



ประกาศสำนักงานบริหารหนี้สาธารณะ

เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2561

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 มาตรา 6 และมาตรา 7 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ออกประกาศไว้ ดังต่อไปนี้

ข้อ 1 ในประกาศนี้

“สำนักงาน” หมายถึง สำนักงานบริหารหนี้สาธารณะ

“นโยบาย” หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่สำนักงานจัดไว้ให้บริการประชาชน ซึ่งสำนักงานประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานที่เกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับประกาศแนบท้ายพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

“แนวปฏิบัติ” หมายถึง ขั้นตอนวิธีการที่สำนักงานได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของเจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมีจุดมุ่งหมายเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์นั้น มีวิธีการที่มั่นคงปลอดภัย

“ผู้ใช้งาน” หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบของสำนักงาน ผู้บริหารสำนักงาน ผู้ให้บริการ และผู้ใช้งานที่ใช้บริการระบบเทคโนโลยีสารสนเทศของสำนักงาน

“บัญชีผู้ใช้งาน” หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้โปรแกรม ระบบงานคอมพิวเตอร์ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้อีกได้

“สินทรัพย์” หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

“สินทรัพย์คอมพิวเตอร์” หมายความว่า โปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“สารสนเทศ” หมายถึง ข้อมูลในรูปแบบต่างๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจ หรือใช้ประโยชน์ต่าง ๆ ตามภารกิจของสำนักงาน

“เครือข่าย” หมายความว่า ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ 2 เครื่องขึ้นไป เข้าด้วยกัน เพื่อสะดวกต่อการร่วมใช้ข้อมูล โปรแกรม หรือเครื่องพิมพ์ และอำนวยความสะดวกในการติดต่อแลกเปลี่ยนข้อมูลระหว่างเครื่องได้ตลอดเวลา

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของสำนักงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ 2 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน แบ่งเป็น 2 ส่วน ได้แก่

ส่วนที่ 1 แนวนโยบาย

ส่วนที่ 2 แนวปฏิบัติ

รายละเอียดภายในของทั้งสองส่วน ประกอบด้วยเนื้อหาสาระสำคัญในประเด็นต่อไปนี้

(1) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศตามเป้าหมายครอบคลุม 4 เรื่อง

ดังนี้

- การเข้าถึงสารสนเทศ
- การเข้าถึงระบบเครือข่าย
- การเข้าถึงระบบปฏิบัติการ
- การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

(2) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

(4) การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ต้องมีแนวปฏิบัติในการบริหารจัดการสิทธิในแต่ละกลุ่ม รวมถึงการระงับสิทธิ

ข้อ 3 ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานให้เป็นไปตามที่กำหนดไว้ในแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานบริหารหนี้สาธารณะ ปีงบประมาณ พ.ศ. 2561

ข้อ 4 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบ และควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ และตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานอย่างน้อยปีละ 1 ครั้ง โดยกลุ่มตรวจสอบภายในของสำนักงาน

ข้อ 5 สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานของสำนักงาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการ ดังนี้

(1) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์สำนักงานและบอร์ดประชาสัมพันธ์ให้แก่ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

(2) จัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงโดยผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ 6 ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้ทดแทน

ข้อ 7 กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่สำนักงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ 8 ให้ศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ รวมถึงกำหนดให้มีการปฏิบัติที่ชัดเจนและให้มีการทบทวนนโยบายและแนวปฏิบัติให้มีความครบถ้วน สมบูรณ์ เป็นไปตามเจตนารมณ์ของกฎหมายที่กำหนดไว้ หลังจากได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์แล้วเป็นเวลาอย่างน้อย 2 ปี และแจ้งผลการดำเนินงานให้สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทราบ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ 24 กันยายน พ.ศ. 2561



(นายภูมิศักดิ์ อรัญญาเกษมสุข)

ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ



สำนักงานบริหารหนี้สาธารณะ
PUBLIC DEBT MANAGEMENT OFFICE

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง พ.ศ. 2561

ศูนย์เทคโนโลยีสารสนเทศ
สำนักงานบริหารหนี้สาธารณะ
กันยายน 2561

คำนำ

สำนักงานบริหารหนี้สาธารณะ (สบน.) ได้ออกประกาศเรื่องนโยบายในการรักษาความปลอดภัย ปีงบประมาณ พ.ศ. 2560 และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปีงบประมาณ พ.ศ. 2560 เพื่อให้มีแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศในการให้บริการอิเล็กทรอนิกส์ภาครัฐ และเพื่อให้สอดคล้องตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 โดยผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแล้ว วันพุธที่ 25 ตุลาคม พ.ศ. 2555

ในปีงบประมาณ พ.ศ. 2561 นี้ ศูนย์เทคโนโลยีสารสนเทศได้ทำการทบทวนและปรับปรุงเนื้อหาเพิ่มเติมให้เป็นปัจจุบัน และแนวปฏิบัติที่กำหนดต่อไปนี้เป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติ เพื่อให้การให้บริการต่าง ๆ ตามภารกิจของ สบน. ที่ดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัย และเชื่อถือได้ และเพื่อให้ง่ายต่อการนำไปปฏิบัติหรืออ้างอิง จึงแบ่งแนวปฏิบัติออกเป็น 12 หมวด ดังนี้

- หมวด 1 แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ
- หมวด 2 แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึง
- หมวด 3 แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ
- หมวด 4 แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน
- หมวด 5 แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบ/ผู้ดูแลเครือข่าย
- หมวด 6 แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย
- หมวด 7 แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ
- หมวด 8 แนวปฏิบัติในการใช้งาน Token Key
- หมวด 9 แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน
- หมวด 10 แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- หมวด 11 แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ
- หมวด 12 แนวปฏิบัติในการเผยแพร่ข้อมูลต่อสาธารณะ

สารบัญ

คำนำ.....	ก
สารบัญ.....	ข
หมวด 1 แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ.....	1
หมวด 2 แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึงของผู้รับผิดชอบระบบ.....	5
หมวด 3 แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ.....	8
หมวด 4 แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน.....	12
หมวด 5 แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบ/ผู้ดูแลเครือข่าย.....	17
หมวด 6 แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย.....	18
หมวด 7 แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน.....	21
หมวด 8 แนวปฏิบัติในการใช้งาน Token Key.....	22
หมวด 9 แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน.....	23
หมวด 10 แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย.....	24
หมวด 11 แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ.....	27
หมวด 12 แนวปฏิบัติในการเผยแพร่ข้อมูลต่อสาธารณะ.....	30
ภาคผนวก ก ขั้นตอนการลงทะเบียนผู้ใช้งานสำนักงานบริหารหนี้สาธารณะ.....	31
ภาคผนวก ข โปรแกรมมาตรฐานในการใช้งานของสำนักงานบริหารหนี้สาธารณะ.....	32
ภาคผนวก ค แผนเตรียมความพร้อมกรณีฉุกเฉิน.....	33
ภาคผนวก ง ผู้รับผิดชอบในการดูแลอุปกรณ์และระบบเทคโนโลยีสารสนเทศ.....	37
ภาคผนวก จ ข้อปฏิบัติและหลักเกณฑ์ในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่.....	39

หมวด 1

แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

ข้อ 1 ผู้รับผิดชอบระบบสารสนเทศของสำนักงานบริหารหนี้สาธารณะ (สบน.) ต้องมีหน้าที่บริหารจัดการควบคุมการเข้าถึงระบบสารสนเทศ ดังนี้

1.1 ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศได้ก็ต่อเมื่อได้รับอนุญาตจากผู้ดูแลระบบ หรือผู้รับผิดชอบระบบงานตามหน้าที่การปฏิบัติงานเท่านั้น

1.2 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ กล่าวคือในการขออนุญาตเข้าใช้งานระบบงาน ผู้ใช้จะต้องทำบันทึกและกรอกเอกสารที่ สบน. กำหนดเพื่อขอเข้าใช้งานระบบ และให้ผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาลงนามอนุมัติเอกสารดังกล่าวเพื่อจัดเก็บไว้เป็นหลักฐาน จากนั้นผู้ดูแลระบบจะสร้างบัญชีสำหรับการเข้าถึงโดยอนุญาตเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับเป็นหลัก

1.3 ผู้ดูแลระบบต้องกำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้ หากผู้ใช้งานใส่รหัสผ่านเพื่อเข้าใช้งานผิด 3 ครั้ง ระบบจะยกเลิกสิทธิการใช้งาน (Block) ไม่ให้ผู้ใช้งานสามารถใช้งานได้จนกว่าผู้ใช้งานจะยื่นเรื่องพร้อมหลักฐานแสดงต่อเจ้าหน้าที่ผู้ดูแลระบบ เพื่อขอรหัสใหม่อีกครั้ง

1.4 ผู้ดูแลระบบต้องกำหนดให้การเข้าใช้ระบบ (Log-in) เพื่อเข้าใช้งานใดๆ จะต้องมีการตรวจจับการเปิดระบบงานไว้ เมื่อไม่มีการใช้งานก็ต้องออกจากระบบ (Log-out) หรือให้ใช้งานระบบ Log-out อัตโนมัติตามระยะเวลาที่เหมาะสม

1.5 ผู้ดูแลระบบต้องอนุญาตให้ผู้ใช้งานเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชัน และระบบสารสนเทศในส่วนที่จำเป็นตามหน้าที่การปฏิบัติงานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

1.6 กำหนดระยะเวลาการเข้าถึงระบบสารสนเทศของ สบน. ดังนี้

(1) ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานภายนอก สบน. สามารถใช้งานได้ตลอด 24 ชั่วโมง

(2) ระบบงานภายใน สบน. (Back Office) สำหรับผู้ใช้งานภายใน สบน. สามารถใช้งานได้ตั้งแต่เวลา 08.30 - 20.00 น.

1.7 กรณีมีการจ้างผู้ให้บริการภายนอก (Outsource) ในการพัฒนา ดูแล และบำรุงรักษาระบบสารสนเทศ มีมาตรการควบคุมดังนี้

(1) กำหนดเกณฑ์และคัดเลือกผู้ให้บริการภายนอกที่มีคุณสมบัติ ตรงตามมาตรฐานที่หน่วยงานต้องการ และมีขั้นตอนการปฏิบัติงานที่รอบคอบ รัดกุม และน่าเชื่อถือ

(2) กำหนดข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้ให้บริการภายนอก และต้องระบุการรักษาความลับของข้อมูล กำหนดขอบเขตงานและเงื่อนไขในการให้บริการอย่างชัดเจน

(3) กรณีให้บริการด้านการพัฒนาระบบงาน กำหนดให้ผู้ให้บริการภายนอกเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงานเท่านั้น และหากมีความจำเป็นที่ผู้ให้บริการภายนอกเข้ามาปฏิบัติหน้าที่ภายในสำนักงาน ต้องมีเจ้าหน้าที่ของหน่วยงานควบคุมดูแลอย่างใกล้ชิด

(4) กำหนดให้ผู้ให้บริการภายนอกจัดทำคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

(5) กำหนดให้ผู้ให้บริการภายนอกรายงานแผนและผลการปฏิบัติงาน ปัญหาและอุปสรรคต่าง ๆ และแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

(6) กำหนดให้มีหลักเกณฑ์ กระบวนการ และขั้นตอนในการตรวจรับงานที่ส่งมอบ โดยผู้ให้บริการภายนอกที่ชัดเจน

ข้อ 2 ผู้รับผิดชอบระบบสารสนเทศของ สบ. ต้องมีหน้าที่บริหารจัดการรักษาความปลอดภัยทางกายภาพ (Physical Security Management) ดังนี้

2.1 กำหนดระดับความสำคัญของพื้นที่ หรือจำแนกพื้นที่การใช้งานกับพื้นที่การควบคุม

2.2 ทดสอบระบบควบคุมการเข้าถึงพื้นที่ทางกายภาพเพื่อให้ทราบว่าระบบยังใช้งานได้ตามปกติหรือไม่

2.3 ผู้ปฏิบัติงานควรปิดประตูและหน้าต่างให้สนิทอยู่เสมอ

ข้อ 3 ผู้รับผิดชอบระบบสารสนเทศของ สบ. ต้องมีหน้าที่บริหารจัดการควบคุมพื้นที่การเข้า - ออกพื้นที่การควบคุม เช่น ห้องปฏิบัติการคอมพิวเตอร์ ดังนี้

3.1 มีการบันทึกวันและเวลาการเข้า - ออกพื้นที่การควบคุมของผู้มาเยือน (Visitor)

3.2 ดูแลผู้มาเยือนในพื้นที่หรือบริเวณที่มีการควบคุมจนกระทั่งเสร็จสิ้นภารกิจ และกลับไปเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

3.3 จัดให้มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของ สบ. โดยบุคคลภายนอกและควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

3.4 จัดสื่อประชาสัมพันธ์เพื่อสร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

3.5 มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

3.6 ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ เช่น ห้องปฏิบัติการคอมพิวเตอร์ เป็นต้น เว้นแต่ได้รับอนุญาต

3.7 มีการพิสูจน์ตัวตน เช่น การแสดงบัตรผ่าน การใช้บัตรแถบแม่เหล็ก การสแกนลายนิ้วมือ เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะห้องปฏิบัติการคอมพิวเตอร์

3.8 จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญโดยเฉพาะห้องปฏิบัติการคอมพิวเตอร์ เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

3.9 บุคคลภายนอก เช่น เจ้าหน้าที่บริษัท นักศึกษาฝึกงานหรือผู้ได้รับการว่าจ้างอื่น ๆ ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

3.10 ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายใน สบน.

