฐบาล	ต่ำ			✓	✓	✓	✓
๒. ศึกษาวิเคราะห์เกี่ยวกับการทำธุรกรรมทางการเงินและข้อมูลที่เกี่ยวข้อง เพื่อให้การบริหารงบชำระหนี้ของรัฐบาลเกิดประโยชน์สูงสุด	ต่ำ				✓	✓	✓
๓. กำหนดกลยุทธ์และแนวทางการบริหารงบชำระหนี้ของรัฐบาล รวมทั้งดำเนินการชำระหนี้	สูง		✓	✓	✓	✓	✓
๔. กำกับและติดตามการชำระเงินที่ให้กู้ต่อและการจัดเก็บค่าธรรมเนียมการค้ำประกันและการให้กู้ต่อ	ต่ำ				✓	✓	✓
๕. บริหารจัดการการชำระเงินที่ให้กู้ต่อ บริหารจัดการเงินกู้ที่เป็นเงินนอกงบประมาณและกองทุนที่มิได้กำหนดให้เป็นหน้าที่ของส่วนราชการใดโดยเฉพาะตามที่ได้รับมอบหมาย	ต่ำ				✓	✓	✓
๖. ประสานกับหน่วยงานที่เกี่ยวข้องเกี่ยวกับการบริหารงบชำระหนี้ของรัฐบาล และการบริหารจัดการตาม ข้อ ๕	ต่ำ				✓	✓	✓

๓.๑๐ สำนักบริหารการระดมทุนโครงการลงทุนภาครัฐ

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. พิจารณาความเหมาะสมของการระดมทุนสำหรับโครงการลงทุนของภาครัฐโดยศึกษาและวิเคราะห์รายละเอียดเกี่ยวกับความเป็นไปได้ของโครงการ รวมทั้งศึกษาเพื่อกำหนดแนวทางการระดมทุนในโครงการลงทุนของภาครัฐ	ปานกลาง			✓	✓	✓	✓
๒. ศึกษา เสนอแนะ หรือจัดทำแผนการบริหารจัดการด้านการเงินสำหรับโครงการลงทุนของภาครัฐที่เป็นการก่อหนี้สาธารณะ	ต่ำ					✓	✓
๓. ให้คำปรึกษาหรือคำแนะนำเกี่ยวกับการระดมเงินทุนหรือจัดหาแหล่งเงินทุน สำหรับโครงการลงทุนของภาครัฐ	ต่ำ					✓	✓
๔. เร่งรัดและติดตามการดำเนินงานของหน่วยงานที่รับผิดชอบโครงการลงทุนของภาครัฐที่เป็นการก่อหนี้สาธารณะให้เป็นไปตามเป้าหมายและแผนงานที่กำหนด	ปานกลาง					✓	✓
๕. ดำเนินการร่วมกับหน่วยงานที่เกี่ยวข้องในการพิจารณาความเหมาะสมและจัดลำดับความสำคัญของโครงการลงทุนภาครัฐ และแผนการใช้จ่ายเงินของโครงการลงทุนของภาครัฐตามแผนการบริหารหนี้สาธารณะประจำปีงบประมาณ	ต่ำ				✓	✓	✓
๖. บริหารศูนย์ข้อมูลที่ปรึกษาที่จัดตั้งตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการพัสดุรวมทั้งส่งเสริมและพัฒนากิจการที่ปรึกษาไทยให้เป็นศูนย์ข้อมูลที่ปรึกษาในระดับภูมิภาค	ต่ำ					✓	✓

๓.๑๑ สำนักพัฒนาตลาดตราสารหนี้

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๑. กำหนดนโยบายและแนวทางในการกู้เงินเพื่อปรับโครงสร้างหนี้และพัฒนาตลาดตราสารหนี้และกำหนดแผนและกลยุทธ์ในการพัฒนาตลาดตราสารหนี้ในประเทศ แผนการออกตราสารหนี้แผนการซื้อคืนหรือไถ่ถอนตราสารหนี้	ปานกลาง					✓	✓
๒. กำหนดกลยุทธ์ในการบริหารและจัดการกองทุนบริหารเงินกู้เพื่อการปรับโครงสร้างหนี้สาธารณะและพัฒนาตลาดตราสารหนี้ในประเทศ	ต่ำ				✓	✓	✓

กิจกรรม	ระดับผลกระทบ	ระยะเวลาของการหยุดชะงัก					
		๐-๒ ชม.	๒-๔ ชม.	๑ วัน	๑ สัปดาห์	๒ สัปดาห์	๑ เดือน
๓. ศึกษาและวิเคราะห์ภาวะตลาดตราสารหนี้ เครื่องมือทางการเงินต่าง ๆ และสถานะเศรษฐกิจการเงินการคลังของประเทศในภาพรวม เพื่อใช้เป็นข้อมูลในการพัฒนาตลาดตราสารหนี้รวมทั้งความเหมาะสมในการกู้เงินที่เอื้อต่อการพัฒนาตลาดตราสารหนี้	ต่ำ				✓	✓	✓
๔. ศึกษา วิจัย และพัฒนาตราสารหนี้และการนำเครื่องมือทางการเงินมาใช้ เพื่อให้การระดมทุนของภาครัฐเป็นไปอย่างมีประสิทธิภาพ	ต่ำ					✓	✓
๕. ประสานงานกับหน่วยงานที่เกี่ยวข้องกับการพัฒนาตราสารหนี้และการพัฒนาตลาดพันธบัตรเอเชีย	ต่ำ					✓	✓

จากการประเมินและระบุระดับผลกระทบในตารางที่ได้กล่าวในข้างต้น สบน. ได้นำกระบวนการที่มีผลกระทบในระดับสูง และมีระยะเวลาของการหยุดชะงักต่ำกว่า ๑ วัน จำนวน ๒ กระบวนการ มาพิจารณาจัดทำแผนบริหารความต่อเนื่องของ สบน. ได้แก่

๑) กระบวนการวิเคราะห์ ประมวลผล ปรับปรุง ตรวจสอบ และเผยแพร่ข้อมูลหนี้สาธารณะและข้อมูลของสำนักงาน ซึ่งศูนย์เทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบ

๒) กระบวนการกำหนดกลยุทธ์และแนวทางการบริหารงบชำระหนี้ของรัฐบาล รวมทั้ง ดำเนินการชำระหนี้ ซึ่งสำนักบริหารการชำระหนี้เป็นผู้รับผิดชอบ

บทที่ ๓
แผนบริหารความต่อเนื่อง (Business Continuity Plan : BCP)

การจัดทำแผนบริหารความต่อเนื่อง (BCP) เป็นการเตรียมความพร้อมเพื่อให้หน่วยงานทั้ง ๒ หน่วยงาน ของ สบน. คือ ศูนย์เทคโนโลยีสารสนเทศ (ศทส.) และสำนักบริหารการชำระหนี้ (สบช.) สามารถตอบสนองต่อสภาวะฉุกเฉินที่ส่งผลให้การปฏิบัติงานของหน่วยงานต้องหยุดชะงัก ดังนั้น การจัดทำแผนประกอบด้วย การกำหนดโครงสร้างและทีมงานแผนบริหารความต่อเนื่อง กำหนดกระบวนการแจ้งผลกระทบ (Call Tree) กำหนดแนวทางการบริหารจัดการในช่วงเกิดเหตุในระยะสั้นและการกลับคืนในระยะกลาง รวมทั้ง การรวบรวมข้อมูลและรายละเอียด โดยมีรายละเอียดในแต่ละหน่วยงาน ดังต่อไปนี้

๓.๑ ศูนย์เทคโนโลยีสารสนเทศ (ศทส.)

๓.๑.๑ โครงสร้างและทีมงานแผนบริหารความต่อเนื่อง (Business Continuity Plan Team)

กระบวนการวิเคราะห์ ประมวลผล ปรับปรุง ตรวจสอบ และเผยแพร่ข้อมูลหนี้สาธารณะและข้อมูลของสำนักงานเป็นส่วนสำคัญในการสนับสนุนการปฏิบัติงานในภารกิจหลักของ สบน. เนื่องจากเป็นการบริหารจัดการข้อมูล (Data) หนี้สาธารณะของประเทศ ดังนั้น เพื่อให้แผนความต่อเนื่อง (BCP) ของ ศทส. สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและเกิดประสิทธิภาพ จะต้องจัดตั้งทีมงานบริหารความต่อเนื่อง (BCP Team) ขึ้น โดย BCP Team ประกอบด้วย

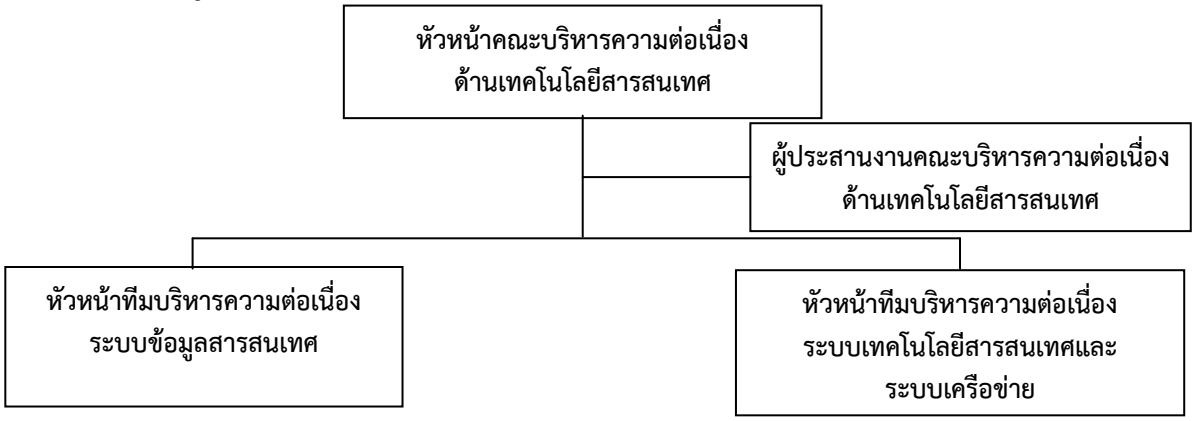
๑) หัวหน้าคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ)

๒) หัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการส่วนวิเคราะห์นโยบายและแผนสารสนเทศ และผู้อำนวยการส่วนบริหารระบบข้อมูลสารสนเทศ)

๓) ผู้ประสานงานคณะบริหารความต่อเนื่อง (ผู้อำนวยการส่วนวิเคราะห์นโยบายและแผนสารสนเทศ)

โดยกำหนดโครงสร้างคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ดังปรากฏตามรูปภาพที่ ๑

รูปภาพที่ ๑ โครงสร้างคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ



ทั้งนี้ แต่ละตำแหน่งจะต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงาน และกู้คืนเหตุการณ์ฉุกเฉินในฝ่ายงานของตนเองให้สามารถบริหารความต่อเนื่องและกลับสู่สภาวะปกติได้โดยเร็ว ตามบทบาทหน้าที่ที่กำหนดไว้ของทีมงานบริหารความต่อเนื่อง (BCP Team) และในกรณีที่บุคลากรหลักไม่สามารถปฏิบัติหน้าที่ได้ ให้บุคลากรสำรองรับผิดชอบทำหน้าที่ในบทบาทของบุคลากรหลักไปก่อน จนกว่าจะมีการมอบหมายจากหัวหน้าคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ โดยคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ประกอบด้วยบุคลากรหลักและบุคลากรสำรอง ปรากฏตามตารางที่ ๔

ตารางที่ ๔ รายชื่อบุคลากรและบทบาทของทีมงานบริหารความต่อเนื่อง (BCP Team)

บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ	เบอร์โทรศัพท์		ชื่อ	เบอร์โทรศัพท์
นางสาววราภรณ์ ปัญญศิริ (ผู้อำนวยการศูนย์ฯ)	๐๘๑-๘๓๐๒๑๖๔	หัวหน้าคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	นายครรชิต พะลัง (นักวิชาการคอมพิวเตอร์ชำนาญการ ปฏิบัติหน้าที่ผู้อำนวยการส่วน)	๐๘๑-๖๒๓๘๙๑๒
นายครรชิต พะลัง (นักวิชาการคอมพิวเตอร์ชำนาญการ ปฏิบัติหน้าที่ผู้อำนวยการส่วน)	๐๘๑-๖๒๓๘๙๑๒	ผู้ประสานงานคณะบริหารความเสี่ยง	นางสาวปฏิมา พักตร์ผ่อง (นักวิชาการคลังปฏิบัติการ)	๐๘๑-๔๙๓๙๙๑๘
- ว่าง – (ผู้อำนวยการส่วนบริหารระบบข้อมูลสารสนเทศ)	๐-๒๒๖๕๘๐๕๐ ต่อ ๕๒๐๗	ทีมงานบริหารความต่อเนื่องระบบข้อมูลสารสนเทศ	นายดำรัส หอกิจรุ่งเรือง (นักวิชาการคลังปฏิบัติการ)	๐๘๕-๙๑๑๑๓๘๑
นายครรชิต พะลัง (นักวิชาการคอมพิวเตอร์ชำนาญการ ปฏิบัติหน้าที่ผู้อำนวยการส่วน)	๐๘๑-๖๒๓๘๙๑๒	ทีมงานบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย	นายวีรยุทธ เจริญสุวรรณกิจ (นักวิชาการคอมพิวเตอร์ชำนาญการ) นางสาวอรวรรณ วิทูรกิตติกุล (นักวิชาการคอมพิวเตอร์) นายมนูญ ทะนันชัย (เจ้าพนักงานเครื่องคอมพิวเตอร์)	๐๘๗-๐๒๕๒๖๖๑ ๐๘๙-๔๘๘๘๖๙๙ ๐๘๙-๑๒๒๗๘๕๐

๓.๑.๒ กลยุทธ์ความต่อเนื่อง (Business Continuity Strategy)

กลยุทธ์ความต่อเนื่อง เป็นแนวทางในการจัดหาและบริหารจัดการทรัพยากรให้มีความพร้อมเมื่อเกิดสภาวะวิกฤต ซึ่งพิจารณาทรัพยากรใน ๕ ด้าน ดังนี้

ทรัพยากร		กลยุทธ์ความต่อเนื่อง
	**อาคาร/สถานที่ปฏิบัติงานสำรอง**	● กำหนดพื้นที่ปฏิบัติงานสำรองที่สามารถปฏิบัติงานได้ ณ สำนักงานบริหารหนี้สาธารณะ ชั้น ๓๒ อาคารทิปโก้ โดยประสานงานและเตรียมความพร้อมไว้ล่วงหน้า ● กำหนดพื้นที่ปฏิบัติงานสำรองที่สามารถปฏิบัติงานที่บ้านได้
	**วัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ**	● กำหนดให้มีการจัดหาคอมพิวเตอร์สำรองที่มีอยู่ภายใน สบน. ก่อนแล้วจึงสรรหาจากภายนอก เช่น หน่วยงานในสังกัดกระทรวงการคลัง หรือบริษัทตัวแทนจำหน่ายอุปกรณ์เครื่องมือ เป็นต้น ● กำหนดจัดหาคอมพิวเตอร์สำรองที่มีคุณลักษณะเหมาะสมกับการใช้งาน พร้อมอุปกรณ์ที่สามารถเชื่อมต่อผ่านอินเตอร์เน็ตเข้าสู่ระบบเทคโนโลยีของ สบน. และหน่วยงานกลาง (GFMIS-TR) ได้ ● กรณีที่คอมพิวเตอร์สำรองมีไม่เพียงพอ กำหนดให้ใช้คอมพิวเตอร์พกพา (Laptop/Notebook) ของหน้าเจ้าหน้าที่ หรือของ สบน. ได้ชั่วคราว
	**เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ**	● มีการจัดเตรียมระบบสารสนเทศสำรอง เช่น ฐานข้อมูลหนี้สาธารณะ ระบบ Email ไว้ที่เครื่องบันทึกข้อมูลแบบพกพา (Back up) ● สามารถสำรองและกู้คืนข้อมูลได้จากเครื่องคอมพิวเตอร์แม่ข่ายจากระบบที่ใช้งานร่วมกันระหว่างสำนักงานปลัดกระทรวงการคลัง กรมบัญชีกลาง และรัฐวิสาหกิจที่ใช้ข้อมูล ● มี server สำรองที่อาคารทิปโก้ ซึ่งสามารถสำรองข้อมูลทันทีที่สถานที่

ทรัพยากร		กลยุทธ์ความต่อเนื่อง
		ปฏิบัติงานหลักเกิดเหตุฉุกเฉิน ● จัดหาโปรแกรมคอมพิวเตอร์ที่มีคุณสมบัติที่สนับสนุนให้สามารถทำงานได้ทุกๆ ที่ เช่น โปรแกรม VDI ● ปฏิบัติงานโดยไม่ใช้ระบบงานเทคโนโลยี (Manual) ไปก่อน แล้วจึงป้อนข้อมูลเข้าในระบบ เมื่อกลับคืนสู่สภาวะปกติ
	**บุคลากรหลัก**	● กำหนดให้ใช้บุคลากรหลักและบุคลากรสำรอง ทำงานทดแทนกันได้ในสภาวะวิกฤต ● กำหนดแนวทางและกลุ่มบุคลากรที่สามารถขอให้ช่วยปฏิบัติงานชั่วคราว จากหน่วยงานราชการอื่นๆ ในสังกัด ● มีเจ้าหน้าที่จากบริษัทที่ปรึกษาด้าน IT฿ (Outsource Consultants) อยู่ประจำในการสนับสนุนและแก้ไขปัญหาทางเทคนิค
	**คู่ค้า/ผู้ให้บริการ/ ผู้มีส่วนได้ส่วนเสียที่สำคัญ**	● ปัจจุบัน สบน. กำหนดให้มีผู้บริการเครือข่ายอินเตอร์เน็ต จำนวน ๑ ราย คือ บริษัท True โดยสามารถเชื่อมโยงระบบเครือข่ายอินเตอร์เน็ตได้ใน ๒ รูปแบบ คือ Lease Line และ ADSL และหากระบบใดระบบหนึ่งไม่สามารถให้บริการได้ ระบบจะปรับเปลี่ยนไปยังระบบหนึ่งได้ภายใน ๒ ชั่วโมง ● จัดหาอุปกรณ์เพื่อใช้งานที่สามารถอำนวยความสะดวกได้ในเบื้องต้น เช่น Smart phone และ Tablet ให้แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญใช้ในกรณีฉุกเฉิน

๓.๑.๓ ผลกระทบทางธุรกิจ (Business Impact Analysis)