3.11 ควรจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

3.12 จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

3.13 ควบคุมบริเวณ เช่น จุดรับส่งของ เป็นต้น หรือมีการแยกบริเวณดังกล่าวออกจากพื้นที่ที่มีการติดตั้ง จัดเก็บ หรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศเพื่อหลีกเลี่ยงการเข้าถึงโดยมิได้รับอนุญาตของผู้ไม่มีสิทธิเข้าถึง และ/หรือผู้ที่อาจสามารถเข้าถึงระบบสารสนเทศได้

ข้อ 4 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดการจัดวางและการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (Hardware) ดังนี้

4.1 จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงของบุคคลภายนอก

4.2 ระบบงานที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่มีความมั่นคงปลอดภัยเพียงพอ

4.3 ไม่ให้มีการนำอาหาร เครื่องดื่ม หรือสูบบุหรี่ภายในบริเวณห้องปฏิบัติการคอมพิวเตอร์

4.4 ตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติอยู่เสมอ

ข้อ 5 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดให้มีระบบป้องกันและสนับสนุนการทำงาน ดังนี้

5.1 มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อความต้องการใช้งาน โดยให้อย่างน้อย ดังนี้

(1) ระบบสำรองกระแสไฟฟ้า (UPS)

(2) ระบบระบายอากาศ

(3) ระบบปรับอากาศ และควบคุมความชื้น

5.2 ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนอย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

5.3 ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่มีระบบสนับสนุนการทำงานภายในห้องปฏิบัติการคอมพิวเตอร์ทำงานผิดปกติหรือหยุดการทำงาน

ข้อ 6 ผู้รับผิดชอบระบบสารสนเทศของ สบн. ต้องกำหนดและควบคุมการเดินสายไฟฟ้า สายสัญญาณการสื่อสาร และสายเคเบิลอื่นๆ ดังนี้

6.1 เครือข่ายภายใน สบн. ในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอก เข้าถึงได้ต้องให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณและ ป้องกันสัตว์ต่างๆ กัดสาย เช่น หนู แมลงสาบ เป็นต้น ซึ่งจะก่อให้เกิดความเสียหายต่อสายสัญญาณ

6.2 ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซง รบกวนของสัญญาณซึ่งกันและกัน

6.3 จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

6.4 ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของ บุคคลภายนอก

ข้อ 7 ผู้รับผิดชอบระบบสารสนเทศของ สบн. ต้องกำหนดการบำรุงรักษาอุปกรณ์ ดังนี้

7.1 กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

7.2 ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

7.3 จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

7.4 จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและ ปรับปรุงอุปกรณ์ดังกล่าว

7.5 ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบ คอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายใน สบн.

7.6 จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มา ทำการบำรุง รักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ 8 ผู้รับผิดชอบระบบสารสนเทศของ สบн. ต้องควบคุมการนำเครื่องคอมพิวเตอร์และ อุปกรณ์ต่อพ่วงอื่น ๆ ออกจาก สบн. ดังนี้

8.1 ให้มีการขออนุญาตก่อนนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่น ๆ ออกจาก สบн.

8.2 บันทึกข้อมูลการนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ ออกจาก สบн. เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำส่งคืน

ข้อ 9 ผู้รับผิดชอบระบบสารสนเทศของ สบн. ต้องบริหารจัดการควบคุมอุปกรณ์ที่ใช้งาน อยู่ภายนอก สบн. ดังนี้

9.1 กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงอื่น ๆ ของ สบн. ออกไปใช้งานนอกสถานที่ ดังนี้

(1) ห้ามผู้ใช้งานละทิ้งเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ ของ สบน. ไว้โดยลำพังในที่สาธารณะ

(2) ให้ผู้ใช้งานรับผิดชอบดูแลเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ ของ สบน. เสมือนเป็นทรัพย์สินของตนเอง

ข้อ 10 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องควบคุมการจำหน่ายอุปกรณ์จัดเก็บข้อมูลหรือการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

10.1 ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะจำหน่ายอุปกรณ์ดังกล่าวให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูล ในหมวด 3 แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ข้อ 1 (12)

10.2 มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์จัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวด 2

แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึงของผู้รับผิดชอบระบบ

ข้อ 1 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน ดังนี้

1.1 การลงทะเบียนบุคลากรหรือผู้ปฏิบัติงานใหม่ ต้องปฏิบัติตามขั้นตอนลงทะเบียนที่ สบน. กำหนดขึ้น เพื่อให้มีสิทธิในการใช้งานระบบสารสนเทศตามความจำเป็นรวมทั้งปฏิบัติตามขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกหรือเมื่อเปลี่ยนตำแหน่งงานภายใน สบน. เป็นต้น

1.2 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบสารสนเทศที่ให้บริการประชาชนภายนอก ระบบรับ-ส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเทอร์เน็ต (Internet) เครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

1.3 กรณีมีความจำเป็นต้องให้สิทธิพิเศษแก่ผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณาเพื่อขอความเห็นชอบและการอนุมัติจากผู้บังคับบัญชา

(1) ควบคุมการใช้งานอย่างเข้มงวด โดยเฉพาะระบบสารสนเทศหรือโปรแกรมประยุกต์ (Application) ที่มีความเสี่ยงและมีความสำคัญสูง

(2) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(3) มีการเปลี่ยนรหัสผ่าน (Password) อย่างเคร่งครัดทุกครั้ง เช่น หลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

1.4 การขอสิทธิเข้าใช้ระบบ GFMS-TR โดยมีรายละเอียดดังนี้

(1) การขอเพิ่มสิทธิเข้าใช้ระบบ GFMS-TR

หน่วยงานต้นสังกัดของผู้ที่จะขอเพิ่มสิทธิใช้งานระบบ GFMS-TR แจ้งความประสงค์ต่อ ศทส. และ ศทส. พิจารณานำเสนอ ผอ.สบน. หรือผู้ที่ได้รับมอบหมาย เพื่อออกหนังสือถึงกรมบัญชีกลาง (บก.) เพื่อขอให้อนุมัติเพิ่มสิทธิการใช้งานในบัตร GFMS Smart Card

(2) การขอเพิ่มสิทธิเข้าใช้ระบบ GFMS-TR ให้แก่ผู้ให้บริการภายนอก (Outsource)

ผู้ให้บริการภายนอก (Outsource) ที่จะขอสิทธิเข้าใช้ระบบ GFMS-TR แจ้งความประสงค์ต่อ สบน. และ ศทส. พิจารณาจัดทำความเห็นเพื่อออกหนังสือ สบน. ถึง บก. เพื่อขอให้เพิ่มสิทธิในการใช้งานระบบ GFMS-TR เพิ่มเติมจากสิทธิเดิมที่มีอยู่ในบัตร GFMS Smart Card ซึ่งการใช้งานระบบ GFMS-TR ทั้งหมดต้องอยู่ภายใต้การกำกับดูแลของ บก.

(3) การเปลี่ยนแปลงผู้ถือครองบัตร GFMS Smart card

ผู้ที่จะถือครองบัตร GFMS Smart Card ต้องกรอกแบบลงทะเบียนผู้มีสิทธิถือบัตรกำหนดสิทธิการใช้ (GFMS Smart Card) พร้อมแนบสำเนาบัตรประจำตัวประชาชนส่งให้ ศทส. เพื่อพิจารณาจัดทำความเห็นในการออกหนังสือ สบน. ถึง บก. เพื่อขอให้เปลี่ยนแปลงผู้ถือครองบัตร GFMS Smart Card

(4) การยืนยันสิทธิในการเข้าถึงระบบของผู้ถือครองบัตร GFMS Smart Card

ผู้ถือครองบัตร GFMS Smart Card ต้องตรวจสอบสิทธิในการเข้าถึงระบบงานว่ามีความถูกต้องตรงตามหน้าที่หรือไม่และต้องได้รับการยืนยันสิทธิโดยผู้บังคับบัญชา

ข้อ 2 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) ของผู้ใช้งาน ดังนี้

2.1 กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน

2.2 ไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

2.3 จัดเก็บข้อมูลการลงทะเบียนขอเข้าใช้งานระบบ เพื่อใช้อ้างอิงหรือตรวจสอบข้อมูลในภายหลัง

2.4 ทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(1) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงานภายในของ สบน.

(2) จัดส่งรายนามให้ผู้บังคับบัญชาของหน่วยงานภายใน สบน. เพื่อให้ทบทวนว่ายังมีรายชื่อของผู้ที่โอน/ลาออกไปแล้ว หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้อง

(3) ผู้บังคับบัญชาของหน่วยงานภายใน สบน. แจ้งกลับว่ามีรายชื่อใดที่ต้องปรับปรุงแก้ไขให้ถูกต้อง

(4) แก้ไขข้อมูลสิทธิให้ถูกต้องตามที่ได้รับแจ้ง (ถ้ามี)

ข้อ 3 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งาน โดยผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานต้องผ่านการพิสูจน์ตัวตนจากระบบ โดยมีแนวทางปฏิบัติ ดังนี้

3.1 การแสดงตัวตนด้วยชื่อบัญชีผู้ใช้งาน (User Account)

3.2 การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน (Password)

3.3 การเข้าใช้ระบบงานสำคัญของ สบน. ผ่านเครือข่ายอินเทอร์เน็ต จะมีการตรวจสอบผู้ใช้งานด้วย

3.4 การเข้าใช้ระบบงานสำคัญของ สบน. จากระยะไกล (Remote Access) จะมีการตรวจสอบเพื่อเพิ่มความปลอดภัยและเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

3.5 ในการใช้งานระบบสารสนเทศ เมื่อมีการว่างเว้นจากการใช้งานเกินเวลา 5 นาที ระบบจะทำการยกเลิกการใช้งานและการเชื่อมต่อเข้าระบบโดยอัตโนมัติ

ข้อ 4 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดวิธีการใช้รหัสผ่านให้มีความมั่นคงปลอดภัย ดังนี้

4.1 การบริหารจัดการรหัสผ่าน มีมาตรการและการควบคุม ดังนี้

(1) กำหนดให้ต้องเปลี่ยนรหัสผ่านทุก 6 เดือน

(2) กำหนดให้รหัสผ่านต้องมีความยาวหรือเท่ากับ 6 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(3) กรณีผู้ใช้งานเปลี่ยนหน้าที่ความรับผิดชอบหรือลาออกจะต้องเปลี่ยนหรือถอดถอนสิทธินั้นทันทีเมื่อได้รับแจ้ง

(4) กำหนดให้การเข้าใช้งานระบบครั้งแรกมีการโต้ตอบด้วยการยืนยันตัวตนและเปลี่ยนรหัสผ่านเพื่อเพิ่มความปลอดภัย

4.2 การใช้รหัสผ่าน มีมาตรการให้ผู้ใช้งานต้องใช้ด้วยความระมัดระวัง ดังนี้

(1) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(2) ไม่ใช้โปรแกรมสำนักงานคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

(3) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(4) กำหนดรหัสผ่านให้ยากต่อการคาดเดา

(5) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เนื่องจากความจำเป็นในการปฏิบัติงาน หลังจากดำเนินการเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(6) กรณีผู้ใช้งานลาออกหรือเปลี่ยนหน้าที่ความรับผิดชอบ ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศ (ศทส.) ทราบทันที

ข้อ 5 การใช้รหัสผ่านให้ปลอดภัย มีมาตรการในการปฏิบัติ ดังนี้

- 5.1 แสดงกระบวนการมอบอำนาจหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน
- 5.2 มีการกำหนดสิทธิการเข้าถึงตามความจำเป็น
- 5.3 มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน
- 5.4 มีวิธีเลือกการใช้รหัสผ่านและการใช้งานรหัสผ่านที่มีคุณภาพ

หมวด 3

แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ข้อ 1 ผู้บังคับบัญชาหน่วยงานภายใน สบн. ต้องจัดให้มีวิธีการกำหนดประเภทข้อมูลและจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ซึ่งเบื้องต้นใช้แนวทางตาม พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540 และระเบียบที่เกี่ยวข้องในการกำหนดชั้นความลับของข้อมูล จึงกำหนดให้มีแนวทางปฏิบัติ ดังนี้

1.1 ผู้ใช้งานต้องแบ่งประเภทของข้อมูลและชั้นความลับของข้อมูลตามที่ ศทส. ได้กำหนดชั้นความลับของข้อมูลเป็น 4 ระดับ ดังนี้

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

1.2 ผู้ใช้งานต้องพิจารณาองค์ประกอบต่อไปนี้เพื่อเป็นแนวทางกำหนดชั้นความลับของข้อมูล

(1) ความสำคัญของเนื้อหา เช่น เนื้อหาของข้อมูลนั้นมีความสำคัญต่อความสำเร็จของงานตามภารกิจของ สบн. มากน้อยเพียงใด หากมีความสำคัญสูง ข้อมูลนั้นจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือลับ เป็นต้น

(2) แหล่งที่มาของข้อมูล เช่น หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับ ชั้นความลับจะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับจะเป็นประเภทเปิดเผยได้ เป็นต้น

(3) วิธีการนำไปใช้ประโยชน์ เช่น หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบต่อด้านการเงินของ สบн. ดังนั้น ข้อมูลนี้จะอยู่ในประเภทชั้นความลับ เป็นต้น

(4) จำนวนบุคคลที่ควรรับทราบ เช่น หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้ เป็นต้น

(5) ผลกระทบหากมีการเปิดเผย เช่น หากข้อมูลนั้นถูกเปิดเผย จะมีผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการเงิน ด้านการปฏิบัติตามกฎระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้น ข้อมูลสามารถจัดอยู่ในชั้นความลับประเภทใดภายใน หรือลับ เป็นต้น

(6) หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่อง เช่น ข้อมูลสำคัญหรือข้อมูลลับที่มาจากเจ้าของเรื่องใดจะต้องคงชั้นความลับไว้เช่นเดิม การนำไปใช้งานควรขออนุญาตจากผู้ที่เป็นเจ้าของเรื่องก่อน เป็นต้น

(7) สำหรับข้อมูลในชั้นความลับ “ลับ” ได้แก่ ลับ ลับมาก หรือลับที่สุด โดยเจ้าของข้อมูลต้องพิจารณาเกณฑ์ต่อไปนี้เพิ่มเติมเพื่อกำหนดชั้นความลับที่ถูกต้อง

- ลับที่สุด หมายความว่า ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงานอย่างร้ายแรงที่สุด
- ลับมาก หมายความว่า ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงานอย่างร้ายแรง
- ลับ หมายความว่า ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงาน

(8) การดำเนินการกับข้อมูลลับ (ถ้ามี) เจ้าของข้อมูลลับต้องจัดทำทะเบียนข้อมูลลับที่ตนเองดูแลหรือรับผิดชอบ ซึ่งมีรายการดังนี้

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

(9) พิจารณาปรับชั้นความลับ (ปรับลด เพิ่ม หรือยกเลิกชั้นความลับ) ตามความจำเป็นปรับปรุงทะเบียนข้อมูลลับให้ถูกต้องและทันสมัย และต้องแจ้งให้หน่วยงานที่สามารถเข้าถึงข้อมูลหรือที่ได้รับการแจกจ่ายทราบด้วยทุกครั้ง เพื่อแก้ไขชั้นความลับให้ถูกต้อง

(10) ในการจัดทำหรือจัดเตรียมข้อมูลลับให้ผู้ใช้งานปฏิบัติ ดังนี้

- จัดทำหรือจัดเตรียมข้อมูลในสถานที่ปลอดภัย เช่น จัดทำภายใน สบน.
ไม่จัดทำในสถานที่สาธารณะซึ่งบุคคลภายนอกสามารถเห็นข้อมูลที่ทำได้ และจำกัดบุคคลเฉพาะผู้ที่เกี่ยวข้อง
ในการเข้าถึงข้อมูล

- ในการจัดทำข้อมูลลับซึ่งใช้กระดาษหรือวัสดุชั่วคราว เช่น กระดาษร่าง
กระดาษคาร์บอน ต้องทำลายกระดาษหรือวัสดุนั้นทันทีที่จัดทำเสร็จเรียบร้อย ถ้าเป็นการจัดทำโดยใช้
เครื่องคอมพิวเตอร์ จะต้องลบหรือทำลายสื่อบันทึกข้อมูลจนไม่สามารถนำไปใช้ประโยชน์ได้
(ดูวิธีการทำลายในตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูลในข้อ (16) ที่จะกล่าวต่อไป)
หากไม่ทำลายต้องเก็บรักษาไว้ในสถานที่ที่ปลอดภัย

- จัดทำข้อมูลโดยแสดงเลขที่หน้าของจำนวนหน้าทั้งหมดไว้ในทุกหน้าของ
ข้อมูลลับ และแสดงไว้ในส่วนที่สามารถเห็นได้ชัดเจน เช่น มุมขวาด้านบนของเอกสาร (การบันทึกเลขหน้ามี
จุดประสงค์ เพื่อให้ทราบว่าข้อมูลลับนั้นเป็นหน้าใดของจำนวนทั้งหมด หากมีการสูญหายไปหน้าใดหน้าหนึ่ง
จะได้ทราบและสามารถติดตามหาผู้ละเมิดและหาทางลดหรือแก้ไขความเสียหายที่เกิดขึ้นได้)

(11) ในการแสดงชั้นความลับบนข้อมูลลับ ให้ปฏิบัติดังนี้

- แสดงชั้นความลับของข้อมูล ซึ่งประกอบด้วย “ลับ” “ลับมาก” หรือ
“ลับที่สุด” ให้ปรากฏเห็นอย่างเด่นชัดทั้งข้อมูลที่มีสภาพเป็นกระดาษ ไฟล์อิเล็กทรอนิกส์ เทป External
Hard Disk, Flash Drive แผ่น CD/DVD หรือข้อมูลลับที่อยู่ในรูปแบบอื่นๆ

- แสดงชั้นความลับบนเอกสารลับในทุกหน้าของเอกสารให้ปรากฏเห็นอย่าง
เด่นชัด

(12) ในการทำสำเนาหรือแจกจ่ายข้อมูลลับให้ปฏิบัติ ดังนี้

- ทำสำเนาหรือแจกจ่ายข้อมูลลับให้แก่ผู้รับปลายทางซึ่งเป็นผู้ที่มีสิทธิในการ
เข้าถึงข้อมูลตามที่ระบุไว้ในทะเบียนข้อมูลลับ หรือสามารถแจกจ่ายให้ได้ตามความจำเป็นในการเข้าถึงข้อมูลนั้น

- แจ้งให้หน่วยงานภายนอกที่อนุญาตให้เข้าถึงข้อมูลลับนั้นได้ ว่าไม่อนุญาต
ให้ทำสำเนาเพิ่มเติม เว้นเสียแต่ได้รับอนุญาตจากผู้มีอำนาจลงนามอนุญาตก่อน

(13) ในการเก็บรักษาเอกสารลับให้ปฏิบัติ ดังนี้

- จัดเก็บเอกสารลับไว้ในแฟ้มข้อมูลลับ และนำไปเก็บไว้ในตู้เก็บเอกสารลับ
โดยแยกเก็บเป็นแต่ละเรื่องหรือแต่ละหัวข้อ

- ไม่จัดเก็บเอกสารลับร่วมกับเอกสารที่อยู่ในชั้นความลับอื่นๆ เช่น ข้อมูล
ใช้ภายในเท่านั้น ข้อมูลส่วนบุคคล หรือข้อมูลที่เปิดเผยได้

- จัดเก็บแฟ้มข้อมูลลับไว้ในตู้และปิดล็อกด้วยกุญแจที่แข็งแรงและมั่นคง

(14) ในการยืมหรือขอเข้าถึงข้อมูลลับให้ปฏิบัติ ดังนี้

- เมื่อมีการยืมหรือขอเข้าถึงข้อมูลลับโดยผู้อื่นที่ไม่ได้เป็นผู้มีสิทธิในการเข้าถึงข้อมูลตามทะเบียนข้อมูลลับ ให้หัวหน้าของส่วนงานที่รับผิดชอบเป็นผู้พิจารณาตรวจสอบคุณสมบัติของผู้ยืมหรือขอเข้าถึงก่อนว่าเป็นผู้มีอำนาจหน้าที่ที่เกี่ยวข้องหรือไม่ หรือมีความจำเป็นในการเข้าถึงข้อมูลนั้นหรือไม่ พร้อมทั้งต้องทำบันทึกหลักฐานการยืมหรือการขอเข้าถึงข้อมูลนั้นด้วย และแจ้งให้ผู้ยืมหรือขอเข้าถึงทราบว่าห้ามทำสำเนาเพิ่มเติม

- เมื่อหมดความจำเป็นในการใช้งานแล้ว หัวหน้าของส่วนงานที่รับผิดชอบกำหนดให้ผู้ยืมจัดส่งข้อมูลนั้นกลับคืนมาโดยทันที สำหรับกรณีการเข้าถึงระบบเทคโนโลยีสารสนเทศ ให้ยกเลิกบัญชีผู้ใช้งานที่ขอเข้าถึงข้อมูลลับโดยทันที

(15) ในการส่งเอกสารลับทางจดหมายอิเล็กทรอนิกส์ (E-Mail) ให้ปฏิบัติตามระเบียบการส่งเอกสารลับของ สบн. เพื่อตรวจสอบที่อยู่ E-Mail ของผู้รับปลายทางให้ถูกต้องก่อนจัดส่งไฟล์ข้อมูลนั้นไปยังผู้รับเพื่อป้องกันการส่งผิดตัวบุคคล

(16) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ

ตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูล

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลายสื่อและข้อมูล
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย ส่วนในกรณีที่ต้องการนำกลับมาใช้ใหม่ให้ใช้โปรแกรม Active@killdisk โดยโปรแกรมจะลบข้อมูลจนไม่สามารถกู้คืนมาได้ด้วยการเขียนทับ ตลอดจนทั่วอุปกรณ์
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้วิธีการทุบหรือบดให้เสียหาย ส่วนในกรณีที่ต้องการนำกลับมาใช้ใหม่ให้ใช้โปรแกรม Active@killdisk โดยโปรแกรมจะลบข้อมูลจนไม่สามารถกู้คืนมาได้ด้วยการเขียนทับ ตลอดจนทั่วอุปกรณ์

(17) ในการจัดการกับไฟล์ข้อมูลลับให้ปฏิบัติ ดังนี้

- จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ (E-File) ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึงและควรแสดงชั้นความลับบนไฟล์ข้อมูลลับ เช่น การทำสัญลักษณ์ลายน้ำและแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

- การสำเนา E-File ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล

- ระมัดระวังการเผยแพร่ หรือแจกจ่าย E-File ที่เป็นความลับของ สบн. ไปยังกลุ่มผู้รับ ต้องเฉพาะกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