ในการวิเคราะห์ผลกระทบทางธุรกิจในบทที่ ๒ ตารางที่ ๓.๕ แล้ว ปรากฏว่า กระบวนการวิเคราะห์ ประมวลผล ปรับปรุง ตรวจสอบ และเผยแพร่ข้อมูลหนี้สาธารณะและข้อมูลของสำนักงาน มีความสำคัญและจำเป็นต้องดำเนินงานให้ข้อมูลมีความครบถ้วน และถูกต้อง รวมทั้ง ให้บริการได้ภายในระยะเวลาอันสั้น สำหรับกระบวนการอื่นๆ ที่ประเมินแล้ว อาจไม่ได้รับผลกระทบในระดับสูงถึงสูงมาก หรือมีความยืดหยุ่นให้สามารถชะลอการดำเนินงานและให้บริการได้ ให้ผู้บริหารของหน่วยงานและกลุ่มงานประเมินความจำเป็นและเหมาะสม ทั้งนี้ หากมีความจำเป็น ให้ปฏิบัติตามแนวทางการบริหารความต่อเนื่องเช่นเดียวกันกับกระบวนการหลัก

๓.๑.๔ กระบวนการแจ้งเหตุฉุกเฉิน Call Tree

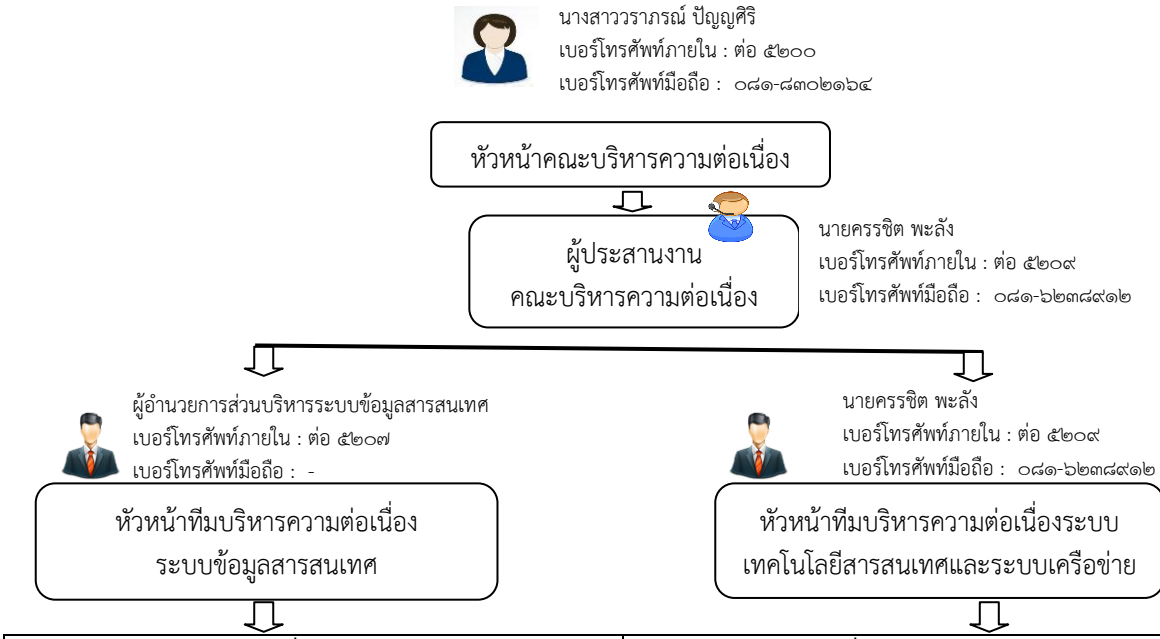
กระบวนการ Call Tree คือ กระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกในคณะบริหารความต่อเนื่องและทีมงานบริหารความต่อเนื่องที่เกี่ยวข้อง ตามผังรายชื่อทางโทรศัพท์ โดยมีวัตถุประสงค์เพื่อการบริหารจัดการขั้นตอนในการติดต่อเจ้าหน้าที่ ภายหลังจากมีการประกาศเหตุการณ์ฉุกเฉินหรือภาวะวิกฤตของหน่วยงาน

จุดเริ่มต้นของกระบวนการ Call Tree จะเริ่มจากหัวหน้าคณะบริหารความต่อเนื่องแจ้งให้ผู้ประสานงานคณะบริหารความต่อเนื่อง โดยผู้ประสานงาน฿ จะแจ้งให้หัวหน้าทีมบริหารความต่อเนื่องรับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่อง ตามสายงานการบังคับบัญชาของแต่ละสายงานเพื่อรับทราบเหตุการณ์ฉุกเฉิน และการประกาศใช้แผนความต่อเนื่องของหน่วยงานที่ได้รับผลกระทบ ตามรายชื่อและช่องทางติดต่อสื่อสารที่ได้ระบุไว้ ดังปรากฏตามรูปภาพที่ ๒

ในกรณีที่ไม่สามารถติดต่อหัวหน้าทีมได้ ให้ติดต่อไปยังบุคลากรสำรอง โดยพิจารณา ดังต่อไปนี้

- ถ้าเหตุการณ์เกิดขึ้นในเวลาทำการ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์ของหน่วยงานเป็นช่องทางแรก
- ถ้าเหตุการณ์เกิดขึ้นนอกเวลาทำการหรือสถานที่ปฏิบัติงานหลักได้รับผลกระทบ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์มือถือเป็นช่องทางแรก
- ถ้าสามารถติดต่อบุคลากรหลักได้ให้แจ้งข้อมูลแก่บุคลากรหลักของหน่วยงานทราบ ดังต่อไปนี้
  - สรุปสถานการณ์ของเหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่อง
  - เวลาและสถานที่สำหรับการนัดประชุมเร่งด่วนของหน่วยงาน สำหรับผู้บริหารของหน่วยงานและทีมงานบริหารความต่อเนื่อง
  - ขั้นตอนการปฏิบัติงาน เพื่อบริหารความต่อเนื่องต่อไป เช่น สถานที่รวมพลในกรณีที่มีการย้ายสถานที่ทำการ

รูปภาพที่ ๒ กระบวนการแจ้งเหตุ Call Tree



ทีมบริหารความต่อเนื่องระบบข้อมูลสารสนเทศ	หัวหน้าทีมบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย
นายดำรัส หอกิจรุ่งเรือง ๐๘๕-๙๑๑๑๓๘๑	นายวีรยุทธ เจริญสุวรรณกิจ ๐๘๗-๐๒๕๒๖๖๑
นายนนทกร กรีวัชรินทร์	นางสาวปฏิมา พักตร์ผ่อง ๐๘๑-๔๙๓๙๙๑๘
นางสาวอินทราภรณ์ สัตยาชัย ๐๘๓ ๗๘๕๐๕๘๒	นางสาวศรฤทัย สนธิเปล่งศรี ๐๘๖-๕๖๖๙๘๒๒

หมายเหตุ : กรณีที่พิจารณาแล้วเห็นว่า บุคลากรในทีมไม่เพียงพอให้พิจารณาบุคลากรที่เป็นลูกจ้างในสังกัดเป็นลำดับแรก

ภายหลังจากได้รับการตอบรับจากบุคลากรหลักครบถ้วนตามผังการติดต่อ (Call Tree) หัวหน้าหน่วยงานมีหน้าที่โทรกลับไปแจ้งยังผู้ประสานงานคณะบริหารความต่อเนื่อง เพื่อรวบรวมสรุปความพร้อมของหน่วยงานในการบริหารความต่อเนื่อง รวมทั้งความปลอดภัยในชีวิตและทรัพย์สินของหน่วยงาน และเจ้าหน้าที่ทั้งหมดในหน่วยงาน ทีมบริหารความต่อเนื่องมีหน้าที่ในการปรับปรุงข้อมูลสำหรับการติดต่อให้เป็นปัจจุบันอยู่ตลอดเวลา เพื่อให้กระบวนการติดต่อพนักงานภายในหน่วยงานสามารถดำเนินได้อย่างต่อเนื่องและสำเร็จลุล่วงภายในระยะเวลาที่คาดหวัง ในกรณีที่เกิดเหตุการณ์ฉุกเฉินและมีการประกาศใช้แผนความต่อเนื่อง

๓.๑.๕ ขั้นตอนในการบริหารความต่อเนื่องและกอบกู้กระบวนการ

การตอบสนองต่อเหตุการณ์ทันที ภายใน ๒๔ ชั่วโมง

ในการปฏิบัติการใดๆ ให้บุคลากรของหน่วยงาน คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นอย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
● ติดตาม สอบถาม และประเมินสถานการณ์ฉุกเฉิน และระยะเวลาในการกอบกู้สถานการณ์กับผู้บริหารของ สบน.	หัวหน้าคณะบริหารความต่อเนื่อง	☐
● แจ้งเหตุฉุกเฉิน วิกฤติ ตามกระบวนการ Call Tree ให้กับบุคลากรหลักในหน่วยงาน	ผู้ประสานงานคณะบริหารความต่อเนื่อง	
● จัดประชุมคณะบริหารความต่อเนื่อง เพื่อรับทราบและประเมินความเสียหายผลกระทบต่อการดำเนินงานและให้บริการ และทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง ● รับทราบและพิจารณาอนุมัติกระบวนงาน งานที่มีความเร่งด่วน และส่งผลกระทบอย่างสูงจำเป็นต้องดำเนินงานหรือปฏิบัติด้วยมือ (Manual Processing) โดยให้ปฏิบัติตามแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) (เอกสารภาคผนวก ๑)	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● แจ้งสรุปสถานการณ์และการประเมินทรัพยากรที่ครอบคลุม - จำนวนและรายชื่อบุคลากรที่ได้รับบาดเจ็บ/เสียชีวิต - ความเสียหายและผลกระทบต่อการดำเนินงานและให้บริการ - ทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง - กระบวนงาน/งานที่มีความเร่งด่วน และส่งผลกระทบอย่างสูงจำเป็นต้องดำเนินงานทันที	หัวหน้าคณะบริหารความต่อเนื่อง	☐
● สื่อสารและทำความเข้าใจเกี่ยวกับสถานการณ์ฉุกเฉินที่เกิดขึ้น และแนวทางในการปฏิบัติงานให้แก่บุคลากรในหน่วยงาน รวมทั้งหน่วยงานภายนอก เช่น รัฐวิสาหกิจ ที่จะต้องรายงานผ่านระบบเทคโนโลยีสารสนเทศของ สบน. (GFMIS-TR) ให้ทราบโดยทั่วถึง	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● พิจารณาและอนุมัติการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง - สถานที่ปฏิบัติงานสำรอง - วัสดุอุปกรณ์ที่สำคัญ - เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ - บุคลากรหลัก - คู่ค้า/ผู้ให้บริการที่สำคัญ	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● รายงานความคืบหน้าให้แก่หัวหน้าคณะบริหารความต่อเนื่องของ ศทส. อย่างสม่ำเสมอ หรือตามที่ได้มีการกำหนด	หัวหน้าทีมบริหารความต่อเนื่อง	☐

หมายเหตุ: ถ้าเหตุการณ์ฉุกเฉินนั้นเกินขีดความสามารถที่หน่วยงานจะรับได้ ให้ติดต่อประสานงานไปยังผู้อำนวยการสำนักงานบริหารหนี้สาธารณะช่วยเหลือต่อไป

การตอบสนองต่อเหตุการณ์ในระยะแรก ภายใน ๗ วัน

ในการปฏิบัติการใดๆ ให้บุคลากรของหน่วยงาน คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นอย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
● ติดตามสถานะภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ และประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● พิจารณาและอนุมัติการจัดหาทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ - สถานที่ปฏิบัติงานสำรอง - วัสดุอุปกรณ์ที่สำคัญ - เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ - บุคลากรหลัก - คู่ค้า/ผู้ให้บริการที่สำคัญ	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● รายงานความคืบหน้าให้แก่หัวหน้าคณะบริหารความต่อเนื่องของ ศทส. และหน่วยงานกำกับดูแล อย่างสม่ำเสมอ หรือตามที่ได้มีการกำหนด	หัวหน้าทีมบริหารความต่อเนื่อง	☐

หมายเหตุ: ถ้าเหตุการณ์ฉุกเฉินนั้นเกินขีดความสามารถที่หน่วยงานจะรับได้ ให้ติดต่อประสานงานไปยังผู้อำนวยการสำนักงานบริหารหนี้สาธารณะช่วยเหลือต่อไป

การตอบสนองต่อเหตุการณ์ฉุกเฉินและกู้คืนกระบวนการปฏิบัติงาน ในระยะเวลาเกิน ๗ วัน

ในการปฏิบัติการใดๆ ให้บุคลากรของหน่วยงาน คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นอย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
● ติดตามสถานภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ และประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● พิจารณาและอนุมัติการจัดหาทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติและสามารถปฏิบัติงานได้ในระยะยาว - สถานที่ปฏิบัติงานสำรอง หรือพิจารณาจัดหาสถานที่ปฏิบัติงานที่รองรับการปฏิบัติงานในสภาวะปกติของหน่วยงานได้ - วัสดุอุปกรณ์ที่สำคัญ หรือพิจารณาจัดซื้อจัดจ้างวัสดุอุปกรณ์และเครื่องมือที่ได้รับความเสียหาย - เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ ประสานกับหน่วยงานด้านเทคโนโลยีสารสนเทศเพื่อกู้คืนข้อมูลหรือวางระบบเทคโนโลยีสารสนเทศให้สามารถทำงานได้ตามปกติ - การสำรวจบุคลากรที่ได้รับผลกระทบและไม่สามารถกลับมาปฏิบัติงานเพื่อสรรหาบุคลากรทดแทนชั่วคราว - คู่ค้า/ผู้ให้บริการที่สำคัญ ประสานกับรัฐวิสาหกิจที่จะต้องรายงานผ่านระบบให้ทราบสถานการณ์ และแนวทางการแก้ปัญหาของ สบน.	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● รายงานความคืบหน้าให้แก่หัวหน้าคณะบริหารความต่อเนื่องของ ศทส. อย่างสม่ำเสมอ หรือตามที่ได้มีการกำหนด	หัวหน้าทีมบริหารความต่อเนื่อง	☐

หมายเหตุ : ถ้าเหตุการณ์ฉุกเฉินนั้นเกินขีดความสามารถที่หน่วยงานจะรับได้ ให้ติดต่อประสานงานไปยังผู้อำนวยการสำนักงานบริหารหนี้สาธารณะหรือผู้บริหารที่ได้รับมอบอำนาจให้ช่วยเหลือต่อไป

๓.๑.๖ การติดตามและรายงายผล

การติดตามและรายงานผลการดำเนินการตามแผน ให้หัวหน้าคณะบริหารความต่อเนื่องรายงานผลการดำเนินงานให้ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะหรือผู้บริหารระดับสูงที่กำกับดูแลทราบเป็นระยะๆ อย่างต่อเนื่อง

๓.๒ สำนักบริหารการชำระหนี้ (สบช.)

๓.๒.๑ โครงสร้างและทีมงานแผนความต่อเนื่อง (Business Continuity Plan Team)

เนื่องจากกระบวนการกำหนดกลยุทธ์และแนวทางการบริหารงบชำระหนี้ของรัฐบาล รวมทั้ง ดำเนินการชำระหนี้ เป็นกระบวนการที่ไม่สามารถรอได้ และหนี้เงินกู้ที่ครบกำหนดจะต้องสามารถชำระได้ถูกต้อง ครบถ้วน ตรงกำหนดเวลา ตามเงื่อนไขของตราสารหนี้และสัญญาเงินกู้ในกรณีฉุกเฉิน โดยในกระบวนการชำระหนี้จะมีส่วนงานหลักที่รับผิดชอบ ๒ ส่วน คือ ส่วนบริหารการชำระหนี้ในประเทศ และส่วนบริหารการชำระหนี้ต่างประเทศ ดังนั้น เพื่อให้แผนความต่อเนื่อง (BCP) ของ สบช. สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและเกิดประสิทธิภาพ จะต้องจัดตั้งทีมงานบริหารความต่อเนื่อง (BCP Team) ขึ้น โดย BCP Team ประกอบด้วย

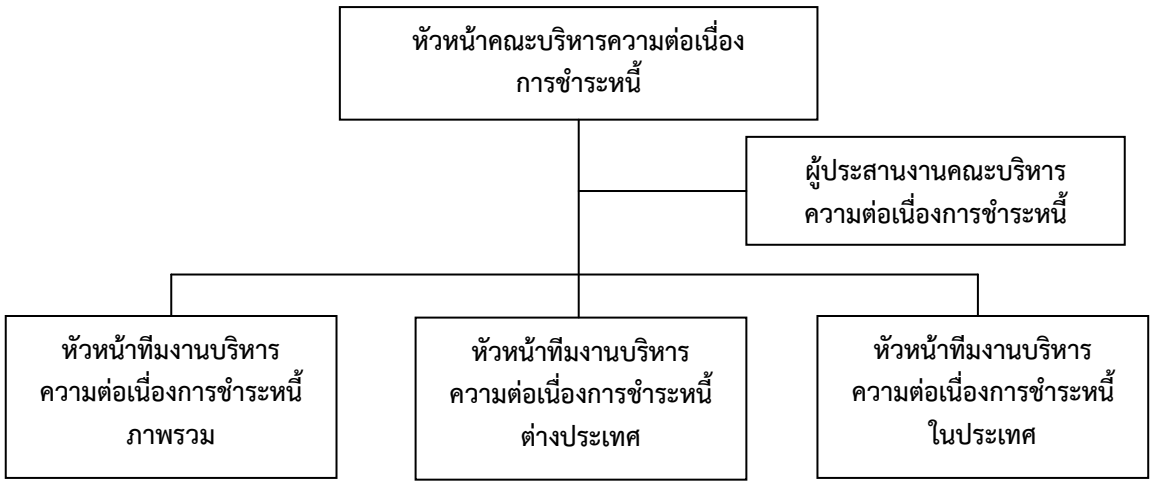
๑) หัวหน้าคณะบริหารความต่อเนื่องการชำระหนี้ (ผู้อำนวยการสำนักบริหารการชำระหนี้)

๒) หัวหน้าทีมงานบริหารความต่อเนื่อง (ผู้เชี่ยวชาญด้านบริหารการชำระหนี้ ผู้อำนวยการส่วนบริหารการชำระหนี้ในประเทศ และผู้อำนวยการส่วนบริหารการชำระหนี้ต่างประเทศ)

๓) ผู้ประสานงานคณะบริหารความต่อเนื่อง (ผู้อำนวยการส่วนบริหารการชำระหนี้ในประเทศ)