- ผู้เป็นเจ้าของ E-File ต้องตรวจสอบความถูกต้องของ E-File ก่อนนำไปใช้งาน
- ห้ามผู้เป็นเจ้าของ E-File ที่มีความลับ หรือที่มีระดับความสำคัญสูง ส่งข้อมูลดังกล่าวไปทางไปรษณีย์ เว้นแต่จะได้ใช้วิธีเข้ารหัสที่ สบн. กำหนดไว้
- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการเข้ารหัสผ่านที่มีความมั่นคงปลอดภัยและไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์
- ห้ามแบ่งปัน (Share) ไฟล์ข้อมูลลับบนเครือข่ายสาธารณะ (Internet) ของ สบн. เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)
- ตรวจสอบการทำงานของระบบป้องกันไวรัสในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับอย่างสม่ำเสมอว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่
- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมสำนักงานเพื่อแก้ไขช่องโหว่ของโปรแกรมในเครื่องตามปกติหรือไม่
- สำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอ หรือตามความจำเป็น
- ต้องทำลาย E-File บนหน่วยความจำหลัก (Hard disk) ของเครื่องคอมพิวเตอร์ ที่ถูกยกเลิกการใช้งาน

หมวด 4

แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

ข้อ 1 การใช้เครื่องคอมพิวเตอร์ภายใน สบн. ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

- 1.1 ห้ามใช้เครื่องคอมพิวเตอร์จนกว่าจะได้รับการอนุมัติให้ใช้งาน โดยให้กรอกข้อมูลขอใช้งานเครื่องคอมพิวเตอร์ตามแบบ ศทส.01 แบบฟอร์มพนักงานใหม่ (ท้ายระเบียบนี้)
 - 1.2 การใช้งานเครื่องคอมพิวเตอร์ต้องตรวจสอบการทำงานของโปรแกรมป้องกันไวรัส และการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) ก่อนใช้งานทุกครั้ง หากพบว่าโปรแกรมดังกล่าวทำงานผิดปกติให้รีบแจ้ง ศทส. เพื่อดำเนินการแก้ไขโดยเร็ว
 - 1.3 เครื่องคอมพิวเตอร์ที่ใช้ภายใน สบн. ให้ติดตั้งโปรแกรมมาตรฐานตามที่กำหนดไว้ท้ายระเบียบนี้ ห้ามเปลี่ยนแปลงหรือติดตั้งโปรแกรมเพิ่มเติม เว้นแต่จะได้รับความเห็นชอบจากหัวหน้าหน่วยงานภายใน สบн. เท่านั้น
- ความในวรรคหนึ่ง ไม่ใช้บังคับแก่การเปลี่ยนแปลงหรือการติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมเพื่อทดลองการใช้งานซึ่งดำเนินการโดย ศทส. หรือผู้ที่ได้รับการว่าจ้างให้มาจัดทำหรือดูแลระบบเทคโนโลยีสารสนเทศของ สบн.

1.4 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์เพื่อไม่ให้บุคคลภายนอกสามารถใช้งานเครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ของ สบн. ได้

1.5 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกจากโปรแกรมตามมาตรฐานที่กำหนดไว้
ท้ายประกาศนี้

1.6 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ในทรัพย์สินทางปัญญาของบุคคลอื่น

1.7 ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องของ สบн.

1.8 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่ายคอมพิวเตอร์

1.9 ต้องระมัดระวังการใช้งานและดูแลเครื่องคอมพิวเตอร์ รวมทั้งระบบเครือข่ายตามที่วิญญูชนทั่วไปจะพึงปฏิบัติ

1.10 เอกสารหรือข้อมูลต่างๆ ไม่ว่าจะอยู่ในรูปแบบใดก็ตามที่ได้มีการกำหนดเงื่อนไขการใช้งานไว้ต้องใช้งานด้วยความระมัดระวัง และต้องปฏิบัติตามเงื่อนไขอย่างเคร่งครัด เพื่อป้องกันมิให้เกิดการละเมิดตามกฎหมาย

1.11 ต้องลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์เพื่อประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

1.12 ต้องออกจากระบบ (Log off) ทุกครั้งที่มีได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์ รวมทั้งปิดเครื่องคอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

1.13 การติดตั้งโปรแกรมเพิ่มเติมต้องเป็นโปรแกรมที่มีลิขสิทธิ์และใช้ในการทำงานซึ่งต้องได้รับอนุญาตจากผู้มีอำนาจ โดยผ่านการลงทะเบียนตามแบบ ศทส.02 แบบฟอร์มลงโปรแกรมเพิ่ม (ท้ายระเบียบนี้)

1.14 การนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้กับระบบเครือข่ายคอมพิวเตอร์ของ สบн. ต้องได้รับการตรวจสอบและอนุญาตจาก ศทส. โดยผ่านการลงทะเบียนตามแบบ ศทส.03 แบบฟอร์มเข้าใช้เครือข่ายบุคคลภายใน และ แบบ ศทส.04 แบบฟอร์มเข้าใช้เครือข่ายบุคคลภายนอก

1.15 ตรวจสอบอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable Media) ก่อนการใช้งานด้วยโปรแกรมป้องกันไวรัสเพื่อป้องกันโปรแกรมที่ไม่พึงประสงค์

ข้อ 2 การใช้เครื่องคอมพิวเตอร์แบบพกพา (Notebook) ของ สบн. นอกจากต้องปฏิบัติตามที่กำหนดไว้ในข้างต้นแล้ว ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

2.1 ต้องตรวจสอบเครื่องคอมพิวเตอร์แบบพกพาที่นำไปใช้ว่าได้ติดตั้งโปรแกรมคอมพิวเตอร์ตามมาตรฐานที่กำหนดไว้ท้ายระเบียบนี้แล้วหรือไม่ หากพบว่ายังไม่ได้ติดตั้งให้แจ้งผู้รับผิดชอบระบบสารสนเทศของ สบн. เพื่อขอรับการติดตั้งก่อนการใช้งาน

2.2 ต้องระมัดระวังไม่ให้บุคคลภายนอกมองเห็นหรือคัดลอกข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาที่นำไปใช้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

2.3 เมื่อหมดความจำเป็นที่ต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาแล้ว ให้รับนำส่งคืนเจ้าหน้าที่ผู้รับผิดชอบทันที ทั้งนี้ให้เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมในการใช้งานของเครื่องคอมพิวเตอร์ที่รับคืนไว้ดังกล่าวด้วย

ข้อ 3 ในกรณีที่เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนเครื่องคอมพิวเตอร์แบบพกพาตรวจพบความเสียหาย ให้แจ้งผู้บังคับบัญชาทราบโดยเร็ว และหากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทเลินเล่ออย่างร้ายแรงของผู้นำไปใช้ ต้องให้ผู้นำไปใช้รับผิดชอบต่อความเสียหายที่เกิดขึ้นดังกล่าว

ข้อ 4 การใช้เครื่องคอมพิวเตอร์เพื่อประโยชน์ส่วนตัวของเจ้าหน้าที่ให้ใช้ได้ภายในสถานที่ สบ. จัดไว้เป็นการเฉพาะเท่านั้น

ข้อ 5 การเข้าถึงระบบงานเทคโนโลยีสารสนเทศ เจ้าหน้าที่ใช้งานต้องปฏิบัติตามข้อกำหนด ดังนี้

5.1 กรอกแบบเพื่อขออนุมัติใช้งานระบบงานและนำเสนอต่อผู้บังคับบัญชาเพื่อขออนุมัติ โดยผ่านการลงทะเบียนตามแบบ ศทส.01 แบบฟอร์มพนักงานใหม่ (ท้ายระเบียบนี้)

5.2 ต้องไม่เข้าถึงระบบงานอื่นที่ไม่ได้รับอนุญาตให้ใช้งาน

5.3 ต้องออกจากระบบงานโดยทันที เมื่อใช้งานเสร็จสิ้น

ข้อ 6 การใช้งานอินเทอร์เน็ต ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

6.1 ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

- การพนัน
- การประมุข
- วิพากษ์วิจารณ์ที่เกี่ยวข้องกับชาติ ศาสนา และพระมหากษัตริย์
- ลามก อนาจาร
- อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

6.2 ห้ามเล่นเกมส์ หรือดาวน์โหลดเกมส์ ภาพยนตร์ เพลง หรือสื่อลามกอนาจารผ่านทางอินเทอร์เน็ต

6.3 ห้ามใช้อินเทอร์เน็ตเพื่อเผยแพร่หรือแจกจ่าย ดังต่อไปนี้

- สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของ
- ข้อมูลประเภทสื่อลามกอนาจาร
- ข้อมูลที่เป็นความลับของ สบ. ไปยังบุคคลที่ไม่ได้รับอนุญาต
- ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

6.4 ห้ามใช้งานข้อมูลที่ได้รับโดยผ่านทางอินเทอร์เน็ตที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของข้อมูลนั้น

6.5 ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ หรือชื่อเสียงของ สบн.

ข้อ 7 การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ผู้ใช้งานต้องปฏิบัติตามข้อกำหนด ดังต่อไปนี้

- 7.1 ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ตามที่ สบн. กำหนดเท่านั้น
- 7.2 ห้ามใช้ E-mail Address ที่ สบн. กำหนดให้ ลงทะเบียนตามเว็บไซต์ที่ไม่เกี่ยวข้องกับงานของ สบн.
- 7.3 ห้ามเข้าถึง E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต
- 7.4 ห้ามปลอมแปลง รับหรือส่ง E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต
- 7.5 ห้ามส่ง E-mail ที่มีลักษณะดังต่อไปนี้
 - จดหมายขยะ (Spam Mail)
 - จดหมายลูกโซ่ (Chain Letter)
 - จดหมายที่ละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น
 - จดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
- 7.6 ห้ามส่ง E-mail ที่มีขนาดใหญ่เกินกว่าที่กำหนด
- 7.7 ต้องระบุชื่อเรื่อง (Subject) และชื่อผู้ส่งใน E-mail ทุกฉบับที่ส่งไป
- 7.8 ต้องใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับ E-mail เท่าที่มีความจำเป็นต้องรับรู้เท่านั้น
- 7.9 ต้องใช้คำที่สุภาพในการส่ง E-mail
- 7.10 ต้องสำรองข้อมูล E-mail Address ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ 8 ห้ามมิให้เจ้าหน้าที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของ สบн. กระทำการในลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้

- 8.1 กระทำผิดกฎหมายหรือก่อให้เกิดความเสียหายแก่บุคคลอื่นหรือขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือละเมิดทรัพย์สินทางปัญญาของ สบн. และของบุคคลอื่น
- 8.2 เปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน ทั้งที่เป็นข้อมูลของ สบн. หรือบุคคลภายนอก
- 8.3 การเข้าถึงข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาต
- 8.4 ขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของ สบн. หรือเจ้าหน้าที่คนอื่นของ สบн.
- 8.5 แสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับ สบн. ไปยังที่อยู่เว็บไซต์ใด ๆ ในลักษณะที่ก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง และก่อให้เกิดความเสียหายแก่ สบн.
- 8.6 กระทำการอื่นใดที่อาจขัดต่อการดำเนินงานตามอำนาจหน้าที่ของ สบн. หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่ สบн.
- 8.7 จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

ข้อ 9 เอกสารที่เป็นความลับหรือมีระดับความสำคัญซึ่งพิมพ์ออกมาจากเครื่องพิมพ์ (Printer) เจ้าหน้าที่ต้องปฏิบัติให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการ ดังต่อไปนี้

- 9.1 จัดหมวดหมู่เอกสารที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก
- 9.2 จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ
- 9.3 การสำเนาเอกสารที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูง ต้องได้รับอนุญาตจากผู้เป็นเจ้าของ
- 9.4 ระมัดระวังการเผยแพร่ หรือแจกจ่ายเอกสารที่เป็นความลับของ สบн. ไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น
- 9.5 ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน
- 9.6 ให้ทำลายเอกสารที่เป็นความลับ หรือมีระดับความสำคัญสูงเมื่อหมดความจำเป็นในการใช้งาน

ข้อ 10. การจัดการข้อมูลที่เป็นความลับที่อยู่ในรูปอิเล็กทรอนิกส์ ผู้ใช้งานปฏิบัติตามแนวทางปฏิบัติในการจัดการกับข้อมูลลับในข้อข้างต้น

ข้อ 11 ผู้ใช้งานควรตรวจสอบ E-mail ที่ได้รับทุกครั้งว่าเข้าข่ายลักษณะการเป็นจดหมายขยะ (Spam mail) หรือไม่ โดยผู้ใช้งานต้องปฏิบัติตามข้อกำหนด ดังนี้