โดยกำหนดโครงสร้างคณะบริหารความต่อเนื่องการชำระหนี้ ดังปรากฏตามรูปภาพที่ ๓

รูปภาพที่ ๓ โครงสร้างคณะบริหารความต่อเนื่องการชำระหนี้



ทั้งนี้ แต่ละตำแหน่งจะต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงาน และกู้คืนเหตุการณ์ฉุกเฉินในส่วนงานของตนเอง ให้สามารถบริหารความต่อเนื่องและกลับสู่สภาวะปกติได้โดยเร็ว ตามบทบาทหน้าที่ที่กำหนดไว้ของทีมงานบริหารความต่อเนื่อง (BCP Team) และในกรณีที่บุคลากรหลักไม่สามารถปฏิบัติหน้าที่ได้ ให้บุคลากรสำรองเป็นผู้รับผิดชอบทำหน้าที่ในบทบาทของบุคลากรหลักไปก่อน จนกว่าจะมีการมอบหมายจากหัวหน้าคณะบริหารความต่อเนื่องการชำระหนี้ โดยทีมงานบริหารความต่อเนื่องการชำระหนี้ ประกอบด้วยบุคลากรหลักและบุคลากรสำรอง ดังปรากฏตามตารางที่ ๕

ตารางที่ ๕ รายชื่อบุคลากรและบทบาทของทีมงานบริหารความต่อเนื่อง (BCP Team)

บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ	เบอร์มือถือ		ชื่อ	เบอร์มือถือ
นายเอด วิบูลย์เจริญ (ผู้อำนวยการสำนัก)	๐๘๙-๘๑๑๕๑๒๕	หัวหน้าคณะบริหารความต่อเนื่องการชำระหนี้	นายเอกราช เขื่อนขันธ์สถิตย์ (ผู้เชี่ยวชาญเฉพาะด้านบริหารการชำระหนี้)	๐๘๕-๑๒๑-๒๕๑๖
นายอัคนิทัต บุญโญ (ผู้อำนวยการส่วนบริหารการชำระหนี้ในประเทศ)	๐๘๙-๑๖๒๗๐๐๒	ผู้ประสานงานคณะบริหารความต่อเนื่องการชำระหนี้	นางสาวจันทิรา ตรงรัศมีทอง (เศรษฐกรชำนาญการ)	๐๘๑-๖๖๒๗๕๘๙
นายเอกราช เขื่อนขันธ์สถิตย์ (ผู้เชี่ยวชาญเฉพาะด้านบริหารการชำระหนี้)	๐๘๕-๑๒๑๒๕๑๖	หัวหน้าทีมงานบริหารความต่อเนื่องการชำระหนี้ภาพรวม	นางสาวชิดชไม ไมตรี (ผู้อำนวยการส่วนบริหารการชำระหนี้ต่างประเทศ)	๐๘๑-๑๗๐๖๗๐๗
นางสาวชิดชไม ไมตรี (ผู้อำนวยการส่วนบริหารการชำระหนี้ต่างประเทศ)	๐๘๑-๑๗๐๖๗๐๗	หัวหน้าทีมงานบริหารความต่อเนื่องการชำระหนี้ต่างประเทศ	นางสาวทิพรัตน์ ไชยศรี (นักวิชาการคลังชำนาญการ) นางศรินยา โพธิ์ขำ (เศรษฐกรปฏิบัติการ)	๐๘๖-๘๙๓๗๗๙๓ ๐๘๑-๙๑๘๘๓๙๒
นายอัคนิทัต บุญโญ (ผู้อำนวยการส่วนบริหารการชำระหนี้ในประเทศ)	๐๘๙-๑๖๒๗๐๐๒	หัวหน้าทีมงานบริหารความต่อเนื่องการชำระหนี้ในประเทศ	นางสาวจันทิรา ตรงรัศมีทอง (เศรษฐกรชำนาญการ) นายวรวุฒิ แซ่ลิ่ม (เศรษฐกรชำนาญการ)	๐๘๑-๖๖๒๗๕๘๙ ๐๘๖-๕๒๔๗๕๓๗

๓.๒.๒ กลยุทธ์ความต่อเนื่อง (Business Continuity Strategy)

กลยุทธ์ความต่อเนื่อง เป็นแนวทางในการจัดหาและบริหารจัดการทรัพยากรให้มีความพร้อมเมื่อเกิดสภาวะวิกฤต ซึ่งพิจารณาทรัพยากรใน ๕ ด้าน ดังนี้

ทรัพยากร		กลยุทธ์ความต่อเนื่อง
	**อาคาร/สถานที่ปฏิบัติงานสำรอง**	● กำหนดให้ใช้พื้นที่ปฏิบัติงานสำรอง ณ สำนักงานบริหารหนี้สาธารณะ ชั้น ๓๒ อาคารทิปโก้ โดยประสานงานและเตรียมความพร้อมไว้ล่วงหน้า
	**วัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ**	● กำหนดให้มีการจัดสรรอุปกรณ์สำรองที่มีอยู่ภายใน สบน. ก่อน แล้วจึงสรรหาจากภายนอก เช่น หน่วยงานในสังกัดกระทรวงการคลัง หรือบริษัทตัวแทนจำหน่ายอุปกรณ์เครื่องมือ เป็นต้น ● กำหนดให้จัดหาคอมพิวเตอร์สำรองที่มีคุณลักษณะเหมาะสมกับการใช้งาน พร้อมอุปกรณ์ที่สามารถเชื่อมโยงกับระบบเทคโนโลยีสารสนเทศของ สบน. และกรมบัญชีกลางได้ (GFMIS, GFMIS-TR) ● กรณีที่คอมพิวเตอร์สำรองมีไม่เพียงพอ กำหนดให้ใช้คอมพิวเตอร์พกพา (Laptop/Notebook) ของเจ้าหน้าที่หรือของ สบน. ได้ชั่วคราว หากมีความจำเป็นเร่งด่วนในช่วงระหว่างการจัดหา
	**เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ**	● ประสานงานกับหน่วยงานด้านเทคโนโลยี เพื่อจัดเตรียมและให้มีระบบงานเทคโนโลยี หรือระบบสารสนเทศสำรอง ● กรณีที่สามารถเดินทางมายังกระทรวงการคลังได้ ให้ประสานงานกับกรมบัญชีกลางเพื่อขอใช้ระบบ GFMIS ในการทำรายการชำระหนี้

ทรัพยากร		กลยุทธ์ความต่อเนื่อง
	**บุคลากรหลัก**	● กำหนดให้ใช้บุคลากรหลักและบุคลากรสำรองภายในหน่วยงาน ทำงานทดแทนกันได้ในสภาวะวิกฤต ● ในกรณีที่บุคลากรไม่เพียงพอหรือขาดแคลนกำหนดให้สามารถขอยืมตัวบุคลากรจากสำนัก/ศูนย์/กลุ่ม ภายใน สบน. เพื่อให้ช่วยปฏิบัติงานชั่วคราว
	**คู่ค้า/ผู้ให้บริการ/ ผู้มีส่วนได้ส่วนเสียที่สำคัญ**	● ประสานงานอย่างใกล้ชิดกับกรมบัญชีกลาง ธนาคารแห่งประเทศไทย และธนาคารพาณิชย์อย่างใกล้ชิดเพื่อดำเนินการชำระหนี้ รวมทั้งติดตามผลการชำระหนี้ ● ประสานงานกับการไฟฟ้านครหลวง เพื่อให้สามารถจ่ายไฟฟ้าได้ตามปกติ ● ประสานงานกับการประปานครหลวงเพื่อให้สามารถจ่ายน้ำประปาได้ตามปกติ ● ในปัจจุบัน สบน. กำหนดให้มีผู้บริการเชื่อมโยงระบบเครือข่ายอินเตอร์เน็ต จำนวน ๑ ราย คือ บริษัท True โดยสามารถเชื่อมโยงเครือข่ายระบบอินเตอร์เน็ตได้ใน ๒ รูปแบบ คือ Lease Line และ ADSL และหากระบบใดระบบหนึ่งไม่สามารถให้บริการได้ ระบบจะปรับเปลี่ยนไปยังอีกระบบหนึ่งได้ภายใน ๒ ชั่วโมง

๓.๒.๓ ผลกระทบทางธุรกิจ (Business Impact Analysis)

จากการวิเคราะห์ผลกระทบทางธุรกิจในบทที่ ๒ ตารางที่ ๒.๙ ปรากฏว่า กระบวนการกำหนดกลยุทธ์และแนวทางการบริหารงบชำระหนี้ของรัฐบาล รวมทั้งดำเนินการชำระหนี้ เป็นกระบวนการที่มีผลกระทบต่อองค์กรในระดับที่สูง โดยเฉพาะการชำระหนี้ ที่มีความจำเป็นต้องดำเนินงานให้แล้วเสร็จภายในระยะเวลาอันสั้น และจะต้องชำระหนี้ให้ถูกต้อง ครบถ้วน และตรงตามกำหนดเวลา สำหรับกระบวนการอื่นๆ ที่ได้มีการประเมินแล้วอาจไม่ได้รับผลกระทบในระดับสูงถึงสูงมาก หรือมีความยืดหยุ่นให้สามารถชะลอการดำเนินงานและให้บริการได้ ให้ผู้บริหารของหน่วยงานหรือกลุ่มงานประเมินความจำเป็นและเหมาะสม ทั้งนี้ หากมีความจำเป็น ก็ให้ปฏิบัติตามแนวทางการบริหารความต่อเนื่องเช่นเดียวกันกับกระบวนการหลัก

๓.๒.๔ กระบวนการแจ้งเหตุฉุกเฉิน Call Tree

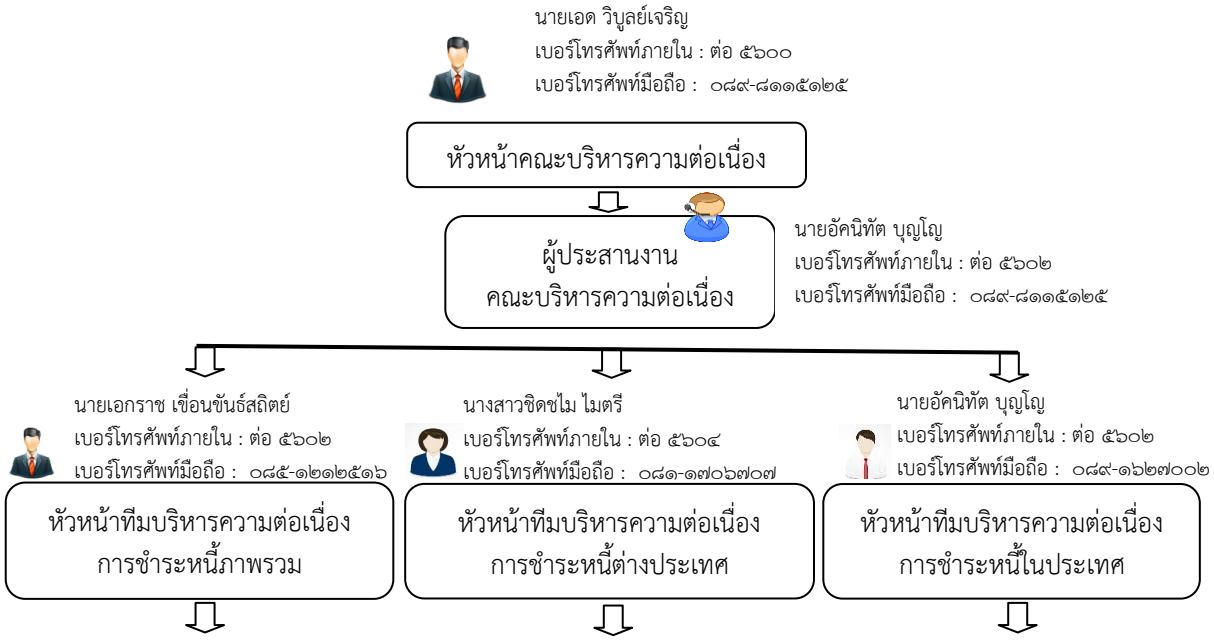
กระบวนการ Call Tree คือ กระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกในคณะบริหารความต่อเนื่องและทีมงานบริหารความต่อเนื่องที่เกี่ยวข้อง ตามผังรายชื่อทางโทรศัพท์ โดยมีวัตถุประสงค์เพื่อการบริหารจัดการขั้นตอนในการติดต่อเจ้าหน้าที่ ภายหลังจากมีการประกาศเหตุการณ์ฉุกเฉินหรือภาวะวิกฤตของหน่วยงาน

จุดเริ่มต้นของกระบวนการ Call Tree จะเริ่มจากหัวหน้าคณะบริหารความต่อเนื่องแจ้งให้ผู้ประสานงานคณะบริหารความต่อเนื่อง โดยผู้ประสานงานฯ จะแจ้งให้หัวหน้าทีมบริหารความต่อเนื่องรับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่อง ตามสายงานการบังคับบัญชาของแต่ละสายงานเพื่อรับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่องของหน่วยงานที่ได้รับผลกระทบ ตามรายชื่อและช่องทางติดต่อสื่อสารที่ได้ระบุไว้ ดังปรากฏตามรูปที่ ๔

ในกรณีที่ไม่สามารถติดต่อหัวหน้าทีมได้ ให้ติดต่อไปยังบุคลากรสำรอง โดยพิจารณา ดังต่อไปนี้

- ถ้าเหตุการณ์เกิดขึ้นในเวลาทำการ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์ของหน่วยงานเป็นช่องทางแรก
- ถ้าเหตุการณ์เกิดขึ้นนอกเวลาทำการหรือสถานที่ปฏิบัติงานหลักได้รับผลกระทบ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์มือถือเป็นช่องทางแรก
- ถ้าสามารถติดต่อบุคลากรหลักได้ให้แจ้งข้อมูลแก่บุคลากรหลักของหน่วยงานทราบ ดังต่อไปนี้:
  - สรุปสถานการณ์ของเหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่อง
  - เวลาและสถานที่สำหรับการนัดประชุมเร่งด่วนของหน่วยงาน สำหรับผู้บริหารของหน่วยงานและทีมงานบริหารความต่อเนื่อง
  - ขั้นตอนการปฏิบัติงาน เพื่อบริหารความต่อเนื่องต่อไป เช่น กระบวนการ และวิธีการชำระหนี้ในกรณีฉุกเฉิน สถานที่รวมพลในกรณีที่มีการย้ายสถานที่ทำการ เป็นต้น

รูปภาพที่ ๔ กระบวนการแจ้งเหตุ Call Tree



ทีมบริหารความต่อเนื่องการชำระหนี้ภาพรวม	ทีมบริหารความต่อเนื่องการชำระหนี้ต่างประเทศ	ทีมบริหารความต่อเนื่องการชำระหนี้ในประเทศ
นางสาวชิดชไม ไมตรี ๐๘๑-๑๗๐๖๗๐๗	นางสาววิมลมาส ไตรสุวรรณ ๐๘๑-๔๒๒๖๑๙๙๙	นางสาววงเดือน สิทธิเดชศักดิ์ ๐๘๙-๑๓๐๙๖๔๙
	นางสาวทิพย์รัตน์ ไชยศรี ๐๘๖-๘๙๓๗๗๙๓	นางสาวจันทิรา ตรงรัศมีทอง ๐๘๑-๖๖๒๗๕๘๙
	นางศรินยา โพธิ์ขำ ๐๘๑-๙๑๘๘๓๙๒	นายวรวุฒิ แซ่ลิ้ม ๐๘๖-๕๒๔๗๕๓๗
		นายณัฐพล ตั้งวัฒนา ๐๘๐-๙๑๐๙๗๘๙
		นางสาวปุญพัฒน์ พลเดช ๐๘๓-๓๗๓๔๖๓๔

ภายหลังจากได้รับการตอบรับจากบุคลากรหลักครบถ้วนตามผังการติดต่อ (Call Tree) หัวหน้าหน่วยงาน มีหน้าที่โทรกลับไปแจ้งยังผู้ประสานงานคณะบริหารความต่อเนื่อง เพื่อรวบรวมสรุปความพร้อมของหน่วยงานในการบริหารความต่อเนื่อง รวมทั้งความปลอดภัยในชีวิตและทรัพย์สินของหน่วยงาน และเจ้าหน้าที่ทั้งหมดในหน่วยงาน ทีมบริหารความต่อเนื่องมีหน้าที่ในการปรับปรุงข้อมูลสำหรับการติดต่อให้เป็นปัจจุบันอยู่ตลอดเวลา เพื่อให้กระบวนการติดต่อเจ้าหน้าที่ภายในหน่วยงานสามารถดำเนินได้อย่างต่อเนื่องและสำเร็จลุล่วงภายในระยะเวลาที่คาดหวัง ในกรณีที่ เกิดเหตุการณ์ฉุกเฉินและมีการประกาศใช้แผนความต่อเนื่อง

๓.๒.๕ ขั้นตอนในการบริหารความต่อเนื่องและกอบกู้ประบวนการ

การตอบสนองต่อเหตุการณ์ทันที ภายใน ๒๔ ชั่วโมง

ในการปฏิบัติการใดๆ ให้บุคลากรของหน่วยงาน คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นอย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
● ติดตาม สอบถาม และประเมินสถานการณ์ฉุกเฉิน และระยะเวลาในการกอบกู้สถานการณ์กับผู้บริหารของ สบน.	หัวหน้าคณะบริหารความต่อเนื่อง	☐
● แจ้งเหตุฉุกเฉิน วิกฤติ ตามกระบวนการ Call Tree ให้กับบุคลากรหลักในหน่วยงาน	ผู้ประสานงานคณะบริหารความต่อเนื่อง	☐
● จัดประชุมคณะบริหารความต่อเนื่อง เพื่อรับทราบและประเมินความเสียหาย ผลกระทบต่อการดำเนินงานและให้บริการ และทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง ● รับทราบและพิจารณาอนุมัติกระบวนงาน งานที่มีความเร่งด่วน และส่งผลกระทบอย่างสูงจำเป็นต้องดำเนินงานหรือปฏิบัติด้วยมือ (Manual Processing) โดยหากเป็นการชำระหนี้ที่ครบกำหนดให้ปฏิบัติตามแนวทางการชำระหนี้ในภาวะฉุกเฉิน (เอกสารภาคผนวก ๑)	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● แจ้งสรุปสถานการณ์และการประเมินทรัพยากรที่ครอบคลุม - จำนวนและรายชื่อบุคลากรที่ได้รับบาดเจ็บ/เสียชีวิต - ความเสียหายและผลกระทบต่อการดำเนินงานและให้บริการ - ทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง - กระบวนงาน/งานที่มีความเร่งด่วน และส่งผลกระทบอย่างสูงจำเป็นต้องดำเนินงานทันที	หัวหน้าคณะบริหารความต่อเนื่อง	☐
● สื่อสารและทำความเข้าใจเกี่ยวกับสถานการณ์ฉุกเฉินที่เกิดขึ้น และแนวทางในการปฏิบัติงานให้แก่บุคลากรในหน่วยงานทราบโดยทั่วถึง	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● พิจารณาและอนุมัติการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง - สถานที่ปฏิบัติงานสำรอง - วัสดุอุปกรณ์ที่สำคัญ - เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ - บุคลากรหลัก - คู่ค้า/ผู้ให้บริการที่สำคัญ	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● รายงานความคืบหน้าให้แก่หัวหน้าคณะบริหารความต่อเนื่องของ สบช. ทราบอย่างสม่ำเสมอ หรือตามที่ได้มีการกำหนดไว้	หัวหน้าทีมบริหารความต่อเนื่อง	☐