11.1 ตรวจสอบแหล่งที่มาของ E-mail ก่อนเปิดอ่าน โดยให้สังเกตลักษณะของจดหมายขยะ (Spam mail) ดังนี้

- ชื่อผู้ส่งจะไม่สามารถค้นหาที่มาได้ และ/หรือเป็นชื่อที่ผู้ใช้งานไม่รู้จัก/ไม่คุ้นเคย
- ชื่อเรื่องของ E-mail จะเป็นข้อความที่โน้มน้าวให้น่าสนใจ เพื่อต้องการให้ผู้ใช้งานเปิดอ่าน ตัวอย่างเช่น “นี่คือคำตอบที่คุณได้ร้องขอจากเราไป” หรือ “ผมได้ส่งไฟล์มาแล้วตามที่ร้องขอ” หรือ “คุณได้รับอนุมัติบัตรเครดิตแล้ว” เป็นต้น

11.2 ตรวจสอบเนื้อหาของ E-mail โดยมีจุดสังเกต ดังนี้

- E-mail ที่ไม่มีเนื้อหา
- E-mail ที่มีเนื้อหาเกี่ยวกับการโฆษณาสินค้า ผลิตภัณฑ์ หรือบริการ
- E-mail ที่มีลักษณะหลอกลวงโดยสอบถามข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ควรเปิดเผยสู่สาธารณะ
- E-mail ที่ใช้เนื้อหาในลักษณะของรูปภาพแทนตัวอักษร
- E-mail ที่แนบไฟล์ที่อาจเป็น Virus หรือ Trojan และมีเนื้อหาเชิญชวนให้ผู้ใช้งานดาวน์โหลดหรือติดตั้งไฟล์ดังกล่าว

ข้อ 12 ในกรณีที่ผู้ใช้งานได้รับจดหมายขยะ (Spam mail) ผู้ใช้งานต้องปฏิบัติตามข้อกำหนด
ดังนี้

12.1 ห้ามเปิดอ่าน E-mail ฉบับนั้นโดยเด็ดขาด และให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยี
และสารสนเทศทราบทันที

12.2 ในกรณีที่เปิดอ่านแล้ว ห้ามคลิกที่ Link ข้อมูล หรือดาวน์โหลดไฟล์ที่แนบมา
กับ E-mail ฉบับนั้น และให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีและสารสนเทศทราบทันที

หมวด 5

แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบสารสนเทศ/ผู้ดูแลระบบเครือข่าย

ข้อ 1 ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศ ระบบจดหมาย
อิเล็กทรอนิกส์ (E-mail) และระบบเครือข่ายของ สบн. ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ
หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์ ระบบงานสารสนเทศ และระบบเครือข่ายให้รีบ
ดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้นในทันที และในกรณีจำเป็นเพื่อป้องกัน
หรือบรรเทาความเสียหายที่จะเกิดขึ้นกับ สบн. ให้ผู้ดูแลระบบ (System Administrator) พิจารณาระงับ
การใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าวได้ทันที

ข้อ 2 ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์
และระบบเครือข่ายให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

ข้อ 3 ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server)
ระบบงานสารสนเทศ และระบบเครือข่าย

ข้อ 4 ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทาง
การสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

ข้อ 5 บริหารจัดการบัญชีผู้ใช้งานและควบคุมการเข้าถึงตามอำนาจหน้าที่เท่านั้น

ข้อ 6 บริหารจัดการระบบงานสารสนเทศ และระบบเครือข่ายตามอำนาจหน้าที่รับผิดชอบเท่านั้น

ข้อ 7 บริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามอำนาจหน้าที่รับผิดชอบเท่านั้น

ข้อ 8 ไม่ใช้อำนาจหน้าที่ของตนเองในการเข้าถึงข้อมูลของผู้ใช้งาน บนระบบคอมพิวเตอร์
ระบบสารสนเทศ และระบบเครือข่าย โดยไม่มีเหตุผลอันสมควร

ข้อ 9 ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้งานที่
ใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่าย โดยไม่มีเหตุผลอันสมควร

ข้อ 10 ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สามารถเปิดเผยได้ให้บุคคลอื่นทราบ โดยไม่มีเหตุผลอันสมควร

ข้อ 11 เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งานและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า 90 วัน นับจากการใช้บริการสิ้นสุดลง

ข้อ 12 กำหนดและปรับปรุงระดับการคัดกรองจดหมาย (E-mail Filtering) ของเครื่องคอมพิวเตอร์แม่ข่าย (Mail Server) ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

ข้อ 13 ตรวจสอบและบำรุงรักษาวัสดุอุปกรณ์ไฟฟ้าภายในห้องปฏิบัติการคอมพิวเตอร์ เช่น สายไฟฟ้า และสายสัญญาณ เป็นต้น อย่างสม่ำเสมอ หากพบความชำรุดให้ติดต่อหน่วยงานที่รับผิดชอบเพื่อให้แก้ไขอย่างทันการณ์

หมวด 6

แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

ข้อ 1 กำหนดมาตรการทางเครือข่ายและการสื่อสารข้อมูลเพื่อป้องกันข้อมูลในเครือข่ายคอมพิวเตอร์ ระบบงานสารสนเทศ หรือบริการต่างๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาตดังต่อไปนี้

1.1 กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

1.2 การปฏิบัติงานขององค์กรจากภายนอก สบน. ในการเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกลจะต้องปฏิบัติ ดังนี้

- ติดต่อ ศทส. เพื่ออธิบายเหตุผลความจำเป็นและกำหนดช่วงเวลาที่ยื่นขอในการใช้งานและลงทะเบียนเป็นลายลักษณ์อักษร

- ศทส. จะกำหนดสิทธิให้เข้าใช้งานเฉพาะระบบที่จำเป็นต้องใช้เท่านั้น

1.3 กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ เช่น เครือข่ายอินเทอร์เน็ต เครือข่ายไร้สาย เป็นต้น

1.4 การเข้าสู่ระบบงานสารสนเทศภายในองค์กร สำหรับผู้ใช้นอกองค์กร (Guest) ต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง ด้วยการใช้รหัสผ่าน โดยจะต้องลงทะเบียนและขอรับได้ที่ ศทส.

1.5 กำหนดข้อปฏิบัติในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์พกพาและโทรศัพท์มือถือ ต้องมีการยืนยันตัวตนในการเข้าใช้งานทุกครั้งด้วยการใช้รหัสผ่านที่ออกให้โดย ศทส. ซึ่งสิทธิที่ได้จะแตกต่างกันและมีข้อกำหนดการใช้งานที่จำกัด โดยมีข้อปฏิบัติและหลักเกณฑ์ตามภาคผนวก จ.

1.6 มีการบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์เครือข่าย เพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

ข้อ 2 ผู้รับผิดชอบหรือผู้ดูแลระบบสารสนเทศภายใน สบн. จะต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

2.1 ผู้ดูแลระบบต้องออกแบบการแบ่งระบบเครือข่าย (Segregation in Networks) ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน ดังนี้

- เขตภายใน (Internal Zone)
- เขตภายนอก (External Zone)

เพื่อเป็นการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

2.2 การเข้าสู่ระบบเครือข่ายภายใน สบн. โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาก่อนที่จะสามารถใช้งานได้ในทุกกรณี

2.3 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายและระบบสารสนเทศที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

2.4 ผู้ดูแลระบบจะต้องตรวจสอบและจำกัดเส้นทางการเข้าถึงเครือข่าย โดยการปิดเส้นทางของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นออกจากระบบ

2.5 ผู้ดูแลระบบจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ใช้งานไปยังเครื่องคอมพิวเตอร์ให้บริการ เช่น ในการเชื่อมต่อเข้าสู่เครื่องคอมพิวเตอร์ให้บริการเพื่อบริหารจัดการระบบ ให้กำหนดเฉพาะชุดเลขประจำเครื่องคอมพิวเตอร์ (IP Address) ของผู้ดูแลระบบเท่านั้นที่สามารถเข้าถึงเครื่องคอมพิวเตอร์ที่ให้บริการนั้นได้

2.6 กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต่างๆ ของระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์อย่างชัดเจนและมีการทบทวนการกำหนดค่าตัวแปร (Parameter) ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนด แก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

2.7 ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก สบн. จะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมป้องกันการบุกรุกในการทำ Packet filtering เป็นต้น

2.8 มีการติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) เพื่อตรวจสอบการใช้งานของบุคคลที่ใช้งานระบบเครือข่ายภายใน สบн. ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

2.9 การเข้าสู่ระบบงานเครือข่ายภายใน สบн. ผ่านทางอินเทอร์เน็ตจะต้องมีการพิสูจน์ตัวตน (Authentication) โดยการกรอกชื่อผู้ใช้ (Username) และรหัสผู้ใช้ (Password) สำหรับ Login เพื่อตรวจสอบความถูกต้อง

2.10 ข้อมูลหมายเลขชุดภายในของเครื่องคอมพิวเตอร์ (Local IP Address) ของระบบงานเครือข่ายภายใน สบน. จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของ สบน. ได้โดยง่าย

2.11 จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.12 การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2.13 ผู้ดูแลระบบกำหนดอุปกรณ์บนเครือข่ายเป็น IP Address แยกตามสำนัก ศูนย์ และกลุ่มแต่ละสิทธิของผู้ใช้งาน โดยให้ควบคุมการใช้งานอย่างเหมาะสมและมีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

2.14 การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อยกว่า 3 เดือน หรือไม่ต่ำกว่า 90 วัน

2.15 มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

ข้อ 3 ผู้รับผิดชอบระบบสารสนเทศของ สบน. จะต้องควบคุมการเข้าใช้งานจากภายนอก สบน. เพื่อดูแลรักษาความปลอดภัยโดยมีแนวทางการปฏิบัติ ดังนี้

3.1 การเข้าสู่ระบบจากระยะไกล (Remote Access) เข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของ สบน. ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรจะต้องขออนุญาตก่อนการใช้งานทุกครั้ง

3.2 วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

3.3 ก่อนการขอเข้าใช้งานระบบสื่อสารจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับ สบน. และต้องได้รับอนุมัติจากผู้บังคับบัญชาทุกครั้ง

3.4 มีการควบคุมช่องทางติดต่อ (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

3.5 การอนุญาตให้ผู้ใดเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

ข้อ 4 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless) ผู้รับผิดชอบระบบสารสนเทศของ สบн. ต้องกำหนดแนวปฏิบัติตามข้อกำหนด ดังต่อไปนี้

4.1 ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายใน สบн. จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน

4.2 ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

4.3 ผู้ดูแลระบบควรใช้ Software หรือ Hardware ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

หมวด 7

แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน

ข้อ 1. ผู้ใช้งานจะต้องยืนยันตัวตนด้วย User Account ของตนเองก่อนเข้าใช้งานระบบปฏิบัติการเครื่องคอมพิวเตอร์ทุกครั้ง

ข้อ 2. ผู้ใช้งานต้องไม่อนุญาตให้บุคคลอื่นใช้ User Account ของตนเองในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

ข้อ 3. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมเพื่อล็อกหน้าจอโดยอัตโนมัติ หลังจากที่ไม่ได้ใช้งานเกินกว่า 15 นาที

ข้อ 4. ผู้ใช้งานควรทำการลงบันทึกออก (Log Off) ทุกครั้งที่มีได้ปฏิบัติงานอยู่หน้าเครื่องคอมพิวเตอร์ รวมทั้งปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเลิกใช้งาน

ข้อ 5. ผู้ใช้งานต้องไม่ใช่โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

ข้อ 6. ผู้ใช้งานต้องกำหนดรหัสผ่านไม่น้อยกว่า 6 ตัวอักษร โดยไม่นำชื่อหรือนามสกุลของตนเองหรือคำที่ง่ายต่อการคาดเดามาตั้ง และต้องเปลี่ยนรหัสผ่านทุก 6 เดือน

หมวด 8

แนวปฏิบัติในการใช้งาน Token Key

ข้อ 1 ข้อกำหนดการใช้งาน Token Key

- 1.1 ผู้มีสิทธิใช้งานต้องได้รับอนุมัติให้ใช้งาน Token Key จาก ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ (ผอ. สบน.) หรือผู้ซึ่ง ผอ. สบน. มอบหมายลงนาม สำหรับให้เข้าใช้งาน
- 1.2 ผู้มีสิทธิใช้งานต้องแนบเอกสารหลักฐานข้อมูลผู้ใช้ให้ผู้ดูแลระบบ เพื่อที่จะสามารถตรวจสอบรายละเอียดผู้ใช้ได้
- 1.3 อุปกรณ์ Token Key มีการจำกัดให้ใช้งานเฉพาะระบบภายใน สบน. 2 ระบบ คือ
 - ระบบ GFMIS-SOE
 - ระบบการประมูลพันธบัตรด้วยวิธีอิเล็กทรอนิกส์ (e-bidding)
- 1.4 ผู้ใช้งานสามารถใช้ Token Key ได้เฉพาะ 1 Token ต่อ 1 ระบบ เท่านั้น
- 1.5 การใช้งาน Token Key ต้องเสียบ Token Key เข้าเครื่องคอมพิวเตอร์ทุกครั้ง เพื่อยืนยันตัวบุคคล (Username) และใส่รหัสของผู้ใช้งาน (Password) ก่อนเข้าใช้งาน
- 1.6 ผู้ใช้งานต้องเปลี่ยนรหัส ทุกๆ 3 เดือน เพื่อความปลอดภัยในการเข้าใช้งานระบบ
- 1.7 ผู้ใช้งานต้องรับผิดชอบต่อการปฏิบัติงานที่เกิดจากการใช้งานตามสิทธิที่ได้รับในการปฏิบัติงานเข้าใช้งานระบบทุกรายการ

ข้อ 2 การดูแลและการเก็บรักษา Token Key ให้ปลอดภัย

- ผู้ใช้งานต้องมีหน้าที่ในการจัดเก็บรักษา Token Key ให้มีความปลอดภัย ดังนี้
- ควรระมัดระวังไม่ให้ Token Key ตกน้ำ หรือแช่น้ำเป็นเวลานาน อาจทำให้ Token Key ไม่สามารถใช้งานได้
 - ห้ามจัดแงะ ทิ่มหรือกระแทกอย่างรุนแรง จะทำให้ Token Key เสียรูปทรงจนไม่สามารถใช้งานได้
 - ต้องไม่อนุญาตให้บุคคลอื่นนำ Token Key ไปใช้งานนอกจากจะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 3 ข้อปฏิบัติในกรณีที่ Token Key สูญหาย หรือชำรุด ต้องดำเนินงานตามขั้นตอน ดังนี้

- ผู้ใช้งานต้องโทรศัพท์แจ้งผู้ดูแลระบบเพื่อระงับการใช้งาน Token Key กรณีที่ผู้ใช้งานไม่แจ้งการสูญหายและมีผู้อื่นนำ Token Key ไปใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นตามแต่กรณี
- ทำหนังสือแจ้งผู้ดูแลระบบภายใน 3 วัน นับจากที่ผู้ใช้งานโทรแจ้งระงับการใช้งาน Token Key เพื่อรับ Token Key อันใหม่สำหรับการใช้งาน
- กรณีที่เป็นผู้ใช้งานคนเดิมไม่ต้องส่งเอกสารข้อมูลส่วนบุคคลอีก

ข้อ 4 ข้อปฏิบัติในกรณีที่มีการย้ายหรือเปลี่ยนแปลงผู้ใช้งาน Token Key ต้องดำเนินงานตามขั้นตอน ดังนี้

- ทำหนังสือแจ้งพร้อมแบบฟอร์มลงทะเบียนผู้ใช้งาน (แบบลงทะเบียน GFMS-SOE)
- ทำหนังสือคำสั่งแต่งตั้งให้ดำรงตำแหน่งผู้ใช้งาน ภายใน 15 วัน นับจากมีคำสั่งย้ายหรือเปลี่ยนแปลงผู้ใช้งาน
- ต้องแนบรายละเอียดข้อมูลส่วนบุคคล เช่น บัตรประจำตัวประชาชนหรือบัตรข้าราชการ เพื่อให้สามารถระบุตัวตนผู้ใช้งานได้

ข้อ 5 กรณีที่ต้องเพิกถอนการใช้งาน Token Key

การเพิกถอนการใช้งาน คือ การทำให้ใบรับรองอิเล็กทรอนิกส์หรือ Token Key ไม่สามารถนำมาใช้ได้อีกต่อไป โดยผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ หรือผู้ใช้งานสามารถเพิกถอนการใช้งานได้ในกรณีดังต่อไปนี้

- มีผู้อื่นสามารถเข้าถึง หรือนำ Token Key ไปใช้งานโดยไม่ได้รับอนุญาต
- มีผู้อื่นล่วงรู้รหัสผ่าน (Password) ที่ใช้ในการเรียกใช้ Token Key ของผู้ใช้งาน

ข้อ 6 การระบุชื่อและยืนยันตัวบุคคลใน Token Key

6.1 ชื่อที่ระบุใน Token Key

ชื่อที่ปรากฏใน Token Key ของผู้ใช้งานต้องมีลักษณะเป็นชื่อ และไม่ซ้ำกัน เพื่อให้รับรองได้ว่าสามารถเชื่อมโยงกับผู้ใช้งานได้

6.2 ชื่อที่ระบุในใบรับรองอิเล็กทรอนิกส์สำหรับยืนยันตัวบุคคล

ชื่อที่ปรากฏในใบรับรองอิเล็กทรอนิกส์แต่ละใบของผู้ใช้งาน จะต้องมีความหมายถึงผู้ใช้งาน เพื่อประโยชน์ในการสืบค้นกลับไปยังผู้ใช้งานได้

หมวด 9

แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

ข้อ 1 ผู้รับผิดชอบระบบสารสนเทศของ สบม. ต้องกำหนดแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล เมื่อมีระบบงานใหม่ เกิดข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่ ควรกำหนดให้ใช้แนวทางการสำรองและกู้คืนข้อมูล ดังนี้

- 1.1 กำหนดระบบงานที่มีความจำเป็นต้องสำรองข้อมูลไว้
- 1.2 กำหนดผู้รับผิดชอบในการสำรองข้อมูลและกรณีเกิดเหตุฉุกเฉิน (ในภาคผนวก ง)
- 1.3 กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อยต้องประกอบด้วย ข้อมูลในฐานข้อมูลของระบบ ข้อมูลสำหรับตัวระบบ เช่น โปรแกรมระบบปฏิบัติการ (Operation Software) และโปรแกรมอื่นๆ ที่เกี่ยวข้อง

- 1.4 กำหนดความถี่ในการสำรองข้อมูลของระบบงาน เช่น ระบบงานที่มีการเปลี่ยนแปลงบ่อยควรมีความถี่ในการสำรองข้อมูลมากขึ้น เป็นต้น
- 1.5 กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งโปรแกรมที่ใช้ในการสำรองข้อมูล
- 1.6 ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และควรนำข้อมูลที่สำรองไปเก็บไว้ นอกสถานที่อย่างน้อย 1 ชุด
- 1.7 ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วนหรือไม่
- 1.8 ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ 1 ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่
- 1.9 จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด โดยแผนฯ ควรมีรายละเอียดอย่างน้อยดังต่อไปนี้
- (1) การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด
 - (2) การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
 - (3) การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน
 - (4) การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้
 - (5) การกำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอกเช่น ผู้ให้บริการเครื่องคอมพิวเตอร์ โปรแกรมและระบบเครือข่าย เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่าง ๆ เช่น เกิดอัคคีภัย การก่อวินาศกรรม เป็นต้น
- 1.10 ให้ทำการปรับปรุงแผนฯ ดังกล่าวอย่างน้อยปีละ 1 ครั้ง
- 1.11 ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนฯ รวมทั้งเมื่อมีการปรับปรุงแผนใหม่จะต้องจัดประชุมใหม่และแจ้งให้ผู้เกี่ยวข้องทราบเช่นเดียวกัน

หมวด 10

แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ 1 การแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย (เพิ่มเติมจากประกาศของ ICT)

- 1.1 ให้เจ้าหน้าที่หรือผู้ปฏิบัติงานแจ้งไปยัง ศทส. ทันทีที่พบเห็นเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของ สบн. ได้แก่
- มีโปรแกรมสำนักงานไม่ประสงค์ดีเข้ามาในระบบคอมพิวเตอร์
 - มีการบุกรุกเข้ามาในระบบเครือข่าย
 - ข้อมูลสำคัญเปลี่ยนแปลง หรือสูญหาย

- มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
- มีการนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์
- มีการใช้ระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์
- พบจุดอ่อนในเครื่องคอมพิวเตอร์ โปรแกรมและระบบเครือข่ายที่ใช้งาน
- มีการโจมตีเข้ามาในระบบจนไม่สามารถให้บริการได้
- ระบบเทคโนโลยีสารสนเทศชำรุดหรือสูญหาย
- บุคคลภายนอกเข้าใช้ระบบงานของ สบн. โดยไม่ได้รับอนุญาต
- มีการติดตั้งโปรแกรมเพื่อขโมยข้อมูลหรือเข้าถึงข้อมูลในระบบเครือข่าย
- เหตุการณ์อื่นๆ ที่เป็นการละเมิดความมั่นคงปลอดภัยของ สบн.

1.2 ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชาหรือ ศทส. ในการตรวจสอบเหตุการณ์ทางด้านการมั่นคงปลอดภัยที่เกิดขึ้นรวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชาหรือ ศทส. ด้วย

ข้อ 2 ผู้รับผิดชอบระบบสารสนเทศของ สบн. เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านการมั่นคงปลอดภัยที่เกิดขึ้นหรือที่พบ ให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

2.1 ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบในระดับใด (สูง กลาง หรือต่ำ)

2.2 แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบตามระดับของผลกระทบ กล่าวคือ รายงานไปสู่ระดับชั้นของผู้บังคับบัญชาที่สูงขึ้นตามลำดับสำหรับเหตุการณ์ที่มีผลกระทบสูงกว่า

2.3 วิเคราะห์และแก้ไขสถานการณ์ตามความจำเป็นกรณีการบุกรุก การโจมตีระบบ หรือระบบได้รับความเสียหาย ประสานงานขอความช่วยเหลือจากผู้รู้ เช่น ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT)

2.4 กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ ให้ผู้ที่ผ่านการอบรมหรือฝึกฝนเป็นผู้ดำเนินการเพื่อป้องกันไม่ให้เกิดหลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัย และจำกัดการเข้าถึงหลักฐานนั้น

2.5 จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลาง ขึ้นไปและแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีข้อมูลอย่างน้อยในรายงานดังนี้

- รายละเอียดเหตุการณ์
- วันเวลาที่เกิดขึ้น
- ชื่อผู้แจ้ง/หน่วยงานผู้แจ้ง
- สถานะของเหตุการณ์ในแต่ละช่วงเวลา
- ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา
- สาเหตุและวิธีการแก้ไข
- ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

ข้อ 3 ความรับผิดชอบของผู้บังคับบัญชากรณีที่มีการละเมิดการปฏิบัตินี้

- 3.1 ให้แจ้งรายงานตามสายการบังคับบัญชาให้หน่วยที่เกี่ยวข้องทราบ
- 3.2 สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด
- 3.3 พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้อับติซ้ำอีก
- 3.4 ให้พิจารณาการลงโทษทางวินัยตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิด และผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้โดยเจตนาหรือไม่เจตนา และการละเมิดนั้นก่อให้เกิดความเสียหายหรือยังไมเกิดความเสียหายต่อทางราชการก็ตาม

ข้อ 4 ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบงานสารสนเทศ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของระบบสารสนเทศดำเนินการ ดังนี้

- 4.1 พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่างๆ ประมวลลับ หรือรหัสผ่านที่จำเป็นในการใช้เครือข่ายสื่อสารข้อมูลสารสนเทศมีผลกระทบกระเทือนเสียหายอย่างไรหรือไม่
- 4.2 ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันทีในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่างๆ ที่เกี่ยวข้องตามที่เห็นสมควร

ข้อ 5 ความรับผิดชอบของผู้ใช้งานต่อประกาศฉบับนี้ ดังนี้

- 5.1 ปฏิบัติตามประกาศนี้อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง
- 5.2 ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบคอมพิวเตอร์และเครือข่ายของ สบน.
- 5.3 ไม่รบกวนหรือแทรกแซงการสื่อสารข้อมูลในเครือข่ายของ สบน.
- 5.4 รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยัง สบน. โดยเร็วที่สุด