หมายเหตุ : ถ้าเหตุการณ์ฉุกเฉินนั้นเกินขีดความสามารถที่หน่วยงานจะรับได้ ให้ติดต่อประสานงานไปยังผู้อำนวยการสำนักงานบริหารหนี้สาธารณะหรือผู้บริหารที่ได้รับมอบอำนาจให้ช่วยเหลือต่อไป

การตอบสนองต่อเหตุการณ์ในระยะแรก ภายใน ๗ วัน

ในการปฏิบัติการใดๆ ให้บุคลากรของหน่วยงาน คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นอย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
● ติดตามสถานภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบและประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● พิจารณาแนวทางการชำระหนี้ - การชำระหนี้ในประเทศที่ครบกำหนด สามารถดำเนินการตั้งเบิกหนี้เงินกู้ที่ครบกำหนดชำระได้ล่วงหน้าก่อนถึงวันที่ครบกำหนดผ่านระบบ GFMIS ได้ โดยสามารถตั้งเบิกล่วงหน้าได้ประมาณ ๑ เดือน - การชำระหนี้ต่างประเทศที่ครบกำหนด สามารถดำเนินการซื้อเงินตราต่างประเทศได้ล่วงหน้า โดยใช้วิธีการซื้อเงินในแบบ Forward แทนการซื้อเงินแบบ spot ซึ่งการดำเนินการดังกล่าวสามารถซื้อเงินล่วงหน้าได้ประมาณ ๑ เดือน	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● พิจารณาและอนุมัติการจัดหาทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ - สถานที่ปฏิบัติงานสำรอง - วัสดุอุปกรณ์ที่สำคัญ - เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ - บุคลากรหลัก - คู่ค้า/ผู้ให้บริการที่สำคัญ	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● รายงานความคืบหน้าให้แก่หัวหน้าคณะบริหารความต่อเนื่องของ สบช. และหน่วยงานกำกับดูแล อย่างสม่ำเสมอ หรือตามที่ได้มีการกำหนดไว้	หัวหน้าทีมบริหารความต่อเนื่อง	☐

หมายเหตุ : ถ้าเหตุการณ์ฉุกเฉินนั้นเกินขีดความสามารถที่หน่วยงานจะรับได้ ให้ติดต่อประสานงานไปยังผู้อำนวยการสำนักงานบริหารหนี้สาธารณะหรือผู้บริหารที่ได้รับมอบอำนาจให้ช่วยเหลือต่อไป

การตอบสนองต่อเหตุการณ์ฉุกเฉินและกู้คืนกระบวนการปฏิบัติงาน ในระยะเวลาเกิน ๗ วัน

ในการปฏิบัติการใดๆ ให้บุคลากรของหน่วยงาน คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นอย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
● ติดตามสถานภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบและประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● พิจารณาแนวทางการชำระหนี้ - การชำระหนี้ในประเทศที่ครบกำหนด สามารถดำเนินการตั้งเบิกหนี้เงินกู้ที่ครบกำหนดชำระได้ล่วงหน้าก่อนถึงวันที่ครบกำหนดผ่านระบบ GFMIS ได้ โดยสามารถตั้งเบิกล่วงหน้าได้ประมาณ ๑ เดือน - การชำระหนี้ต่างประเทศที่ครบกำหนด สามารถดำเนินการซื้อเงินตราต่างประเทศได้ล่วงหน้า โดยใช้วิธีการซื้อเงินในแบบ Forward แทนการซื้อเงินแบบ spot ซึ่งการดำเนินการดังกล่าวสามารถซื้อเงินล่วงหน้าได้ประมาณ ๑ เดือน	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● พิจารณาและอนุมัติการจัดหาทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติและสามารถปฏิบัติงานได้ในระยะยาว - สถานที่ปฏิบัติงานสำรอง หรือพิจารณาจัดหาสถานที่ปฏิบัติงานที่รองรับการปฏิบัติงานในสภาวะปกติของหน่วยงานได้ - วัสดุอุปกรณ์ที่สำคัญ หรือพิจารณาจัดซื้อจัดจ้างวัสดุอุปกรณ์และเครื่องมือที่ได้รับความเสียหาย - เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ ประสานกับหน่วยงานด้านเทคโนโลยีสารสนเทศเพื่อกู้คืนข้อมูลหรือวางระบบเทคโนโลยีสารสนเทศให้สามารถทำงานได้ตามปกติ - การสำรวจบุคลากรที่ได้รับผลกระทบและไม่สามารถกลับมาปฏิบัติงาน เพื่อสรรหาบุคลากรทดแทนชั่วคราว - คู่ค้า/ผู้ให้บริการที่สำคัญ	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องของหน่วยงาน	☐
● รายงานความคืบหน้าให้แก่หัวหน้าคณะบริหารความต่อเนื่องของ สบช. อย่างสม่ำเสมอ หรือตามที่ได้มีการกำหนดไว้	หัวหน้าทีมบริหารความต่อเนื่อง	☐

หมายเหตุ : ถ้าเหตุการณ์ฉุกเฉินนั้นเกินขีดความสามารถที่หน่วยงานจะรับได้ ให้ติดต่อประสานงานไปยังผู้อำนวยการสำนักงานบริหารหนี้สาธารณะหรือผู้บริหารที่ได้รับมอบอำนาจให้ช่วยเหลือต่อไป

๓.๒.๖ การติดตามและรายงายผล

การติดตามและรายงานผลการดำเนินการตามแผน ให้หัวหน้าคณะบริหารความต่อเนื่องรายงานผลการดำเนินงานให้ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะหรือผู้บริหารระดับสูงที่กำกับดูแลทราบเป็นระยะๆ อย่างต่อเนื่อง

ภาคผนวก ๑

ประกาศสำนักงานบริหารหนี้สาธารณะ
เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๕๕

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

“นโยบาย” หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมอิเล็กทรอนิกส์ที่สำนักงานบริหารหนี้สาธารณะ จัดไว้ให้บริการประชาชน ซึ่งสำนักประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานที่ต้องเกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับประกาศแนบท้ายพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

“แนวปฏิบัติ” หมายถึง ขั้นตอนวิธีการที่สำนักงานได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของเจ้าหน้าที่และผู้ปฏิบัติงานของสำนักที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมีจุดมุ่งหมายเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์นั้น มีวิธีการที่มั่นคงปลอดภัย

“ผู้ใช้งาน” หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบของสำนักงาน ผู้บริหารองค์กร ผู้รับบริการ ผู้รับจ้างทำของ และผู้ใช้งานที่ใช้บริการระบบเทคโนโลยีสารสนเทศของสำนักงาน

“บัญชีผู้ใช้งาน” หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาต เช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“สินทรัพย์ (asset)” หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

“สินทรัพย์คอมพิวเตอร์” หมายความว่า โปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“สารสนเทศ” หมายถึง ข้อมูลในรูปแบบต่างๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจ หรือใช้ประโยชน์ต่างๆ ตามภารกิจของสำนักงาน

“เครือข่าย” หมายความว่า ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ ๒ เครื่องขึ้นไปเข้าด้วยกัน เพื่อสะดวกต่อการร่วมใช้ข้อมูล โปรแกรม หรือเครื่องพิมพ์ และอำนวยความสะดวกในการติดต่อแลกเปลี่ยนข้อมูลระหว่างเครื่องได้ตลอดเวลา

“ความมั่นคงปลอดภัยด้านสารสนเทศ” (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)” หมายความว่า

กรณีที่ ๑ คือ เหตุการณ์ที่เกิดขึ้นแล้วกับระบบคอมพิวเตอร์และเครือข่ายของสำนักงาน

กรณีที่ ๒ คือ เหตุการณ์ที่เป็นจุดอ่อนหรือสงสัยว่าจะเป็นจุดอ่อน

ทั้งสองกรณีสามารถสร้างความเสียหายให้กับองค์กรได้ในลักษณะใดลักษณะหนึ่ง ซึ่งอาจส่งผลให้

- เกิดการหยุดชะงักต่อกระบวนงานที่สำคัญ (เช่น ระบบ GFMIS-TR เป็นต้น)
- เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของสำนักงาน
- เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่สำนักงาน กำหนดไว้
- เกิดภาพลักษณ์ที่ไม่ดีต่อสำนักงานหรือทำให้สูญเสียชื่อเสียง (เช่น การไปโพสต์ข้อความพาดพิงถึงสำนักงาน ในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของสำนักงาน)

ตัวอย่างของเหตุการณ์ที่เกิดขึ้นแล้ว ได้แก่

- การพบการแพร่ระบาดของโปรแกรมไม่ประสงค์ดีในเครือข่ายของสำนักงาน
- การพบจุดอ่อนในซอฟต์แวร์ ระบบงาน หรือฮาร์ดแวร์ที่ใช้งาน
- การแจ้งเตือนของระบบป้องกันการบุกรุกตามที่สำนักงานได้กำหนดไว้
- ระบบสารสนเทศซึ่งให้บริการแก่ประชาชนถูกบุกรุกทางเครือข่าย
- การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
- การใช้ทรัพยากรขององค์กรผิดวัตถุประสงค์ (เช่น การใช้เครือข่ายขององค์กรเพื่อกระทำการที่ขัดต่อ พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อ

กระทำการที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญา เพื่อทำการส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ เป็นต้น)

- ระบบ อุปกรณ์ ฮาร์ดแวร์ หรือทรัพย์สินสารสนเทศอื่นๆ ถูกขโมย
- การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่ายของสำนักงาน
- การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย หรือเหตุการณ์อื่นๆ ที่เป็นการละเมิดระเบียบฉบับนี้

ตัวอย่างของเหตุการณ์ที่เป็นจุดอ่อน ได้แก่

- ระบบงานมีช่องทางอื่นในการเข้าสู่ระบบได้โดยไม่ผ่านการพิสูจน์ตัวตนตามปกติ
- บุคคลภายนอกเดินตามพนักงานเข้าห้องสำนักงานโดยไม่มีการแลกบัตร
- บุคคลภายนอกไม่ได้ลงทะเบียนก่อนเข้าเครือข่ายสำนักงาน
- พนักงานไม่มีการระบุตัวตนก่อนที่จะเข้าถึงเครือข่ายสำนักงาน

ทั้งเหตุการณ์ที่เกิดขึ้นแล้วหรือเหตุการณ์ที่เป็นจุดอ่อน จำเป็นต้องได้รับรายงานจากผู้ใช้งานที่พบเหตุ เพื่อให้มีการจัดการกับเหตุการณ์เหล่านั้นอย่างเหมาะสม ได้ผล และทันกาล

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident)” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“สำนักงาน” หมายความว่า สำนักงานบริหารหนี้สาธารณะ

ข้อ ๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน แบ่งเป็น ๒ ส่วน ได้แก่

ส่วนที่ ๑ แนวนโยบาย

ส่วนที่ ๒ แนวปฏิบัติ

รายละเอียดภายในของทั้งสองส่วน ประกอบด้วยเนื้อหาสาระสำคัญในประเด็นต่อไปนี้

(๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ตามเป้าหมายครอบคลุม ๔ เรื่อง ดังนี้

- การเข้าถึงสารสนเทศ
- การเข้าถึงระบบเครือข่าย
- การเข้าถึงระบบปฏิบัติการ
- การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(๒) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

(๔) การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ต้องมีแนวปฏิบัติในการบริหารจัดการสิทธิ ในแต่ละกลุ่ม รวมถึงการระงับสิทธิ

ข้อ ๓ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานให้เป็นไปตามที่กำหนดไว้ในแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำนักงาน พ.ศ.๒๕๕๕

ข้อ ๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบและควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ และดำเนินการตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานอย่างน้อยปีละ ๑ ครั้ง โดยกลุ่มตรวจสอบภายในของสำนักงาน

ข้อ ๕ สร้างความรู้ความเข้าใจให้กับผู้ใช้งานของสำนักงาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการ

(๑) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์สำนักงานและบอร์ดประชาสัมพันธ์ให้แก่ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

(๒) จัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ ๖ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พ.ร.บ.ข้อมูลข่าวสารของ ทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ หรือข้อกำหนดอื่นๆ ที่ได้ประกาศใช้ทดแทน

ข้อ ๗ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๘ ให้ศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้รวมถึงกำหนดให้มีปฏิบัติที่ชัดเจนและให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๔ มิถุนายน พ.ศ. ๒๕๕๕

(นายทวี ไอศูรย์พิศาลศิริ)
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
รองผู้อำนวยการสำนักงานบริหารหนี้สาธารณะปฏิบัติราชการแทน
ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง
พ.ศ. ๒๕๕๕

ศูนย์เทคโนโลยีสารสนเทศ
สำนักงานบริหารหนี้สาธารณะ
มิถุนายน ๒๕๕๕

คำนำ

ตามที่สำนักงานบริหารหนี้สาธารณะ ได้จัดทำแนวนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มีแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศในการให้บริการอิเล็กทรอนิกส์ภาครัฐ และเพื่อให้สอดคล้องตาม พ.ร.ฎ. ธุรกรรมอิเล็กทรอนิกส์ทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๓

ศูนย์เทคโนโลยีสารสนเทศจึงจัดทำแนวปฏิบัติที่มีความสอดคล้องกับแนวนโยบายดังกล่าว โดยเนื้อหาสาระโดยสังเขป ได้แก่ การอนุญาตการเข้าถึงสารสนเทศที่มีระดับชั้นความลับต่างกัน วิธีการเข้าถึงระบบงานตามหน้าที่รับผิดชอบ วิธีการป้องกันการเข้าถึงทางเครือข่าย การบริหารจัดการสิทธิการเข้าถึง เป็นต้น รวมถึงการระบุหน้าที่รับผิดชอบของผู้ใช้งาน ผู้ปฏิบัติงานที่เกี่ยวข้อง ทั้งในด้านของผู้ที่ทำหน้าที่เป็นผู้ดูแลระบบ ผู้ดูแลเครือข่าย ผู้ดูแลฐานข้อมูล เป็นต้น

แนวปฏิบัติต่างๆ เหล่านี้จึงเป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติเพื่อให้เกิดความมั่นคงปลอดภัยในการให้บริการต่างๆ ตามภารกิจของสำนักงานผ่านการทำธุรกรรมอิเล็กทรอนิกส์ เพื่อสร้างความเชื่อมั่นให้กับประชาชนผู้ใช้บริการและสร้างความน่าเชื่อถือให้กับองค์กรต่อไป

แนวปฏิบัตินี้ จึงแบ่งเป็นหมวดเพื่อให้ง่ายต่อการอ้างอิงไปปฏิบัติ ประกอบด้วย

หมวด ๑. แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

หมวด ๒. แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึง

หมวด ๓. แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

หมวด ๔. แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

หมวด ๕. แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบ/ผู้ดูแลเครือข่าย

หมวด ๖. แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

หมวด ๗. แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

หมวด ๘. แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

หมวด ๙. แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

หมวด ๑๐. แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ

หมวด ๑๑. แนวปฏิบัติในการเผยแพร่ข้อมูลสาธารณะ

สารบัญ

หมวด ๑

แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

ข้อ ๑. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานดังนี้

(๑) ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ตนต้องใช้งานได้ก็ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบข้อมูล และ/หรือ ผู้รับผิดชอบระบบงาน ตามความจำเป็นต่อการใช้งานแล้วเท่านั้น

(๒) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบกล่าวคือในการขออนุญาตเข้าระบบงานนั้น ผู้ใช้จะต้องมีการทำเป็นบันทึกและกรอกแบบเอกสารที่สำนักงานกำหนดเพื่อขออนุญาตเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน จากนั้น ผู้ดูแลระบบจะสร้างบัญชีสำหรับการเข้าถึงโดยอนุญาตเฉพาะในส่วนที่จำเป็นและโดยคำนึงถึงประเภทข้อมูล และชั้นความลับ

(๓) ผู้ดูแลระบบ ต้องกำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้ หากผู้ใช้งานใส่รหัสผ่านเข้าระบบผิด ๓ ครั้ง จนกว่าจะยื่นเรื่องพร้อมหลักฐานแสดงความเป็นตัวตนต่อเจ้าหน้าที่ดูแลระบบ เพื่อขอรหัสใหม่อีกครั้ง

(๔) ผู้ดูแลระบบ ต้องกำหนดให้การ Log-in เพื่อเข้าใช้ระบบงานใดๆ จะต้องมีการตรวจจับการเปิดระบบงานไว้ เมื่อไม่มีการใช้งาน จะทำการ Log-out ระบบให้อัตโนมัติ ในระยะเวลาที่เหมาะสม

(๕) ผู้รับผิดชอบข้อมูลและผู้รับผิดชอบระบบงาน ต้องอนุญาตให้ผู้ใช้งานเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

(๖) กำหนดระยะเวลาการเข้าถึงระบบสารสนเทศของสำนักงาน ดังนี้

(๖.๑) ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานภายนอก ๒๔ ชั่วโมง

(๖.๒) ระบบงานภายในสำนักงาน (Back office) สำหรับผู้ใช้งานภายใน ๘.๓๐ - ๒๐.๐๐ น.