ข้อ 6 มีการควบคุมสินทรัพย์ด้านสารสนเทศต่อการเข้าถึงต้องได้รับการอนุญาตโดยปฏิบัติ ดังนี้

- 6.1 กำหนดมาตรการป้องกันทรัพย์สินขององค์กร โดยรวบรวมสินทรัพย์ทั้งหมดไว้อย่างเป็นระบบ
- 6.2 เมื่อใช้งานระบบเสร็จ ต้องออกจากระบบทันที
- 6.3 ป้องกันไม่ให้ผู้ที่ไม่เกี่ยวข้องใช้อุปกรณ์ด้านสารสนเทศโดยไม่ได้รับอนุญาต
- 6.4 นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

หมวด 11

แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ

ข้อ 1 ผู้รับผิดชอบระบบสารสนเทศของ สบн. ต้องควบคุมการพัฒนาหรือจัดหาระบบงาน เพื่อให้ระบบงานที่ได้รับมีความมั่นคงปลอดภัยเพียงพอ ดังนี้

1.1 ให้ประเมินความเสี่ยงและระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษร ข้อกำหนดดังกล่าวอย่างน้อย ควรมีคุณสมบัติของการเข้าสู่ระบบงาน (Login) ที่มีความมั่นคงปลอดภัย ดังนี้

(1) ไม่มีหรือไม่แสดงรูปแบบการใช้งาน (Function) ให้การช่วยเหลือในระหว่างที่ Login

(2) บันทึกความพยายามในการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ และแสดงประวัติ การ Login 3 ครั้งล่าสุด

(3) ตัดการเชื่อมต่อหลังจากที่ทำการ Login ไม่สำเร็จเกินกว่า 3 ครั้ง

(4) เมื่อใส่ข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้อง ให้แสดงข้อความปรากฏ เช่น “ข้อมูลการ Login ไม่ถูกต้อง”

(5) ให้แสดงข้อความเตือนที่หน้าจอภายหลังจากการ Login เสร็จสิ้น ข้อความเตือน ดังกล่าว ได้แก่ “ระบบนี้เป็นระบบที่เป็นทรัพย์สินของ สบн. การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้นจึง จะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงานหากมีการตรวจพบและเป็นความผิดจะดำเนินการ ลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม สิทธิในการตรวจสอบพฤติกรรมการใช้งาน ในระหว่างที่ผู้ใช้งานใช้ระบบงานนี้โดยไม่ถือว่าเป็นการละเมิดความเป็นส่วนตัว”

(6) ไม่แสดงรายละเอียดของระบบใดๆ จนกว่าจะ Login สำเร็จ

(7) การกำหนดหรือตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับเข้าถึงระบบงาน

(8) การเข้ารหัสข้อมูลสำคัญที่มีการรับส่งระหว่างเครื่องคอมพิวเตอร์ลูกข่ายกับ เครื่องคอมพิวเตอร์ที่ให้บริการ

(9) การเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลลับ ที่จัดเก็บไว้ในฐานข้อมูล

(10) การตัดและหมดเวลาการใช้งานหลังจากที่ไม่ได้ใช้ระบบงานเกินกว่าระยะเวลา ตามที่กำหนดไว้ เช่น 15 - 30 นาที

(11) การบันทึกบัญชีชื่อผู้ใช้งานที่ Login เข้าระบบ หมายเลข IP Address วันเวลาที่เข้าใช้ระบบ ความสำเร็จหรือไม่สำเร็จในการ Login ของผู้ใช้งาน

1.2 พัฒนาหรือจัดหาระบบงานให้ได้ตามข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ระบุไว้

1.3 พัฒนาหรือจัดหาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลระบบเพื่อทำการบันทึกและ ปรับปรุงสิทธิของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

1.4 กำหนดให้มีการจัดทำแผนการทดสอบโดยผู้พัฒนาระบบ นำเสนอแผนฯ ดังกล่าว เพื่อพิจารณาอนุมัติโดยผู้มีอำนาจ ดำเนินการทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการทดสอบ ให้ผู้มีอำนาจได้รับทราบเพื่อใช้คำแนะนำในการปรับปรุงต่างๆ ที่จำเป็นแผนการทดสอบที่จัดทำอย่างน้อย ประกอบด้วย

- แผนการทดสอบ UAT (User Acceptance Test)
- แผนการทดสอบ System Integration Test
- แผนการทดสอบข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Test)

1.5 ไม่อนุญาตการนำข้อมูลสำคัญของ สบн. ไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นเสียแต่ได้รับการอนุมัติจากผู้บังคับบัญชาในระดับสูงก่อน และหากเป็นไปได้ ให้ตัดข้อมูลส่วนที่สำคัญทิ้งไป ให้เหลือเฉพาะส่วนที่เพียงพอต่อการนำไปใช้ในการทดสอบ

1.6 การส่งข้อมูลผ่านระบบสารสนเทศต้องไม่สามารถถูกเปลี่ยนแปลงพร้อมทั้งยังคงความถูกต้องครบถ้วน (Integrity) และความถูกต้องแท้จริง (Authenticity) ✓

ข้อ 2 ภายหลังจากที่ได้มีการตรวจรับระบบที่พัฒนาขึ้นใหม่แล้ว ผู้รับผิดชอบระบบสารสนเทศของ สบн. ต้องกำหนดการควบคุมการติดตั้งโปรแกรมลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการ ดังนี้

2.1 ให้มีการควบคุมการเปลี่ยนแปลงระบบงานภายใน สบн. เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

2.2 ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงระบบงานภายใน สบн.

2.3 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

2.4 กำหนดให้มีการจัดเก็บรหัสโปรแกรม (Source Code) และบรรณานุกรมคำศัพท์ (Library) สำหรับโปรแกรมของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

2.5 กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน เช่น โปรแกรมระบบปฏิบัติการ โปรแกรมระบบงาน เป็นต้น

2.6 ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

2.7 ทำการปรับปรุง Library สำหรับโปรแกรมระบบงาน ให้มีความทันสมัยและสอดคล้องกับระบบทั้งหมดที่ทำการติดตั้ง

2.8 ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิมให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล โปรแกรม ค่าปรับแต่งและติดตั้งระบบ หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จจะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้

2.9 ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่ทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ให้ถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

2.10 ให้กำหนดแผนการติดตั้งสำหรับระบบงานซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า เช่น แผนการติดตั้งเครื่องคอมพิวเตอร์ โปรแกรมระบบเครือข่าย และอื่น ๆ

2.11 สำหรับโปรแกรมที่จะทำการติดตั้ง ให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตโปรแกรมนั้น

2.12 ให้อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานโปรแกรมที่จะทำการติดตั้งอย่างเคร่งครัด

2.13 สำหรับการติดตั้งโปรแกรมมอเนกประสงค์ (Utility Software) ต้องตรวจสอบก่อนว่าเป็นโปรแกรมที่มีการทำงานที่ถูกต้องและเชื่อถือได้

2.14 ติดตั้งโปรแกรมสำนักงานแก้ไขช่องโหว่ (Patch) ที่เกี่ยวข้องกับระบบงานตามความจำเป็น เช่น โปรแกรมสำนักงานแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมสำนักงานแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

2.15 ตรวจสอบและปิดพอร์ต (Port) บนระบบงานที่ไม่มีความจำเป็นในการใช้งานก่อนเปิดระบบให้บริการ

2.16 จัดให้มีการป้องกันไวรัสคอมพิวเตอร์บนระบบงานที่ทำการติดตั้ง

ข้อ 3 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating System Changes) ดังนี้

3.1 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

3.2 พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่ สบน. ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

ข้อ 4 การดำเนินงานของงบประมาณที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ หรือวัสดุอุปกรณ์อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ต้องผ่านการพิจารณาลั่นกรองความเหมาะสมเบื้องต้นจาก ศทส. และนำเสนอให้ ผอ. สบน. ลงนาม หรือ ผู้ซึ่ง ผอ. สบน. มอบหมายลงนาม โดยคณะกรรมการคอมพิวเตอร์กระทรวงการคลัง (คคค.) เป็นผู้พิจารณาอนุมัติก่อนจะพิจารณาในขั้นตอนต่อไป

หมวด 12

แนวปฏิบัติในการเผยแพร่ข้อมูลต่อสาธารณะ

ข้อ 1 การเผยแพร่ข้อมูลในความรับผิดชอบของ สบн. ต่อสาธารณะโดยผ่านระบบเทคโนโลยีสารสนเทศของ สบн. หน่วยงานเจ้าของข้อมูลจะต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำออกเผยแพร่ และหากข้อมูลที่น่าออกเผยแพร่เกี่ยวข้องกับเรื่องนโยบายจะต้องได้รับความเห็นชอบจาก ผอ. สบн. หรือผู้ซึ่ง ผอ. สบн. มอบหมายก่อนนำออกเผยแพร่ ในกรณีที่ข้อมูลที่น่าออกเผยแพร่มีความผิดพลาด และมีความเสียหายเกิดขึ้น โดยความเสียหายนั้นเกิดจากความจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ให้เป็นความรับผิดชอบของเจ้าหน้าที่ผู้นำข้อมูลดังกล่าวออกเผยแพร่

ข้อ 2 การเผยแพร่ข้อมูลต่อสาธารณะโดยผ่านระบบเทคโนโลยีสารสนเทศของ สบн. ให้ดำเนินการโดยหน่วยงานเจ้าของข้อมูล เว้นแต่กรณีที่ ผอ. สบн. หรือผู้ซึ่ง ผอ. สบн. มอบหมาย ได้สั่งการหรือเห็นชอบไว้เป็นอย่างอื่น

ประกาศ ณ วันที่ 24 กันยายน พ.ศ. 2561



(นายภูมิศักดิ์ อรัญญาเกษมสุข)

ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ

ภาคผนวก ก

ขั้นตอนการลงทะเบียนผู้ใช้งานสำนักงานบริหารหนี้สาธารณะ มีขั้นตอนการปฏิบัติ ดังนี้

- (1) การลงทะเบียนขอเข้าใช้งานเครื่องคอมพิวเตอร์ E-mail และระบบงานภายใน สบн. ให้ใช้แบบ ศทส. 01 แบบฟอร์มพนักงานใหม่
- (2) การลงทะเบียนขอติดตั้งโปรแกรมเพิ่มเติมในเครื่องคอมพิวเตอร์ สบн. ให้ใช้แบบ ศทส. 02 แบบฟอร์มลงโปรแกรมเพิ่มในเครื่องคอมพิวเตอร์ สบн.
- (3) การลงทะเบียนขออนุญาตใช้บริการอินเทอร์เน็ตผ่านเครือข่าย สบн. สำหรับบุคคลภายใน สบн. ให้ใช้แบบ ศทส. 03 แบบฟอร์มเข้าใช้เครือข่าย (บุคคลภายใน)
- (4) การลงทะเบียนขออนุญาตใช้บริการอินเทอร์เน็ตผ่านเครือข่าย สบн. สำหรับบุคคลภายนอก สบн. ให้ใช้แบบ ศทส. 04 แบบฟอร์มเข้าใช้เครือข่าย (บุคคลภายนอก)

ภาคผนวก ข

การติดตั้งโปรแกรมคอมพิวเตอร์ตามมาตรฐานที่ สบ. กำหนด
มีขั้นตอนการปฏิบัติ ดังนี้

1. ชุดโปรแกรมระบบปฏิบัติการ Microsoft Windows
2. ชุดโปรแกรมสำนักงาน Microsoft Office
3. โปรแกรม Acrobat Reader
4. โปรแกรมประเภท Zip File
5. โปรแกรม Anti-virus (NOD 32)
6. โปรแกรม Microsoft Lync
7. โปรแกรม Flash Player
8. โปรแกรมเขียนข้อมูล (Nero Burning ROM)
9. โปรแกรมรหัสผ่านเดียว (Single Sign-on)
10. โปรแกรมประเภท Browser (Firefox, Chrome)

ภาคผนวก ค
แผนเตรียมความพร้อมกรณีฉุกเฉิน
แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ
(IT Contingency Plan)