ข้อ ๒. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องจัดการรักษาความปลอดภัยทางกายภาพ (physical security management) ดังนี้

(๑) กำหนดระดับความสำคัญของพื้นที่ หรือจำแนกพื้นที่ที่ใช้งานกับพื้นที่ที่มีการควบคุม

(๒) ดำเนินการทดสอบระบบควบคุมการเข้าถึงพื้นที่ทางกายภาพเพื่อตรวจสอบยังใช้งานได้ตามปกติหรือไม่

(๓) ผู้ปฏิบัติงานควรปิดประตูและหน้าต่างให้ล็อคอยู่เสมอ

ข้อ ๓. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องจัดการควบคุมการเข้า-ออกพื้นที่ควบคุม เช่น ศูนย์คอมพิวเตอร์ของสำนักงาน ดังนี้

(๑) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาเยือน (visitors)

(๒) ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญสำหรับจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๓) จัดให้ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของสำนักงาน โดยบุคคลภายนอกและควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๔) จัดสื่อประชาสัมพันธ์เพื่อสร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๕) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๖) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๗) มีการพิสูจน์ตัวตน เช่น การแสดงบัตรผ่าน การใช้บัตรแถบแม่เหล็ก การใช้สแกนลายนิ้วมือ เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะในศูนย์สารสนเทศกลาง (data center)

(๘) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญโดยเฉพาะศูนย์สารสนเทศกลาง (data center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๙) บุคคลภายนอก เช่น เจ้าหน้าที่บริษัท, นักศึกษาฝึกงานหรือผู้ได้รับการว่าจ้างอื่นๆ ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

(๑๐) ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

(๑๑) ควรจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๒) จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

ข้อ ๔. ผู้รับผิดชอบระบบสารสนเทศ ต้องกำหนดการจัดวางและการป้องกันฮาร์ดแวร์และอุปกรณ์ต่างๆ ดังนี้

(๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงของบุคคลภายนอก

(๒) ระบบงานที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่มีความมั่นคงปลอดภัยเพียงพอ

(๓) ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในศูนย์คอมพิวเตอร์ (data center) ของสำนักงาน

(๔) ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติหรือไม่

ข้อ ๕. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องกำหนดระบบและอุปกรณ์สนับสนุนการทำงาน ดังนี้

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

(๑.๑) ระบบสำรองกระแสไฟฟ้า (UPS)

(๑.๒) ระบบระบายอากาศ

(๑.๓) ระบบปรับอากาศ และควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องกำหนดและควบคุมการเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ ดังนี้

(๑) เครือข่ายของสำนักงาน ในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้นั้น ต้องให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณเพื่อทำให้เกิดความเสียหายและป้องกันสัตว์ต่างๆ กัดสาย เช่น หนู เป็นต้น

(๒) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๓) จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๔) ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

ข้อ ๗. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องกำหนดการบำรุงรักษาอุปกรณ์ ดังนี้

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วย

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องควบคุมการนำอุปกรณ์คอมพิวเตอร์ของสำนักงาน ออกนอกหน่วยงาน ดังนี้

(๑) ให้มีการขออนุญาตก่อนนำสิ่งอุปกรณ์หรือทรัพย์สินออกนอกหน่วย

(๒) บันทึกข้อมูลการนำสิ่งอุปกรณ์ของสำนักงาน ออกนอกหน่วยเพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องจัดการป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์คอมพิวเตอร์ของสำนักงาน ออกไปใช้งานนอกสถานที่

(๒) ห้ามผู้ใช้งานละทิ้งอุปกรณ์คอมพิวเตอร์ของสำนักงาน ไว้โดยลำพังในที่สาธารณะ

(๓) ให้ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์คอมพิวเตอร์ของสำนักงาน เสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องควบคุมการจำหน่ายอุปกรณ์คอมพิวเตอร์หรือการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

(๑) ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะแทงจำหน่ายอุปกรณ์ดังกล่าว (ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูล ในหมวด ๓ แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ข้อ ๑ (๑๒)

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวด ๒
แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึงของผู้รับผิดชอบระบบ

ข้อ ๑. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน ดังนี้

(๑) การลงทะเบียนพนักงานใหม่ พนักงานหรือผู้ปฏิบัติงานใหม่ ต้องปฏิบัติตามขั้นตอนลงทะเบียนที่สำนักงาน กำหนดขึ้น เพื่อให้มีสิทธิในการใช้งานระบบสารสนเทศ ตามความจำเป็นรวมทั้งปฏิบัติตามขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในสำนักงาน เป็นต้น

(๒) กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบสารสนเทศที่ให้บริการประชาชนภายนอก ระบบรับ-ส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบระบบอินเทอร์เน็ต (Internet)

เครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

(๓) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณาเพื่อขอความเห็นชอบและอนุมัติจากผู้บังคับบัญชา

(๓.๑) ควบคุมการใช้งานอย่างเข้มงวด โดยเฉพาะระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงและมีความสำคัญสูง

(๓.๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓.๓) มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

ข้อ ๒. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (user account) และรหัสผ่านของเจ้าหน้าที่ดังนี้

(๑) กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน

(๒) ไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

(๓) จัดเก็บข้อมูลการลงทะเบียนของผู้ที่ร้องขอใช้ระบบไว้เพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบในภายหลัง

(๔) ทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้งเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางดังนี้

(๔.๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงานภายในของสำนักงาน

(๔.๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานภายในนั้นเพื่อดำเนินการทบทวนว่ามีรายชื่อที่ออกไปแล้ว หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

(๔.๓) ผู้บังคับบัญชาของหน่วยงานภายในแจ้งกลับว่ามีรายชื่อใดที่ต้องดำเนินการแก้ไขให้ถูกต้อง

(๔.๔) ดำเนินการแก้ไขข้อมูลสิทธิให้ถูกต้องตามที่ได้รับแจ้ง

ข้อ ๓. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องจัดให้มีการพิสูจน์ตัวตนเพื่อเข้าใช้ระบบงานสำคัญสำหรับผู้ใช้ที่อยู่ภายนอกดังนี้

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบของสำนักงาน ต้องผ่านการพิสูจน์ตัวตนจากระบบของสำนักงาน โดยมีแนวทางปฏิบัติดังนี้

(๑) การแสดงตัวตนด้วยชื่อบัญชีผู้ใช้งาน

(๒) การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน

(๓) การเข้าสู่ระบบงานสำคัญของสำนักงาน ผ่านเครือข่ายอินเทอร์เน็ตนั้น จะมีการตรวจสอบ

ผู้ใช้งานด้วย

(๔) การเข้าสู่ระบบงานสำคัญของสำนักงาน จากระยะไกลเพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

(๕) ในการใช้งานระบบสารสนเทศ เมื่อมีการว่างเว้นจากการใช้งานเป็นเวลา 5 นาที ให้ทำการยกเลิกโปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

ข้อ ๔. ผู้รับผิดชอบระบบสารสนเทศ ต้องกำหนดวิธีการใช้รหัสผ่านให้มีความมั่นคงปลอดภัย ดังนี้

๔.๑ การบริหารจัดการรหัสผ่าน มีมาตรการและการควบคุม ดังนี้

(๔.๑.๑) กำหนดให้ต้องเปลี่ยนรหัสผ่านทุก 6 เดือน

(๔.๑.๒) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๖ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔.๑.๓) กรณีผู้ใช้งานเปลี่ยนหน้าที่ความรับผิดชอบหรือลาออก จะต้องเปลี่ยนหรือถอดถอนสิทธินั้นทันทีที่ได้รับแจ้ง

(๔.๑.๔) กำหนดให้การเข้าใช้งานระบบครั้งแรกมีการโต้ตอบด้วยการยืนยันตัวตนและเปลี่ยนรหัสผ่านเพื่อเพิ่มความปลอดภัย

๔.๒ การใช้รหัสผ่าน มีมาตรการให้ผู้ใช้งานต้องใช้ด้วยความระมัดระวัง ดังนี้

(๔.๒.๑) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๔.๒.๒) ไม่ใช้โปรแกรมสำนักงานคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password)

(๔.๒.๓) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๔.๒.๔) กำหนดรหัสผ่านให้ยากต่อการเดา

(๔.๒.๕) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๔.๒.๖) กรณีผู้ใช้งานลาออกหรือเปลี่ยนหน้าที่ความรับผิดชอบ จะต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบทันที

ข้อ ๕. การใช้รหัสผ่านให้ปลอดภัย มีมาตรการในการปฏิบัติ ดังนี้

(๑) แสดงกระบวนการมอบอำนาจหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒) มีการกำหนดสิทธิการเข้าถึงตามความจำเป็น

(๓) มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

(๔) มีวิธีเลือกการใช้รหัสผ่านและการใช้งานรหัสผ่านที่มีคุณภาพ

หมวด ๓

แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ข้อ ๑. ผู้บังคับบัญชาหน่วยงานภายในสำนักงาน ต้องจัดให้มีวิธีการกำหนดประเภทข้อมูลและจัดการ การเข้าถึงข้อมูลตามระดับชั้นความลับ ซึ่งเบื้องต้นสำนักงาน ใช้แนวทางตามพ.ร.บ.ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบที่เกี่ยวข้อง ในการกำหนดชั้นความลับของข้อมูล จึงกำหนดให้มีแนวทางปฏิบัติ ดังนี้

(๑) ผู้ใช้งาน ต้องแบ่งประเภทของข้อมูลและชั้นความลับของข้อมูล ตามที่ศูนย์เทคโนโลยีสารสนเทศได้กำหนดชั้นความลับของข้อมูลเป็น ๔ ระดับ ดังนี้

- ลับ (Top secret/Secret/Confidential)
- ใช้ภายในเท่านั้น (Internal use)
- ส่วนบุคคล (Personal)
- เปิดเผยได้ (Public)

(๒) ผู้ใช้งาน พิจารณาจากองค์ประกอบต่อไปนี้เพื่อเป็นแนวทางกำหนดชั้นความลับของข้อมูล

(ก) ความสำคัญของเนื้อหา เช่น เนื้อหาของข้อมูลนั้นมีความสำคัญต่อความสำเร็จของงานตามภารกิจของ สำนักงาน มากน้อยเพียงใด หากมีความสำคัญสูง ข้อมูลนั้นจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือลับ เป็นต้น

(ข) แหล่งที่มาของข้อมูล เช่น หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับ ชั้นความลับก็จะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับก็จะเป็นประเภทเปิดเผยได้ เป็นต้น

(ค) วิธีการนำไปใช้ประโยชน์ เช่น หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบด้านการเงินของสำนักงาน ดังนั้นข้อมูลนี้จะอยู่ในประเภทลับ เป็นต้น

(ง) จำนวนบุคคลที่ควรรับทราบ เช่น หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้ เป็นต้น

(จ) ผลกระทบหากมีการเปิดเผย เช่น หากข้อมูลนั้นถูกเปิดเผย จะมีผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการเงิน ด้านการปฏิบัติตามกฎระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้นข้อมูลจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือลับ เป็นต้น

(ฉ) หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่อง เช่น ข้อมูลสำคัญหรือข้อมูลลับที่มาจากเจ้าของเรื่องใดจะต้องคงชั้นความลับไว้เช่นเดิม การนำไปใช้งานควรขออนุญาตจากผู้ที่เป็นเจ้าของเรื่องก่อน เป็นต้น

(๓) สำหรับข้อมูลในชั้นความลับ “ลับ” ได้แก่ ลับ ลับมาก หรือลับที่สุดเจ้าของข้อมูลพิจารณาเกณฑ์ต่อไปนี้เพิ่มเติมเพื่อกำหนดชั้นความลับที่ถูกต้อง

- ลับที่สุด หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะ

ก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

- ลับมาก หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

- ลับ หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

(๔) การดำเนินการกับข้อมูลลับ (ถ้ามี) เจ้าของข้อมูลลับฯ ดำเนินการจัดทำทะเบียนข้อมูลลับที่ตนเองดูแลหรือรับผิดชอบ ซึ่งมีรายละเอียดประกอบด้วย

- ชื่อของข้อมูล
- ระดับชั้นความลับและระดับชั้นการเข้าถึง
- ชื่อเจ้าของข้อมูลลับ
- หน่วยงานภายในที่สามารถเข้าถึงได้
- หน่วยงานภายนอกที่อนุญาตให้เข้าถึงได้
- สถานที่ที่จัดเก็บข้อมูล
- ช่องทางการเข้าถึง
- ระยะเวลาการเก็บรักษาข้อมูล
- ระยะเวลาที่ได้เข้าถึง

(๕) พิจารณาปรับชั้นความลับ (ปรับลด เพิ่ม หรือยกเลิกชั้นความลับ) ตามความจำเป็น ปรับปรุงทะเบียนข้อมูลลับให้ถูกต้องและทันสมัย และต้องแจ้งให้หน่วยงานที่สามารถเข้าถึงข้อมูลหรือที่ได้รับการแจกจ่ายทราบด้วยทุกครั้ง เพื่อแก้ไขชั้นความลับให้ถูกต้อง

(๖) ในการจัดทำหรือจัดเตรียมข้อมูลลับ ให้ผู้ใช้งาน ปฏิบัติดังนี้

(๖.๑) จัดทำหรือจัดเตรียมข้อมูลในสถานที่ที่ปลอดภัย เช่น จัดทำในสำนักงาน ไม่ทำในสถานที่ที่เป็นสาธารณะซึ่งบุคคลภายนอกสามารถเห็นข้อมูลที่จัดทำได้ และจำกัดผู้ที่เป็นผู้ดำเนินการจัดทำ

(๖.๒) ในการจัดทำข้อมูลลับซึ่งใช้กระดาษหรือวัสดุชั่วคราว เช่น กระดาษร่าง กระดาษคาร์บอน ต้องทำลายกระดาษหรือวัสดุนั้นทันทีที่จัดทำเสร็จเรียบร้อย ถ้าเป็นการจัดทำโดยใช้เครื่องคอมพิวเตอร์ จะต้องทำการลบ หรือทำลายสื่อบันทึกข้อมูลจนไม่สามารถนำไปใช้ประโยชน์ได้ (ดูวิธีการทำลายใน ตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูล) หากไม่ทำลาย ต้องเก็บรักษาไว้ในสถานที่ที่ปลอดภัย

(๖.๓) จัดทำข้อมูลโดยแสดงเลขที่หน้าของจำนวนหน้าทั้งหมดไว้ในทุกหน้าของข้อมูลลับ และแสดงไว้ในส่วนที่สามารถเห็นได้ชัดเจน เช่น มุมขวาด้านบนของเอกสาร (การบันทึกเลขหน้ามีจุดประสงค์เพื่อให้ทราบว่าข้อมูลลับนั้นเป็นหน้าใดของจำนวนทั้งหมดกี่หน้า หากมีการสูญหายไปหน้าใดหน้าหนึ่ง จะได้ทราบและสามารถติดตามหาผู้ละเมิดและหาทางลดหรือแก้ไขความเสียหายที่เกิดขึ้นได้)

(๗) ในการแสดงชั้นความลับบนข้อมูลลับ ให้ปฏิบัติดังนี้

(๗.๑) แสดงชั้นความลับของข้อมูล (ซึ่งประกอบด้วย “ลับ” “ลับมาก” หรือ “ลับ

ที่สุด") ให้ปรากฏเห็นอย่างเด่นชัดทั้งข้อมูลที่มีสภาพเป็นกระดาษ ไฟล์อิเล็กทรอนิกส์ เทป External Harddisk, Flash Drive แผ่น CD/DVD หรือข้อมูลลับที่อยู่ในรูปแบบอื่นๆ

(๗.๒) แสดงชั้นความลับบนเอกสารลับในทุกหน้าของเอกสารให้ปรากฏเห็นอย่างเด่นชัด

(๘) ในการทำสำเนาหรือแจกจ่ายข้อมูลลับ ให้ปฏิบัติดังนี้

(๘.๑) ทำสำเนาหรือแจกจ่ายข้อมูลลับให้แก่ผู้รับปลายทางซึ่งเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลตามที่ระบุไว้ในทะเบียนข้อมูลลับ หรือสามารถแจกจ่ายให้ได้ตามความจำเป็นในการเข้าถึงข้อมูลนั้น

(๘.๒) แจ้งให้หน่วยงานภายนอกที่อนุญาตให้เข้าถึงข้อมูลลับนั้นได้ ว่าไม่อนุญาตให้ทำสำเนาเพิ่มเติม เว้นเสียแต่ได้รับอนุญาตจากผู้มีอำนาจลงนามอนุญาตก่อน

(๙) ในการเก็บรักษาเอกสารลับ ให้ปฏิบัติดังนี้

(๙.๑) จัดเก็บเอกสารลับไว้ในแฟ้มข้อมูลลับ และนำไปเก็บไว้ในตู้เก็บเอกสารลับโดยแยกเก็บเป็นแต่ละเรื่องหรือแต่ละหัวข้อ

(๙.๒) ไม่จัดเก็บเอกสารลับร่วมกับเอกสารที่อยู่ในชั้นความลับอื่นๆ เช่น ข้อมูลใช้ภายในเท่านั้น ข้อมูลส่วนบุคคล หรือข้อมูลที่เปิดเผยได้

(๙.๓) จัดเก็บแฟ้มข้อมูลลับไว้ในตู้และปิดล็อคด้วยกุญแจที่มั่นคง

(๑๐) ในการยืมหรือขอเข้าถึงข้อมูลลับ ให้ปฏิบัติดังนี้

(๑๐.๑) เมื่อมีการขอยืมหรือขอเข้าถึงข้อมูลลับโดยผู้อื่นที่ไม่ได้เป็นผู้มีสิทธิในการเข้าถึงข้อมูลตามทะเบียนข้อมูลลับ ให้ หัวหน้าหน่วยงานภายใน เป็นผู้พิจารณาตรวจสอบคุณสมบัติของผู้ยืมหรือขอเข้าถึงก่อนว่าเป็นผู้มีอำนาจหน้าที่ที่เกี่ยวข้องหรือไม่ หรือมีความจำเป็นในการเข้าถึงข้อมูลนั้นหรือไม่ พร้อมทั้งต้องทำบันทึกหลักฐานการยืมหรือการขอเข้าถึงข้อมูลนั้นด้วย แจ้งให้ผู้ยืมหรือขอเข้าถึงทราบว่าห้ามทำการสำเนาเพิ่มเติม

(๑๐.๒) เมื่อหมดความจำเป็นในการใช้งานแล้ว หัวหน้าหน่วยงานภายใน กำหนดให้ผู้ขอยืมจัดส่งข้อมูลนั้นกลับคืนมาโดยทันที สำหรับกรณีการเข้าถึงระบบเทคโนโลยีสารสนเทศ ให้ทำการยกเลิกบัญชีผู้ใช้งานที่ขอเข้าถึงข้อมูลลับโดยทันที

(๑๑) ในการส่งเอกสารลับ ให้ปฏิบัติตามระเบียบการส่งเอกสารลับของสำนักงาน ตรวจสอบการแสดงที่อยู่อีเมล์ของผู้รับปลายทางให้ถูกต้อง ก่อนจัดส่งไฟล์นั้นไปยังผู้รับเพื่อป้องกันการส่งผิดตัวบุคคล

(๑๒) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ

ประเภทสื่อบันทึกข้อมูล	**วิธีการทำลายสื่อและข้อมูล**
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย ส่วนในกรณีที่ต้องการนำกลับมาใช้ใหม่ให้ใช้โปรแกรม Active@killdisk โดยโปรแกรมจะลบข้อมูลจนไม่สามารถกู้คืนมาได้ด้วยการเขียนทับตลอดจนทั่วอุปกรณ์
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย

ฮาร์ดดิสก์	ใช้วิธีการทุบหรือบดให้เสียหาย ส่วนในกรณีที่ต้องการนำกลับมาใช้ใหม่ให้ใช้โปรแกรม Active@killdisk โดยโปรแกรมจะลบข้อมูลจนไม่สามารถกู้คืนมาได้ด้วยการเขียนทับตลอดจนทั่วอุปกรณ์

(๑๓) ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้

(๑๓.๑) จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึงและควรแสดงชั้นความลับบนไฟล์ข้อมูลลับ เช่น การทำลายน้ำและแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

(๑๓.๒) การสำเนาข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล

(๑๓.๓) ระมัดระวังการกระจาย หรือแจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับของสำนักงานบริหารหนี้สาธารณะไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

(๑๓.๔) ผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ต้องตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน

(๑๓.๕) ห้ามผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูง ส่งข้อมูลดังกล่าวไปทางไปรษณีย์ เว้นแต่จะได้ใช้วิธีเข้ารหัสที่สำนักงานบริหารหนี้สาธารณะกำหนดไว้

(๑๓.๖) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัยและไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์

(๑๓.๗) ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายของสำนักงานเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

(๑๓.๘) ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

(๑๓.๙) ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมสำนักงานแก้ไขช่องโหว่เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

(๑๓.๑๐) ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

(๑๓.๑๑) ต้องทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

หมวด ๔
แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

ข้อ ๑. การใช้คอมพิวเตอร์ของ สำนักงาน ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

(๑) ห้ามใช้คอมพิวเตอร์จนกว่าจะได้รับการอนุมัติให้ใช้ได้โดยผ่านการลงทะเบียน ตามแบบท้ายระเบียบนี้ (แบบ ทส.๑) และต้องสแกนไวรัสก่อนการใช้งานทุกครั้ง

(๒) ต้องตรวจสอบว่าโปรแกรมสำนักงานป้องกันไวรัสยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ หากพบว่าโปรแกรมดังกล่าวทำงานผิดปกติให้รีบแจ้งศูนย์เทคโนโลยีสารสนเทศเพื่อดำเนินการแก้ไขโดยเร็ว

(๓) คอมพิวเตอร์ที่ใช้ในสำนักงาน ให้ติดตั้งโปรแกรมมาตรฐานตามที่กำหนดไว้ท้ายระเบียบนี้ การเปลี่ยนแปลงหรือติดตั้งโปรแกรมเพิ่มเติมต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานภายใน หรือผู้ที่ได้รับมอบหมาย

ความในวรรคหนึ่ง ไม่ใช้บังคับแก่การเปลี่ยนแปลงหรือการติดตั้งโปรแกรมสำนักงานเพิ่มเติมเพื่อทดลองการใช้งานซึ่งดำเนินการโดยศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับการว่าจ้างให้มาจัดทำหรือดูแลระบบเทคโนโลยีสารสนเทศของสำนักงานบริหารหนี้สาธารณะ

(๔) ห้ามติดตั้งโปรแกรมสำนักงานคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ เพื่อให้บุคคลภายนอกสามารถใช้งานเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของสำนักงานบริหารหนี้สาธารณะได้

(๕) ห้ามติดตั้งโปรแกรมสำนักงานคอมพิวเตอร์เพิ่มเติมนอกจากโปรแกรมสำนักงานมาตรฐานที่กำหนดไว้ท้ายประกาศนี้

(๖) ห้ามติดตั้งโปรแกรมสำนักงานคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

(๗) ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟท์แวร์ที่มีลิขสิทธิ์ถูกต้องของสำนักงานบริหารหนี้สาธารณะ

(๘) ห้ามติดตั้งโปรแกรมสำนักงานคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย

(๙) ต้องระมัดระวังการใช้งานและดูแลคอมพิวเตอร์ รวมทั้งระบบเครือข่ายตามที่วิญญูชนทั่วไปจะพึงปฏิบัติ

(๑๐) เอกสารหรือข้อมูลต่าง ๆ ไม่ว่าจะอยู่ในรูปแบบใดก็ตามที่ได้มีการกำหนดเงื่อนไขการใช้งานไว้ต้องใช้งานด้วยความระมัดระวัง และต้องปฏิบัติตามเงื่อนไขอย่างเคร่งครัด เพื่อป้องกันมิให้เกิดการละเมิดตามกฎหมาย

(๑๑) ต้องลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากคอมพิวเตอร์เพื่อประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

(๑๒) ต้องออกจากระบบ (Log off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์ รวมทั้งปิด

คอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

(๑๓) การติดตั้งโปรแกรมเพิ่มเติมต้องเป็นโปรแกรมที่มีลิขสิทธิและใช้ในการทำงานซึ่งต้องได้รับอนุญาตจากผู้มีอำนาจ โดยผ่านการลงทะเบียนตามแบบท้ายระเบียบนี้ (แบบ ศทส. ๐๒)

(๑๔) การนำคอมพิวเตอร์ส่วนตัวมาใช้กับระบบเครือข่ายของสำนักงานต้องได้รับการตรวจสอบและอนุญาตจากศูนย์เทคโนโลยีสารสนเทศโดยผ่านการลงทะเบียนตามแบบท้ายระเบียบนี้ (แบบ ศทส. ๐๓) สำหรับบุคคลภายใน และ (แบบ ศทส. ๐๔) สำหรับบุคคลภายนอก โดยต้องสแกนไวรัสก่อนการใช้งานทุกครั้ง

ข้อ ๒. การใช้คอมพิวเตอร์แบบพกพาของสำนักงานนอกจากต้องปฏิบัติตามที่กำหนดไว้ในข้างต้นแล้ว ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

(๑) ต้องตรวจสอบคอมพิวเตอร์แบบพกพาที่นำไปใช้ว่าได้ติดตั้งโปรแกรมกรมสำนักงานมาตรฐาน ที่กำหนดไว้ท้ายระเบียบนี้แล้วหรือไม่ หากพบว่ายังไม่ได้ติดตั้งให้แจ้งสำนักงานบริหารหนี้สาธารณะเพื่อขอรับการติดตั้งก่อนการใช้งาน

(๒) ต้องระมัดระวังไม่ให้บุคคลภายนอกมองเห็นหรือคัดลอกข้อมูลจากคอมพิวเตอร์แบบพกพาที่นำไปใช้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้คอมพิวเตอร์แบบพกพาแล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบของหน่วยงานทันที ทั้งนี้ให้เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนตรวจสอบสภาพความพร้อมในการใช้งานของคอมพิวเตอร์ที่รับคืนไว้ดังกล่าวด้วย

ข้อ ๓. ในกรณีที่เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนคอมพิวเตอร์แบบพกพาตรวจพบความเสียหายให้แจ้งผู้ส่งคืน ผู้บังคับบัญชา และสำนักงานบริหารหนี้สาธารณะทราบโดยเร็ว และหากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทเลินเล่ออย่างร้ายแรงของผู้นำไปใช้ ต้องให้ผู้นำไปใช้รับผิดชอบต่อความเสียหายที่เกิดขึ้นดังกล่าว

ข้อ ๔. การใช้คอมพิวเตอร์เพื่อประโยชน์ส่วนตัวของเจ้าหน้าที่ให้ใช้ได้ภายในสถานที่ที่สำนักงานบริหารหนี้สาธารณะจัดไว้เป็นการเฉพาะเท่านั้น

ข้อ ๕. การเข้าถึงระบบงานเทคโนโลยีสารสนเทศ เจ้าหน้าที่ใช้งานต้องปฏิบัติตาม ข้อกำหนดดังต่อไปนี้

(๑) กรอกแบบเพื่อขออนุมัติใช้งานระบบงานและนำเสนอต่อผู้บังคับบัญชาเพื่อขออนุมัติโดยผ่านการลงทะเบียนตามแบบท้ายระเบียบนี้ (แบบ ศทส. ๐๑)

(๒) ต้องไม่เข้าถึงระบบงานอื่นที่ตนไม่ได้รับอนุมัติให้ใช้งาน

(๓) ต้องออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

ข้อ ๖. การใช้งานอินเทอร์เน็ต ผู้ใช้งานต้องปฏิบัติตาม ข้อกำหนด ดังต่อไปนี้

(๑) ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

(ก) การพนัน

(ข) การประมูล

(ค) วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และ พระมหากษัตริย์

(ง) ลามก อนาจาร

(จ) อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

(๒) ห้ามใช้โปรแกรมสำนักงานสนทนา

(๓) ห้ามเล่น หรือดาวน์โหลดเกมส์ ภาพยนตร์ เพลง หรือสื่อลามกอนาจารผ่านทางอินเตอร์เน็ต

(๔) ห้ามใช้อินเทอร์เน็ตเพื่อส่ง กระจาย หรือ แจกจ่าย ดังต่อไปนี้

(ก) สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของ

(ข) ข้อมูลประเภทสื่อลามกอนาจาร

(ค) ข้อมูลที่เป็นความลับของสำนักงานบริหารหนี้สาธารณะ ไปยังบุคคลที่ไม่ได้รับอนุญาต

(ง) ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

(๕) ห้ามใช้งานข้อมูลที่ได้รับโดยผ่านทางอินเตอร์เน็ตที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของข้อมูลนั้น

(๖) ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ หรือชื่อเสียงของสำนักงาน

ข้อ ๗. การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องปฏิบัติตาม ข้อกำหนด ดังต่อไปนี้

(๑) ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ตามที่สำนักงานบริหารหนี้สาธารณะ กำหนดเท่านั้น

(๒) ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ที่สำนักงานบริหารหนี้สาธารณะกำหนดให้ลงทะเบียนตามเว็บไซต์ที่ไม่เกี่ยวข้องกับงานของสำนักงานบริหารหนี้สาธารณะ

(๓) ห้ามดู ใช้ หรือเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาต

(๔) ห้ามปลอมแปลง รับหรือส่งจดหมายอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาต

(๕) ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้

(ก) จดหมายขยะ (Spam Mail)

(ข) จดหมายลูกโซ่ (Chain Letter)

(ค) จดหมายที่ละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

(ง) จดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

(๖) ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีขนาดใหญ่เกินกว่าที่สำนักงาน กำหนด

(๗) ต้องระบุชื่อเรื่อง (Subject) และชื่อผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

(๘) ต้องใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับจดหมายอิเล็กทรอนิกส์เท่าที่มีความจำเป็นต้องรับรู้เท่านั้น

(๙) ต้องใช้คำที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์

(๑๐) ต้องสำรองข้อมูลที่อยู่จดหมายอิเล็กทรอนิกส์ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ ๘. ห้ามมิให้เจ้าหน้าที่ที่ใช้ระบบเทคโนโลยีสารสนเทศของสำนักงาน กระทำการในลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้

(๑) กระทำผิดกฎหมายหรือก่อให้เกิดความเสียหายแก่บุคคลอื่นหรือขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือละเมิดทรัพย์สินทางปัญญาของสำนักงานบริหารหนี้สาธารณะและของบุคคลอื่น

(๒) เปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน ทั้งที่เป็นข้อมูลของสำนักงานบริหารหนี้สาธารณะ หรือบุคคลภายนอก

(๓) การเข้าถึงข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาต

(๔) ขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของสำนักงานบริหารหนี้สาธารณะ หรือเจ้าหน้าที่อื่นของสำนักงานบริหารหนี้สาธารณะ

(๕) แสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับสำนักงานบริหารหนี้สาธารณะ ไปยังที่อยู่เว็บ (website) ใดๆ ในลักษณะที่ก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง และก่อให้เกิดความเสียหายแก่สำนักงานบริหารหนี้สาธารณะ

(๖) กระทำการอื่นใดที่อาจขัดต่อการดำเนินงานตามอำนาจหน้าที่ของสำนักงานบริหารหนี้สาธารณะ หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่สำนักงาน

ข้อ ๙. เอกสารที่เป็นความลับหรือมีระดับความสำคัญซึ่งพิมพ์ออกมาจากเครื่องพิมพ์ เจ้าหน้าที่ต้องปฏิบัติให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการ ดังต่อไปนี้

(๑) จัดหมวดหมู่เอกสารที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก

(๒) จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ

(๓) การสำเนาเอกสารที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูง ต้องได้รับอนุญาตจากผู้เป็นเจ้าของ

(๔) ระมัดระวังการกระจาย หรือแจกจ่ายเอกสารที่เป็นความลับของสำนักงานบริหารหนี้สาธารณะไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

(๕) ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน

(๖) ให้ทำลายเอกสารที่เป็นความลับ หรือมีระดับความสำคัญสูงเมื่อหมดความจำเป็นในการใช้งาน

ข้อ ๑๐. การจัดการข้อมูลที่เป็นความลับที่อยู่ในรูปอิเล็กทรอนิกส์ ผู้ใช้งานปฏิบัติตามแนวทางปฏิบัติในการจัดการกับข้อมูลลับในข้อข้างต้น

หมวด ๕
แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบ/ผู้ดูแลเครือข่าย

ข้อ ๑ ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์ ระบบงานสารสนเทศ และระบบเครือข่ายของสำนักงานบริหารหนี้สาธารณะ ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะ

เกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบ (System Administrator) พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าวได้ทันที

ข้อ ๒ ติดตั้งและปรับปรุงโปรแกรมสำนักงานคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

ข้อ ๓ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) ระบบงานสารสนเทศ และระบบเครือข่าย

ข้อ ๔ ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

ข้อ ๕ บริหารจัดการบัญชีผู้ใช้งานและควบคุมการเข้าถึงตามอำนาจหน้าที่เท่านั้น

ข้อ ๖ บริหารจัดการระบบงานสารสนเทศ และระบบเครือข่ายตามอำนาจหน้าที่ที่ตนเองรับผิดชอบเท่านั้น

ข้อ ๗ บริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามอำนาจหน้าที่ที่ตนเองรับผิดชอบเท่านั้น

ข้อ ๘ ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งาน ที่ใช้งานระบบคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่ายโดยไม่มีเหตุผลอันสมควร

ข้อ ๙ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งาน ที่ใช้งานระบบคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่าย โดยไม่มีเหตุผลอันสมควร

ข้อ ๑๐ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สามารถเปิดเผยได้ให้บุคคลอื่นทราบ โดยไม่มีเหตุผลอันสมควร

ข้อ ๑๑ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งานและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วัน นับแต่การใช้บริการสิ้นสุดลง

หมวด ๖
แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

ข้อ ๑. กำหนดมาตรการทางเครือข่ายสื่อสารข้อมูลเพื่อป้องกันข้อมูลในเครือข่าย ระบบงาน หรือบริการต่างๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

(๑) กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

(๒) การปฏิบัติงานขององค์กรจากภายนอกสำนักงานในการเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล จะต้องปฏิบัติ ดังนี้

- ติดต่อศูนย์เทคโนโลยีสารสนเทศเพื่ออธิบายเหตุผลความจำและกำหนดช่วงเวลาที่สิ้นสุดในการใช้งาน และลงทะเบียนเป็นลายลักษณ์อักษร

- ศูนย์เทคโนโลยีสารสนเทศจะกำหนดสิทธิให้เข้าใช้งานเฉพาะระบบที่จำเป็นต้องใช้เท่านั้น

(๓) กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ เช่น เครือข่ายอินเทอร์เน็ต เครือข่ายไร้สาย เป็นต้น

(๔) การเข้าสู่ระบบงานเครือข่ายและสารสนเทศภายใน สำหรับผู้ใช้นอกองค์กร (Guest) ต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง ด้วยการใส่รหัสผ่าน โดยจะต้องทำการลงทะเบียนและขอรับได้ที่ศูนย์เทคโนโลยีสารสนเทศ

(๕) กำหนดข้อปฏิบัติในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์พกพาและโทรศัพท์มือถือ ต้องมีการยืนยันตัวตนในการเข้าใช้งานทุกครั้งด้วยการใช้รหัสผ่าน ที่ออกให้โดยศูนย์เทคโนโลยีสารสนเทศ ซึ่งสิทธิที่ได้จะแตกต่างและมีข้อกำหนดการใช้งานที่จำกัด โดยมีข้อปฏิบัติและหลักเกณฑ์ตามภาคผนวก จ.

(๖) มีการบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

ข้อ ๒. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ผู้รับผิดชอบต้องปฏิบัติตามข้อกำหนด ดังต่อไปนี้

(๑) ผู้ดูแลระบบ ต้องมีการออกแบบแบ่งระบบเครือข่าย (Segregation in networks) ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ ดังนี้ เขตภายใน (Internal Zone) เขตภายนอก (External Zone) เพื่อเป็นการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

(๒) การเข้าสู่ระบบเครือข่ายภายในของสำนักงาน โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาก่อนที่จะสามารถใช้งานได้ในทุกกรณี

(๓) ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายและสารสนเทศที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๔) ผู้ดูแลระบบ ต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน รวมทั้งตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๕) ผู้ดูแลระบบ จัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ใช้งานไปยังเครื่องคอมพิวเตอร์ให้บริการ เช่น ในการเชื่อมต่อเข้าสู่เครื่องคอมพิวเตอร์ให้บริการเพื่อบริหารจัดการระบบ ให้กำหนดเฉพาะชุดไอพีแอดเดรสของผู้ดูแลระบบเท่านั้นที่สามารถเข้าถึงเครื่องคอมพิวเตอร์ให้บริการนั้นได้

(๖) กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่าตัวแปร (Parameter) ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๗) ระบบเครือข่ายทั้งหมดของหน่วยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก

หน่วย ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมสำนักงานในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ เป็นต้น

(๘) มีการติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๙) การเข้าสู่ระบบงานเครือข่ายภายในหน่วย ผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

(๑๐) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของคอมพิวเตอร์ (IP Address) ภายใน (Local) ของระบบงานเครือข่ายภายในของสำนักงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของสำนักงาน ได้โดยง่าย

(๑๑) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๑๒) จัดให้มีการใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๑๓) ผู้ดูแลระบบกำหนดอุปกรณ์บนเครือข่ายเป็น IP Address และแยกตามสำนัก และกลุ่มแต่ละสิทธิของผู้ใช้งาน โดยให้ควบคุมการใช้งานอย่างเหมาะสมและมีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

(๑๔) การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อยกว่า ๓ เดือน หรือไม่ต่ำกว่า ๙๐ วัน

(๑๕) มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

ข้อ ๓. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องจัดการควบคุมการเข้าใช้งานระบบจากภายนอก หน่วยงานที่มีระบบสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งเอาไว้ภายในหน่วยของตนเอง เพื่อดูแลรักษาความปลอดภัยของระบบภายในจากการเข้าถึงระบบจากภายนอกโดยมีแนวทางปฏิบัติ ดังนี้

(๑) การเข้าสู่ระบบจากระยะไกล (remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของสำนักงาน การควบคุมบุคคลที่เข้าสู่ระบบของสำนักงาน จากระยะไกลจึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

(๓) ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสำนักงาน อย่างเพียงพอและต้องได้รับอนุมัติจากผู้บังคับบัญชา

(๔) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

(๕) การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ(Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็นช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

ข้อ ๔. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ผู้รับผิดชอบต้องปฏิบัติตามข้อกำหนด ดังต่อไปนี้

(๑) ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในสำนักงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน

(๒) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

หมวด ๗
แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน

ข้อ ๑. ผู้ใช้งานจะต้องยืนยันตัวตนด้วย User account ของตนเองก่อนเข้าใช้งานระบบปฏิบัติการเครื่องคอมพิวเตอร์ทุกครั้ง

ข้อ ๒. ผู้ใช้งานต้องไม่อนุญาตให้บุคคลอื่นใช้ User account ของตนเองในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

ข้อ ๓. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมสำนักงานถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพโดยอัตโนมัติ หลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๕ นาที

ข้อ ๔. ผู้ใช้งานควรทำการลงบันทึกออก (Log off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์ รวมทั้งปิดคอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

ข้อ ๕. ผู้ใช้งานต้องไม่ใช้โปรแกรมสำนักงานคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password)

ข้อ ๖. ผู้ใช้งานต้องกำหนดรหัสผ่านไม่น้อยกว่า 6 ตัวอักษร โดยไม่นำชื่อหรือนามสกุลของตนเองหรือคำที่ง่ายต่อการคาดเดามาตั้ง และต้องเปลี่ยนรหัสผ่านทุก 6 เดือน

หมวด ๘
แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

ข้อ ๑. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องกำหนดแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล เมื่อมีระบบงานใหม่ เกิดข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่ ควรกำหนดให้ใช้แนวทางการสำรองและกู้คืนข้อมูลดังนี้

(๑) กำหนดระบบงานที่มีความจำเป็นต้องสำรองข้อมูลไว้

(๒) กำหนดผู้รับผิดชอบในการสำรองข้อมูลและกรณีเกิดเหตุฉุกเฉิน (ในภาคผนวก ง)

(๓) กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อยต้องประกอบด้วยข้อมูลในฐานข้อมูลของระบบ ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง

(๔) กำหนดความถี่ในการสำรองข้อมูลของระบบงาน เช่น ระบบงานที่มีการเปลี่ยนแปลงบ่อยควรมีความถี่ในการสำรองข้อมูลมากขึ้น เป็นต้น

(๕) กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์ที่ใช้ในการสำรองข้อมูล

(๖) ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

(๗) ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วน หรือไม่

(๘) ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ หรือไม่

(๙) จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด แผนควรมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๙.๑) การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

(๙.๒) การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๙.๓) การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน

(๙.๔) การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

(๙.๕) การกำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอกเช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่างๆ เช่น เกิดอัคคีภัย การก่อวินาศกรรม เป็นต้น

(๑๐) ให้ทำการปรับปรุงแผนดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

(๑๑) ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนรับมือฯ รวมทั้งเมื่อมีการปรับปรุงแผนใหม่จะต้องจัดประชุมใหม่และแจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

หมวด ๙
แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๑. การแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย (เพิ่มเติมจากประกาศของ ICT)

(๑) ให้เจ้าหน้าที่หรือผู้ปฏิบัติงานแจ้งไปยังศูนย์เทคโนโลยีสารสนเทศทันทีที่พบเห็นเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของสำนักงาน อันได้แก่

(ก) มีโปรแกรมสำนักงานไม่ประสงค์ดีเข้ามาในระบบ

(ข) มีการบุกรุกเข้ามาในเครือข่าย

(ค) ข้อมูลสำคัญเปลี่ยนแปลง หรือสูญหาย

(ง) มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(จ) มีการนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์

(ฉ) มีการใช้ระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์

(ช) พบจุดอ่อนในระบบงาน ซอฟต์แวร์ หรือฮาร์ดแวร์ที่ใช้งาน

(ซ) มีการโจมตีเข้ามาในระบบจนไม่สามารถให้บริการได้

(ฌ) ระบบเทคโนโลยีสารสนเทศชำรุดหรือสูญหาย

(ญ) บุคคลภายนอกเข้าใช้ระบบงานของสำนักงานบริหารหนี้สาธารณะโดยไม่ได้รับอนุญาต

(ฎ) มีการติดตั้งซอฟต์แวร์เพื่อขโมยข้อมูลหรือเข้าถึงข้อมูลในเครือข่าย หรือ

(ฏ) เหตุการณ์อื่นๆ ที่เป็นการละเมิดความมั่นคงปลอดภัยของสำนักงานบริหารหนี้สาธารณะ

(๒) ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชาหรือศูนย์เทคโนโลยีสารสนเทศในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นรวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชาหรือศูนย์เทคโนโลยีสารสนเทศด้วย

ข้อ ๒. ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่พบ ให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

(๑) ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบในระดับใด (สูง กลาง หรือต่ำ)

(๒) แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบตามระดับของผลกระทบ กล่าวคือ รายงานไปสู่ระดับชั้นของผู้บังคับบัญชาที่สูงขึ้นตามลำดับสำหรับเหตุการณ์ที่มีผลกระทบสูงกว่า

(๓) วิเคราะห์และแก้ไขสถานการณ์ตามความจำเป็นกรณีการบุกรุก การโจมตีระบบ หรือระบบได้รับความเสียหาย ประสานงานขอความช่วยเหลือจากผู้รู้ เช่น ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT)

(๔) กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ ให้ผู้ที่ผ่านการอบรมหรือฝึกฝนเป็นผู้ดำเนินการเพื่อป้องกันไม่ให้หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัย และจำกัดการเข้าถึงหลักฐานนั้น

(๕) จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับ

ปานกลาง ขึ้นไปและแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีข้อมูลอย่างน้อยในรายงานดังนี้

(ก) รายละเอียดเหตุการณ์

(ข) วันเวลาที่เกิดขึ้น

(ค) ชื่อผู้แจ้ง/หน่วยงานผู้แจ้ง

(ง) สถานะของเหตุการณ์ในแต่ละช่วงเวลา

(จ) ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา

(ฉ) สาเหตุและวิธีการแก้ไข

(ช) ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

ข้อ ๓. ความรับผิดชอบของผู้บังคับบัญชากรณีที่มีการละเมิดการปฏิบัตินี้

(๑) ให้แจ้งรายงานตามสายการบังคับบัญชาให้หน่วยที่เกี่ยวข้องทราบ

(๒) สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

(๓) พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

(๔) ให้พิจารณาสั่งการลงโทษทางวินัยตามแบบธรรมเนียมทหารหรือดำเนินคดีตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิด และผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้ จะโดยเจตนาหรือไม่เจตนา และการละเมิดนั้นจะเกิดความเสียหายหรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

ข้อ ๔. ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบงานสารสนเทศ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของระบบสารสนเทศดำเนินการ ดังนี้

(๑) พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่างๆ ประมวลลับ หรือรหัสผ่านที่จำเป็นในการใช้ เครือข่ายสื่อสารข้อมูลสารสนเทศมีผลกระทบกระเทือนเสียหายอย่างใดหรือไม่

(๒) ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันทีในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่างๆ ที่เกี่ยวข้องตามที่เห็นสมควร

ข้อ ๕. ความรับผิดชอบของผู้ใช้งานต่อประกาศฉบับนี้มี ดังนี้

(๑) ปฏิบัติตามประกาศนี้อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

(๒) ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบคอมพิวเตอร์และเครือข่ายของสำนักงาน

(๓) ไม่รบกวนหรือแทรกแซงการสื่อสารข้อมูลในเครือข่ายคอมพิวเตอร์ของสำนักงาน

(๔) รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังสำนักงานบริหารหนี้สาธารณะโดยเร็วที่สุด

ข้อ ๖. มีการควบคุมสินทรัพย์ด้านสารสนเทศต่อการเข้าถึงต้องได้รับการอนุญาตโดยปฏิบัติดังนี้

(๑) กำหนดมาตรการป้องกันทรัพย์สินขององค์กร โดยรวบรวมสินทรัพย์ทั้งหมดไว้อย่างเป็นระบบ

(๒) เมื่อใช้งานระบบเสร็จ ต้องออกจากระบบทันที

(๓) ป้องกันไม่ให้ผู้ที่ไม่เกี่ยวข้องใช้อุปกรณ์ด้านสารสนเทศโดยไม่ได้รับอนุญาต

(๔) นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

หมวด ๑๐
แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ

ข้อ ๑. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องควบคุมการพัฒนาหรือจัดหาระบบงานเพื่อให้ระบบงานที่ได้รับมีความมั่นคงปลอดภัยเพียงพอ ดังนี้

(๑) ให้ประเมินความเสี่ยงและระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษร ข้อกำหนดดังกล่าวอย่างน้อยควรมี

(ก) คุณสมบัติของการล็อกอินเข้าสู่ระบบงานที่มีความมั่นคงปลอดภัย ดังนี้

- ไม่มีหรือไม่แสดงฟังก์ชั่น (function) ให้การช่วยเหลือในระหว่างที่ทำการล็อกอิน (login)
- บันทึกความพยายามในการล็อกอินทั้งที่สำเร็จและไม่สำเร็จและแสดงประวัติการล็อกอิน ๓ ครั้งล่าสุด
- ตัดการเชื่อมต่อหลังจากที่ทำการล็อกอินไม่สำเร็จเกินกว่า ๓ ครั้ง
- เมื่อมีการใส่ข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้อง ให้แสดงข้อความรวมๆ เช่น “ข้อมูลการล็อกอิน ไม่ถูกต้อง”
- ให้แสดงข้อความเตือนที่หน้าจอภายหลังจากการล็อกอินเสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ “ระบบนี้เป็นระบบที่เป็นทรัพย์สินของสำนักงานบริหารหนี้สาธารณะ การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้นจึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงานหากมีการตรวจพบและเป็นความผิดจะดำเนินการลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม สำนักงานบริหารหนี้สาธารณะมีสิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้งานใช้ระบบงานนี้โดยไม่ถือว่าเป็นการละเมิดความเป็นส่วนตัว”
- ไม่แสดงรายละเอียดของระบบใดๆ จนกว่าจะล็อกอินสำเร็จ

(ข) การกำหนดหรือตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับเข้าถึงระบบงาน

(ค) การเข้ารหัสข้อมูลสำคัญที่มีการรับส่งระหว่างเครื่องลูกข่ายกับเครื่องคอมพิวเตอร์ให้บริการ

(ง) การเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลลับ ที่จัดเก็บไว้ในฐานข้อมูล

(จ) การตัดและหมดเวลาการใช้งานหลังจากที่ไม่ได้ใช้ระบบงานเกินกว่าระยะเวลาตามที่กำหนดไว้ เช่น ๑๕-๓๐ นาที

(ฉ) การบันทึกบัญชีชื่อผู้ใช้งานที่ล็อกอินเข้าระบบ หมายเลขไอพีแอดเดรส วันเวลาที่เข้าใช้ระบบ ความสำเร็จหรือไม่สำเร็จในการล็อกอินของผู้ใช้งาน

(๒) พัฒนาหรือจัดหาระบบงานให้ได้ตามข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ระบุไว้

(๓) พัฒนาหรือจัดหาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลระบบเพื่อทำการบันทึกและปรับปรุงสิทธิของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

(๔) กำหนดให้มีการจัดทำแผนการทดสอบโดยผู้พัฒนาระบบ นำเสนอแผนดังกล่าวเพื่อ

พิจารณาอนุมัติโดยผู้มีอำนาจ ดำเนินการทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการทดสอบให้ผู้มีอำนาจได้รับทราบเพื่อให้คำแนะนำในการปรับปรุงต่างๆ ที่จำเป็นแผนการทดสอบที่จัดทำอย่างน้อยประกอบด้วย

(ก) แผนการทดสอบ UAT (User Acceptance Test)

(ข) แผนการทดสอบ System Integration Test

(ค) แผนการทดสอบข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Test)

(๕) ไม่อนุญาตการนำข้อมูลสำคัญของสำนักงาน ไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นเสียแต่ได้รับการอนุมัติจากผู้บังคับบัญชาระดับสูงก่อน และหากเป็นไปได้ให้ตัดข้อมูลส่วนที่สำคัญทิ้งไป ให้เหลือเฉพาะส่วนที่เพียงพอต่อการนำไปใช้ในการทดสอบ

ข้อ ๒. ภายหลังจากที่ได้มีการตรวจรับระบบที่พัฒนาขึ้นใหม่แล้ว ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องกำหนดการควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการ

(๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบงานของหน่วยเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

(๒) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานของหน่วย

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

(๔) กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๕) กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบงาน เป็นต้น

(๖) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

(๗) ทำการปรับปรุงไลบรารี่สำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัยและสอดคล้องกับทั้งหมดที่ทำการติดตั้ง

(๘) ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล ซอฟต์แวร์ ค่าคอนฟิกกูเรชัน หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จจะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้

(๙) ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่จะทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

(๑๐) ให้กำหนดแผนการติดตั้งสำหรับระบบงานซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้ง

แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า เช่น แผนการติดตั้งฮาร์ดแวร์ ซอฟต์แวร์ และอื่นๆ

(๑๑) สำหรับซอฟต์แวร์ที่จะทำการติดตั้ง ให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

(๑๒) ให้อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานซอฟต์แวร์ที่จะทำการติดตั้งอย่างเคร่งครัด

(๑๓) สำหรับการติดตั้งซอฟต์แวร์ยูทิลิตี้ (utility software) ต้องตรวจสอบก่อนว่าเป็นซอฟต์แวร์ที่มีการทำงานที่ถูกต้องและเชื่อถือได้

(๑๔) ติดตั้งโปรแกรมสำนักงานแก้ไขช่องโหว่ต่างๆ (patch) ที่เกี่ยวข้องกับระบบงานตามความจำเป็น เช่น โปรแกรมสำนักงานแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมสำนักงานแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

(๑๕) ตรวจสอบและปิดพอร์ต (port) บนระบบงานที่ไม่มีความจำเป็นในการใช้งานก่อนเปิดระบบให้บริการ

(๑๖) จัดให้มีการป้องกันไวรัสคอมพิวเตอร์บนระบบงานที่ทำการติดตั้ง

(๑๗) จำกัดการเชื่อมต่อทางเครือข่ายเพื่ออนุญาตให้เฉพาะกลุ่มผู้ใช้งานที่เกี่ยวข้องเท่านั้นจึงจะสามารถเชื่อมต่อเพื่อเข้าสู่ระบบงานที่ทำการติดตั้งนั้น

ข้อ ๓. ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสำนักงาน ต้องกำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (technical review of applications after operating system changes) ดังนี้

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้าน งบประมาณที่จำเป็นต้องใช้ ในกรณีที่สำนักงาน ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

ข้อ ๔. การจัดซื้อจัดจ้างที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ หรือจัดซื้อเครื่องคอมพิวเตอร์หรือวัสดุอุปกรณ์อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ต้องผ่านการพิจารณากลั่นกรองความเหมาะสม ความคุ้มค่า ประโยชน์ที่จะได้รับและความสอดคล้องกับโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศของสำนักงานบริหารหนี้สาธารณะ จากศูนย์เทคโนโลยีสารสนเทศก่อนนำเสนอผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ หรือผู้ซึ่งผู้อำนวยการสำนักงานบริหารหนี้สาธารณะมอบหมายพิจารณาอนุมัติจัดซื้อจัดจ้าง

หมวด ๑๑
แนวปฏิบัติในการเผยแพร่ข้อมูลสาธารณะ

ข้อ ๑. การเผยแพร่ข้อมูลในความรับผิดชอบของสำนักงานบริหารหนี้สาธารณะสู่สาธารณะโดยผ่านระบบเทคโนโลยีสารสนเทศของสำนักงานบริหารหนี้สาธารณะ หน่วยงานเจ้าของข้อมูลจะต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำออกเผยแพร่ และหากข้อมูลที่นำออกเผยแพร่เกี่ยวข้องกับเรื่องนโยบายจะต้องได้รับความเห็นชอบจากผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ หรือผู้ซึ่งผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ มอบหมายก่อนนำออกเผยแพร่ในกรณีที่ข้อมูลที่นำออกเผยแพร่มีความผิดพลาดและมีความเสียหายเกิดขึ้น โดยความเสียหายนั้นเกิดจากความจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ให้เป็นความรับผิดของเจ้าหน้าที่ที่นำข้อมูลดังกล่าวออกเผยแพร่

ข้อ ๒. การเผยแพร่ข้อมูลสู่สาธารณะโดยผ่านระบบเทคโนโลยีสารสนเทศของสำนักงานบริหารหนี้สาธารณะ ให้ดำเนินการโดยหน่วยงานเจ้าของข้อมูล เว้นแต่กรณีที่ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะหรือผู้ซึ่งผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ มอบหมายได้สั่งการหรือเห็นชอบไว้เป็นอย่างอื่น

ประกาศ ณ วันที่ ๑๔ มิถุนายน พ.ศ. ๒๕๕๕

(นายทวี ไอศูรย์พิศาลศิริ)
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
รองผู้อำนวยการสำนักงานบริหารหนี้สาธารณะปฏิบัติราชการแทน
ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ

ภาคผนวก ก

ขั้นตอนการลงทะเบียนผู้ใช้งานสำนักงานบริหารหนี้สาธารณะ

มีขั้นตอนการปฏิบัติดังนี้

๑. การลงทะเบียนขอเข้าใช้งานเครื่องคอมพิวเตอร์ อีเมล์ และระบบงานในภายในสำนักงานบริหารหนี้สาธารณะ ให้ใช้แบบฟอร์ม ศทส. ๐๑ แบบฟอร์มการขอรับสิทธิ

๒. การลงทะเบียนขอติดตั้งโปรแกรมเพิ่มเติมในเครื่องคอมพิวเตอร์สำนักงานบริหารหนี้สาธารณะ ให้ใช้แบบฟอร์ม ศทส. ๐๒ แบบฟอร์มการขอติดตั้งโปรแกรมเพิ่มในเครื่องคอมพิวเตอร์สำนักงานบริหารหนี้สาธารณะ

๓. การลงทะเบียนขออนุญาตใช้บริการอินเตอร์เน็ตผ่านเครือข่ายสำนักงานบริหารหนี้สาธารณะ สำหรับบุคคลภายในสำนักงานบริหารหนี้สาธารณะ ให้ใช้แบบฟอร์ม ศทส. ๐๓

๔. การลงทะเบียนขออนุญาตใช้บริการอินเตอร์เน็ตผ่านเครือข่ายสำนักงานบริหารหนี้สาธารณะ สำหรับบุคคลภายนอกสำนักงานบริหารหนี้สาธารณะ ให้ใช้แบบฟอร์ม ศทส. ๐๔

ภาคผนวก ข

โปรแกรมสำนักงานมาตรฐานในการใช้งานของสำนักงานบริหารหนี้สาธารณะ

๑. Microsoft Office

๒. Microsoft Windows

๓. Acrobat Reader

๔. Compress and Decompress Program

๕. Anti-virus

ภาคผนวก ค

แผนเตรียมความพร้อมกรณีฉุกเฉิน

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

(IT Contingency Plan)

๑. หลักการและเหตุผล

สำนักงานบริหารหนี้สาธารณะ เป็นหน่วยงานที่มีพันธกิจในการบริหารจัดการหนี้สาธารณะ โดยการวางแผน กำกับ และดำเนินการก่อหนี้ค้ำประกัน และปรับโครงสร้างหนี้ของรัฐบาล หน่วยงานในกำกับดูแลของรัฐ องค์กรปกครองส่วนท้องถิ่น และรัฐวิสาหกิจ ซึ่งรวมทั้งการชำระหนี้ของรัฐบาล และการติดตามและประเมินผลการดำเนินงาน จึงได้มีการนำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงาน เพื่อเพิ่มประสิทธิภาพในการบริหารหนี้สาธารณะของประเทศ ในขณะเดียวกันระบบฐานข้อมูลและสารสนเทศของสำนักงานบริหารหนี้สาธารณะ อาจได้รับความเสียหายจากการให้บริการ ซึ่งได้แก่ ไวรัสคอมพิวเตอร์ การบุกรุก (Hacker) ไฟฟ้าดับ หรือความเสียหายจากการปฏิบัติงานของเจ้าหน้าที่ และปัจจัยอื่นๆ ที่เกี่ยวข้อง ทำให้เกิดผลกระทบต่อการดำเนินงาน

เพื่อเป็นการป้องกันและแก้ไขปัญหาที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศของสำนักงานบริหารหนี้สาธารณะ ศูนย์เทคโนโลยีสารสนเทศจึงต้องมีการจัดทำแผนรองรับการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

๒. วัตถุประสงค์

๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ ให้มีเสถียรภาพและมีความพร้อมใช้งาน

๒.๒ เพื่อลดความเสียหายที่จะอาจเกิดขึ้นแก่ระบบฐานข้อมูลและสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๕ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบฐานข้อมูลและสารสนเทศ

๓. การประเมินสถานการณ์ความเสี่ยง

จากการประเมินสถานการณ์ความเสี่ยงที่อาจเกิดขึ้นและเป็นอันตราย เกิดความเสียหายต่อระบบฐานข้อมูลและสารสนเทศ มีดังนี้

๓.๑ ความเสี่ยงจากไฟฟ้าดับ

๓.๒ ความเสี่ยงจากไฟไหม้

๓.๓ ความเสี่ยงจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ (Hacker)

๓.๔ ความเสี่ยงจากไวรัสคอมพิวเตอร์

๓.๕ ความเสี่ยงอุปกรณ์เครื่องแม่ข่ายชำรุด

๓.๖ ความเสี่ยงการปฏิบัติงานของเจ้าหน้าที่

๓.๗ ความเสี่ยงในกรณีที่ระบบเครือข่ายมีปัญหา

๔. การเตรียมการป้องกันและการแก้ไข

๔.๑ การสำรองข้อมูลและระบบงาน (Back up) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลถูกทำลายหรือถูกบุกรุก หรือไม่สามารถให้บริการได้

๔.๒ การป้องกันไวรัสคอมพิวเตอร์

๔.๒.๑ ติดตั้งโปรแกรมสำนักงานป้องกันและตรวจจับไวรัส (Anti-Virus) ครอบคลุมทุกเครื่องแม่ข่ายและลูกข่าย เพื่อป้องกันความเสียหายของข้อมูล

๔.๒.๒ Update ข้อมูลไวรัสอย่างสม่ำเสมอในทุกวัน โดยโปรแกรมสามารถทำการ Update ไวรัสได้จาก Server Anti-Virus แบบอัตโนมัติ

๔.๒.๓ ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นดิสก์หรือสื่อบันทึกข้อมูลต่างๆ

๔.๒.๔ มีการแนะนำผู้ใช้คอมพิวเตอร์ให้ระวังภัยจากการเปิด File และ E-mail โดย Scan แผ่นก่อนการใช้งาน ไม่เปิดอ่าน E-mail โดยไม่รู้ที่มาและให้ลบเมล์นั้นทิ้งทันที อย่าเปิดอ่าน

๔.๓ การป้องกันและแก้ไขปัญหาที่เกิดจากไฟฟ้าดับ

๔.๓.๑ ติดตั้งอุปกรณ์สำรองไฟฟ้า (Uninterruptible Power Supply, UPS) ที่สำนักงาน สำหรับในกรณีที่ไฟฟ้าดับ ซึ่งสามารถจะสำรองไฟฟ้าไว้ได้ภายในระยะเวลา ๑๕ นาที ซึ่งเพียงพอที่จะสั่งการให้ระบบทำการ Shutdown โดยที่ไม่เกิดความเสียหายต่ออุปกรณ์หรือข้อมูล

๔.๓.๒ ดำเนินการเชื่อมโยงระบบไฟฟ้าสำรองของฝ่ายอาคาร

๔.๔ การป้องกันความเสี่ยงจากไฟไหม้

๔.๔.๑ ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) เพื่อการควบคุมเพลิงเบื้องต้นได้

๔.๔.๒ ในกรณีที่เกิดไฟไหม้ภายในห้อง Server หรือภายในสำนักงาน จะมีการตัดการจ่ายกระแสไฟฟ้าภายในบริเวณใกล้เคียง

๔.๕ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ (Hacker)

๔.๕.๑ ติดตั้งอุปกรณ์ Firewall เพื่อรักษาความปลอดภัยให้กับระบบเครือข่ายและป้องกันการใช้งานระบบเครือข่ายที่ผิดวัตถุประสงค์ ป้องกันการบุกรุกจากภายนอก

๔.๖ การป้องกันอุปกรณ์เครื่องแม่ข่ายชำรุด

๔.๖.๑ มีการใช้ Hard disk แบบ RAID - ๕ เพื่อป้องกันข้อมูลเสียหายให้กับระบบงานต่างๆ

๔.๗ การป้องกันความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่

๔.๗.๑ จัดอบรมเสริมสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศเบื้องต้นในด้าน Hardware และ Software เพื่อลดความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่ให้น้อยที่สุด

๔.๘ การป้องกันความเสี่ยงในกรณีที่ระบบเครือข่ายมีปัญหา

๔.๘.๑ ดำเนินการติดตั้งเส้นทางสำรองสำหรับระบบงานบริการ ให้สามารถบริการได้อย่างต่อเนื่อง

๔.๘.๒ จัดจ้างบริษัทดำเนินการบำรุงรักษาระบบเครือข่าย

๕. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ มีดังนี้

๕.๑ เจ้าหน้าที่ดูแลระบบงานและฐานข้อมูล รับผิดชอบดูแล บำรุงรักษาระบบงานและฐานข้อมูล โดยมีหน้าที่ ตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบงานคอมพิวเตอร์ และการสำรองระบบงาน/ฐานข้อมูล

๕.๒ เจ้าหน้าที่ดูแลระบบเครือข่าย รับผิดชอบ ดูแล บำรุงรักษา ระบบเครือข่าย และความปลอดภัยของฐานข้อมูลทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบเครือข่าย

๖. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

๖.๑ กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

๖.๑.๑ ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๖.๑.๒ ในกรณีไฟไหม้ ให้ตัดระบบจ่ายไฟ ให้ใช้ น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๖.๑.๓ ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลบำรุงรักษาระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๖.๑.๔ ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบในการบำรุงรักษานำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๖.๒ กรณีเครื่องลูกข่าย

๖.๒.๑ ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศทราบ หรือกรณีมีเหตุอันทำให้ฝ่ายเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ฝ่ายเทคโนโลยีสารสนเทศจะต้องดำเนินการแจ้งให้บริษัทที่รับผิดชอบในการบำรุงรักษารีบดำเนินการให้โดยด่วน

๖.๒.๒ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว และแจ้งให้เจ้าหน้าที่ฝ่ายสารสนเทศดำเนินการ

๗. แผนการนำระบบเทคโนโลยีสารสนเทศกลับสู่สภาพปกติ

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์เครือข่าย โดยปกติจะต้องอยู่ในสภาพพร้อมให้บริการได้ตลอด ๒๔ ชั่วโมง หากไม่สามารถให้บริการ จะต้องดำเนินการกู้คืนระบบให้เร็วที่สุดเท่าที่จะทำได้ เพื่อให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาวะปกติ เมื่อระบบเสียหายหรือหยุดทำงาน ดังนี้

๗.๑ ซ่อมอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๗.๒ สำรองอุปกรณ์ทดแทนหรือยืมอุปกรณ์จากหน่วยงานอื่นมาใช้ทดแทน

๗.๓ นำข้อมูลที่ได้ทำการสำรองไว้ (Backup) กลับมาใช้ (Restore) เพื่อกู้ระบบให้กลับมาภายใน ๒๔ ชั่วโมง

๗.๔ ตรวจสอบระบบปฏิบัติการ ระบบงานและฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลอื่นๆ ที่เกี่ยวข้อง

ภาคผนวก ง

ผู้รับผิดชอบในการสำรองข้อมูลและดูแลระบบต่างๆ ในกรณีเกิดเหตุฉุกเฉิน

รายชื่ออุปกรณ์และระบบที่แต่ละคนรับผิดชอบ

	System	ครรชิต	วีรยุทธ	ดำรัส	มนูญ	อรวรรณ	สมฤทัย
1	Firewall	×					
2	Network Wire & Wireless & Nac		×	×	×		
3	Exchange Mail Server & Spam Gateway		×			×	
4	SSL & Radius		×	×			
5	Blade & Storage		×	×	×		
6	Domain Controller & File Server		×	×			
7	AntiVirus Eset Nod32 Server		×	×	×		
8	Infoblox (DNS&DHCP)	×					
9	Backup Tivoli Storage Manager		×		×	×	×
10	Patch Management		×	×			

	Application	ครรชิต	วีรยุทธ	ดำรัส	มนูญ	อรวรรณ	สมฤทัย
1	ระบบศูนย์ที่ปรึกษาไทย	×	×	×	×		
2	อินทราเน็ต		×			×	×
3	เว็บไซต์หลัก		×		×		×
4	ระบบอีเมล์		×			×	
5	ระบบ E-office			×		×	
6	ระบบ DR-site	×		×	×		
7	ระบบบริหารความเสี่ยง	×					
8	ระบบ DPIS		×	×	×		
9	ระบบ Risk Model	×					
10	ระบบโครงการไทยเข้มแข็ง	×					

ภาคผนวก จ

ข้อปฏิบัติและหลักเกณฑ์ในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

มีขั้นตอนการปฏิบัติดังนี้

๑. ผู้ใช้งานต้องมาลงทะเบียนตามแบบ ศทส. ๐๓ โดยจะได้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งาน

๒. ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓. ผู้ใช้งานมีหน้าที่รับผิดชอบในการ Update โปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๔. ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่

๕. หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่นๆ ได้

๖. ผู้ใช้งานควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๗. ผู้ใช้งานไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

๙. หากผู้ใช้งานลาออกจะต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบทันที เพื่อป้องกันการสวมสิทธิ

ภาคผนวก ๒

ขั้นตอนการปฏิบัติงานการชำระหนี้ในสถานการณ์ฉุกเฉิน มี ๒ วิธี* คือ

๑. การจ่ายเงินในระบบ GFMIS

๒. การหักเงินจากบัญชีเงินคงคลังบัญชีที่ ๒

ในกรณีที่ สบน. ได้ดำเนินการตั้งเบิกในระบบ GFMIS ในวิธีที่ ๑ แล้ว ต่อมาเกิดเหตุการณ์สถานการณ์ฉุกเฉินขึ้นให้ สบน. ประสานงานกับกรมบัญชีกลาง (สำนักบริหารการรับ-จ่ายเงินภาครัฐ ซึ่งรับผิดชอบอยู่ ๒ ส่วน คือ ส่วนบริหารรายรับ (ปลดบล็อค) และส่วนประมวลผลการจ่ายเงิน (Run Payment) ทันที โดยให้ผู้บังคับบัญชาระดับสำนักหรือระดับส่วน เป็นผู้ประสานงาน เพื่อให้กรมบัญชีกลางดำเนินการปลดบล็อค และ Run Payment แต่หากไม่สามารถประสานงานกับกรมบัญชีกลางได้ ก็จะใช้วิธีที่ ๒ คือ การหักเงินจากบัญชีเงินคงคลังบัญชีที่ ๒ โดยสรุปขั้นตอน ได้ดังนี้

๑. การจ่ายเงินในระบบ GFMIS

ขั้นตอนดำเนินการ	ผู้รับผิดชอบ	ระยะเวลาที่ดำเนินการ (ดำเนินการภายในเวลา)
- ตั้งเบิกในระบบ GFMIS และทดสอบการลดยอดหนี้คงค้างในระบบ GFMIS-TR	เจ้าหน้าที่	๑๐ นาที
- ผ่านรายการในระบบ GFMIS	เจ้าหน้าที่	๒๐ นาที
-อนุมัติรายการในระบบ GFMIS	ผู้อำนวยการส่วนฯ หรือผู้ที่ได้รับมอบหมาย	๒๐ นาที
- ตรวจสอบการปลดบล็อคของกรมบัญชีกลางในระบบ GFMIS แล้วรายงานผู้อำนวยการส่วนฯ	เจ้าหน้าที่ ผู้อำนวยการส่วนฯ	๕ นาที
- ติดตามผลการยืนยันการรับเงิน จากเจ้าหนี้(ธปท. หรือธนาคารพาณิชย์ต่าง ๆ ฯลฯ)	เจ้าหน้าที่	๑๐ นาที
- ลดยอดหนี้คงค้างในระบบ GFMIS-TR	ผู้อำนวยการส่วนฯ	๒๐ นาที

๒. การหักเงินจากบัญชีเงินคงคลังบัญชีที่ ๒

ขั้นตอนดำเนินการ	ผู้รับผิดชอบ	ระยะเวลาที่ดำเนินการ (ดำเนินการภายในเวลา)
- ตรวจสอบรายละเอียดของหนี้จะต้องจ่าย เช่น เลขที่บัญชีของเจ้าหนี้(เป็นบัญชีบาทเน็ต) จำนวนเงินให้ถูกต้อง	เจ้าหน้าที่	๑๐ นาที
- เสนอร่างหนังสือถึง ธปท. ให้ชำระหนี้โดยหักเงินคงคลังบัญชีที่ ๒ ต่อผู้มีอำนาจลงนาม (ผู้ที่มีบัตรลายมือชื่อที่ได้ส่งให้ ธปท.)	ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ หรือผู้ที่มีอำนาจสั่งจ่าย**	๓๐ นาที
-ลงทะเบียนส่งหนังสืออนุมัติ (ออกเลขหนังสือ)	เจ้าหน้าที่	๕ นาที

ขั้นตอนดำเนินการ	ผู้รับผิดชอบ	ระยะเวลาที่ดำเนินการ (ดำเนินการภายในเวลา)
	และสารบรรณกลาง	
-ติดตามผลการได้รับชำระหนี้จากเจ้าหนี้	เจ้าหน้าที่	๑๐ นาที
-บันทึกรายจ่ายในระบบ GFMIS และลดยอดหนี้คงค้างในระบบ GFMIS-TR เมื่อได้รับเอกสารเดบิตโน้ตจาก ธปท.	เจ้าหน้าที่ ผู้อำนวยการส่วนฯ	๓๐ นาที
- ยืนยันการหักบัญชีเงินคงคลังบัญชีที่ ๒ ให้กรมธนารักษ์ ทราบ	เจ้าหน้าที่ ผู้อำนวยการส่วน	๓๐ นาที

หมายเหตุ: * ในการดำเนินการทุกขั้นตอนเจ้าหน้าที่ต้องตรวจสอบข้อมูลทั้งในระบบ GFMIS / GFMIS-TR และเอกสารหลักฐานที่เกี่ยวข้องด้วยความละเอียดรอบคอบ หากมีข้อมูลส่วนใดคลาดเคลื่อนจากข้อเท็จจริง ควรรายงานให้ผู้อำนวยการส่วนทราบ พร้อมทั้งดำเนินการแก้ไขทันทีเมื่อสามารถพิสูจน์ทราบข้อเท็จจริงในทางเอกสารแล้ว

** ผู้มีอำนาจสั่งจ่าย ได้แก่

๑) รองปลัดกระทรวงการคลังหัวหน้ากลุ่มภารกิจด้านรายจ่ายและหนี้สิน
๒) ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ
๓) ที่ปรึกษาด้านหนี้สาธารณะ
๔) รองผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ ทั้ง ๒ ท่าน
๕) ผู้อำนวยการสำนักบริหารการชำระหนี้

การติดต่อประสานงานการชำระหนี้ในสถานการณ์ฉุกเฉิน

หน่วยงานที่ต้องประสานงาน	ผู้รับผิดชอบ	โทรศัพท์
<u>วิธีที่๑ (ระบบ GFMIS)</u> กรมบัญชีกลาง	นางอุไร ร่มโพธิหยก (ที่ปรึกษาด้านพัฒนาระบบบัญชี)	๐๒ -๑๒๗-๗๑๐๘ ๐๘๙-๐๓๑-๑๑๗๑ (มือถือ)
สำนักบริหารการรับ-จ่ายเงินภาครัฐ (สรจ.)	น.ส. พรวิลัย เดชอมรชัย	๐๒-๑๒๗-๗๑๓๒ ๐๘๑-๙๓๙-๐๘๗๑ (มือถือ)
ส่วนบริหารรายรับ (ปลดบล็อก)	ว่าง นางภิญญามาศ ชวนวัฒนา (เจ้าหน้าที่)	๐๒-๑๒๗-๗๐๐๐ ต่อ ๔๖๘๑ ๐๘๗-๗๐๑-๘๗๔๔ (มือถือ)
ส่วนประมวลผลการจ่ายเงิน (Run Payment)	นางสิริพร อาจหาญ นภาวรรณ์ ศานติ์สุทธิกุล (ฝ่าย)	๐๒-๑๒๗-๗๓๒๐ ๐๘๑-๙๐๙-๓๕๑๗ (มือถือ)

หน่วยงานที่ต้องประสานงาน	ผู้รับผิดชอบ	โทรศัพท์
<u>วิธีที่๒ (ระบบการหักเงินจากบัญชีเงินคงคลังบัญชีที่ ๒</u> ธนาคารแห่งประเทศไทย ส่วนตราสารหนี้ ฝ่ายเงินฝากและตราสารหนี้	นายยรรยง ดำรงศิริ น.ส. เพียรศิริ มีสวัสดิ์ (เจ้าหน้าที่การเงินอาวุโส)	๐๒-๒๘๓-๕๔๖๙ ๐๘๑-๒๙๗-๒๔๘๕ (มือถือ)