1. หลักการและเหตุผล

สำนักงานบริหารหนี้สาธารณะ (สบน.) เป็นหน่วยงานที่มีพันธกิจในการบริหารจัดการหนี้สาธารณะโดยการวางแผน กำกับ และดำเนินการก่อหนี้ ค่าประกัน และปรับโครงสร้างหนี้ของรัฐบาล หน่วยงานในกำกับดูแล ของรัฐ องค์การปกครองส่วนท้องถิ่น และรัฐวิสาหกิจ ซึ่งรวมทั้งการชำระหนี้ของรัฐบาล การติดตามและประเมินผลการดำเนินงาน จึงได้นำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงาน เพื่อเพิ่มประสิทธิภาพในการบริหารหนี้สาธารณะของประเทศ ในขณะเดียวกันระบบฐานข้อมูลและสารสนเทศของ สบน.อาจได้รับความเสียหายจากการให้บริการ ซึ่งได้แก่ ไวรัสมัลแวร์ การบุกรุก (Hacker) ไฟฟ้าดับ และปัจจัยอื่น ๆ ที่เกี่ยวข้อง ที่ทำให้เกิดผลกระทบต่อการดำเนินงาน

เพื่อเป็นการป้องกันและแก้ไขปัญหาที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ (ศทส.) จึงต้องจัดทำแผนรองรับการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

2. วัตถุประสงค์

- 2.1 เพื่อเป็นการบริหารความเสี่ยง และเป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมใช้งาน
- 2.2 เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ
- 2.3 เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถให้บริการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขปัญหาสถานการณ์ได้อย่างทันท่วงที
- 2.4 เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
- 2.5 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบฐานข้อมูลและสารสนเทศ

3. ประเมินความเสี่ยงจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้น

จากการประเมินความเสี่ยงที่อาจเกิดขึ้นต่อความเสียหายของระบบฐานข้อมูลและสารสนเทศ มีความน่าจะเป็นที่อาจเกิดขึ้นสูงไปต่ำ ตามลำดับดังนี้

- 3.1 ความเสี่ยงจากไฟฟ้าดับ
- 3.2 ความเสี่ยงจากอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย (Server) ชำรุด
- 3.3 ความเสี่ยงจากไวรัสคอมพิวเตอร์
- 3.4 ความเสี่ยงจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ (Hacker)
- 3.5 ความเสี่ยงจากไฟไหม้

4. แผนการป้องกันและเตรียมความพร้อม

4.1 กรณีไฟฟ้าดับ

4.1.1 ติดตั้งอุปกรณ์สำรองไฟฟ้า (Uninterruptible Power Supply : UPS) ที่ สบน. สำหรับในกรณีที่ไฟฟ้าดับ ซึ่งจะสามารถสำรองไฟฟ้าไว้ได้เป็นระยะเวลา 20-25 นาที ซึ่งเพียงพอที่จะสั่งการให้ระบบปิดการทำงาน (Shutdown) โดยที่ไม่เกิดความเสียหายต่ออุปกรณ์หรือข้อมูล

4.1.2 ประชาสัมพันธ์การปิดระบบสารสนเทศเพื่อให้บุคลากรรับทราบ

4.2 กรณีที่ระบบเครือข่ายขัดข้อง

4.2.1 ติดตั้งเส้นทางสำรองสำหรับระบบงานบริการ ให้สามารถบริการได้อย่างต่อเนื่อง

4.2.2 จัดจ้างบริษัทดำเนินการบำรุงรักษาระบบเครือข่าย

4.2.3 สำรองข้อมูลและระบบงาน (Back up) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลถูกทำลายหรือถูกบุกรุก หรือไม่สามารถให้บริการได้

4.3 กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server) ชำรุด

4.3.1 ตั้งค่าการทำงานของ Harddisk เป็น RAID-5 เพื่อป้องกันข้อมูลเสียหายให้แก่ระบบงานต่าง ๆ ในกรณีที่ Harddisk เกิดการขัดข้องหรือชำรุด

4.3.2 ดูแลเครื่องคอมพิวเตอร์เครื่องคอมพิวเตอร์แม่ข่าย (Server) ไม่ให้ขาดอายุการรับประกัน

4.4 กรณีไวรัสคอมพิวเตอร์

4.4.1 ติดตั้งโปรแกรมสำหรับป้องกันและตรวจจับไวรัส (Anti-Virus) ครอบคลุมทุกเครื่องคอมพิวเตอร์เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) เพื่อป้องกันความเสียหายของข้อมูล

4.4.2 Update ข้อมูลไวรัสอย่างสม่ำเสมอในทุกวัน โดยโปรแกรมสามารถทำการ Update ข้อมูลไวรัสได้จากเครื่องคอมพิวเตอร์เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบอัตโนมัติ

4.4.3 ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นดิสก์หรือสื่อบันทึกข้อมูลต่าง ๆ

4.5 กรณีการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ (Hacker)

4.5.1 ติดตั้งอุปกรณ์ Firewall เพื่อรักษาความปลอดภัยให้ระบบเครือข่ายและป้องกันการใช้งานระบบเครือข่ายที่ผิดวัตถุประสงค์ ป้องกันการบุกรุกจากภายนอก

4.5.2 ติดตั้งอุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention Systems : IPS) เพื่อทำหน้าที่ป้องกัน (Block) การบุกรุกระบบเครือข่าย

4.6 กรณีไฟไหม้

ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) เพื่อการควบคุมเพลิงเบื้องต้นได้

5. แผนปฏิบัติและขั้นตอนสำหรับสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้น

5.1 ขั้นตอนการแก้ไขจากกรณีไฟฟ้าดับ

5.1.1 ตู้ Rack ที่ 3 ให้ปิดเครื่องคอมพิวเตอร์แม่ข่าย (Server) ทั้งหมด

5.1.2 ตู้ Rack ที่ 4 ให้ปิดเครื่องคอมพิวเตอร์แม่ข่าย (Server) ทั้งหมด

5.1.3 ตู้ Rack ที่ 5 ให้ปิดเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบจัดเก็บ

ข้อมูล (Tape)

5.1.4 ตู้ Rack ที่ 6 ให้ปิดเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบจัดเก็บ

ข้อมูล (SAN)

5.1.5 ตู้ Rack ที่ 1 และ 2 ให้ปิดอุปกรณ์กระจายสัญญาณ (Switch)

และ Appliance

5.1.6 ปิดระบบเครื่องปรับอากาศ (Air-conditioning System)

5.1.7 ปิดระบบอุปกรณ์สำรองไฟฟ้า (UPS)

5.2 ขั้นตอนการแก้ไขกรณีระบบเครือข่ายขัดข้อง

5.2.1 ตรวจสอบจากอุปกรณ์ Network Monitor ที่ IP 192.168.1.28 เพื่อตรวจสอบ

จุดที่เกิดปัญหาและสาเหตุ

5.2.2 ประสานงานเจ้าหน้าที่ บริษัท พอยท์ ไอที จำกัด (นายสุรพันธ์ พะวันรัมย์

โทร. 087-992-7502)

5.2.3 ประสานงานเจ้าหน้าที่ บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

(นายศมากร จงอนุรักษ์ โทร. 082-090-7189)

5.3 ขั้นตอนการแก้ไขกรณีอุปกรณ์เครื่องแม่ข่าย (Server) ชำรุด

5.3.1 เปลี่ยนอุปกรณ์ทดแทน ติดตั้งระบบปฏิบัติการและย้ายข้อมูล

5.3.2 ประสานงานเจ้าหน้าที่ บริษัท พอยท์ ไอที จำกัด ในกรณีที่อุปกรณ์อยู่ในระหว่าง

รับประกัน (นายสุรพันธ์ พะวันรัมย์ โทร. 087-992-7502)

5.3.3 ประสานงานส่วนงานพัสดุเพื่อเปลี่ยนเลขทะเบียนครุภัณฑ์

5.4 ขั้นตอนการแก้ไขกรณีพบไวรัสคอมพิวเตอร์

5.4.1 ประกาศให้ผู้ใช้งานตรวจสอบข้อมูลและทำการสำรองข้อมูลที่สำคัญ

5.4.2 ตรวจสอบภาพรวมระบบมอนิเตอร์ ที่ IP 192.168.1.220

5.4.3 ตัดความเชื่อมโยงของเครื่องคอมพิวเตอร์ที่พบไวรัสออกจากระบบเครือข่าย

เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย

5.5 ขั้นตอนการแก้ไขกรณีการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ (Hacker)

5.5.1 ตรวจสอบจากอุปกรณ์ Network Monitor ที่ IP 192.168.1.28 เพื่อตรวจสอบจุดที่เกิดปัญหาและสาเหตุ

5.5.2 ตรวจสอบช่องโหว่หรือความเสียหายจากการถูกโจมตี เพื่อป้องกันโดยการปิด Port ที่ไม่จำเป็นต่อไป

5.5.3 ประสานงานเจ้าหน้าที่บริษัท พอยท์ ไอที จำกัด ในกรณีที่ถูกบุกรุกอยู่ในระหว่างรับประกัน (นายสุรพันธ์ พะวันรัมย์ โทร. 087-992-7502)

5.6 ขั้นตอนการแก้ไขกรณีไฟไหม้

5.6.1 ตัดระบบจ่ายไฟ เพื่อลดความเสียหาย

5.6.2 ตรวจสอบความเสียหายและทำความสะอาดสารเคมี (FM 200) ที่ถูกฉีดพ่นออกมาเพื่อดับเพลิง เพื่อแจ้งบริษัท พอยท์ ไอที จำกัด (นายสุรพันธ์ พะวันรัมย์ โทร 087-992-7502) เพื่อเติมสารเคมีต่อไป

6. เจ้าหน้าที่ผู้รับผิดชอบ

6.1 นายครรชิต พะลัง	โทร 081-623-8912
6.2 นายดำรัส หอกิจรุ่งเรือง	โทร 094-691-5359
6.3 นางสาวอรรวรรณ วิฑูรภิตติกุล	โทร 089-488-8699
6.4 นายพิรวัชร จรูญเกียรติศักดิ์	โทร 080-225-1937
6.5 นายหฤษฎ์ หวังเสรี	โทร 087-710-0053

7. การซ่อม

กำหนดให้มีการซ่อมและทบทวนความเข้าใจอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ หากหน่วยงานใกล้เคียง เช่น สำนักงานปลัดกระทรวงการคลัง และสำนักงานเศรษฐกิจการคลัง เป็นต้น กำหนดแผนการซ่อมกรณีไฟไหม้ ต้องส่งเจ้าหน้าที่ผู้รับผิดชอบของ สบन. เข้าร่วมในการซ่อมด้วย

ภาคผนวก ง

ผู้รับผิดชอบดูแลอุปกรณ์และระบบเทคโนโลยีสารสนเทศ

ที่	อุปกรณ์	ครรชิต	ดำรงส	อรรวรรณ	พิรวัชร	หญญ
1	อุปกรณ์ประเภท Firewall	×		×		
2	อุปกรณ์ด้านเครือข่าย Network	×		×	×	
3	เครื่องคอมพิวเตอร์แม่ข่าย (Server)	×		×		
4	อุปกรณ์ SSL & Radius	×		×		
5	อุปกรณ์จัดเก็บข้อมูล (Storage)	×		×		
6	เครื่องคอมพิวเตอร์ตั้งโต๊ะ (PC)	×	×	×	×	
7	อุปกรณ์ Infoblox (DNS & DHCP)	×		×		
8	อุปกรณ์กระจายสัญญาณ (Switch)	×		×		
9	อุปกรณ์ Video Conference	×		×	×	
10	อุปกรณ์ PDMO Channel	×		×		×

ที่	ระบบเทคโนโลยีสารสนเทศ	ครรชิต	ดำรงส	อรรวรรณ	พิรวัชร	หญญ
1	ระบบฐานข้อมูลศูนย์ข้อมูลที่ปรึกษา (www.consultant.pdmo.go.th)	×	×	×		
2	ระบบงานจัดอันดับความเสี่ยงทางเครดิตของรัฐวิสาหกิจ (Credit Scoring)	×	×	×		
3	ระบบบริหารจัดการโครงการลงทุนด้านโครงสร้างพื้นฐาน (Infrastructure Investment Project Management : IIPM)	×	×	×		
4	ระบบบริหารจัดการโครงการเงินกู้เพื่อฟื้นฟูเศรษฐกิจและ พัฒนาโครงสร้างพื้นฐาน (e-DPL)	×	×	×		
5	ระบบสารสนเทศทรัพยากรบุคคลระดับกรม (DPIS)	×		×		
6	ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ (GFMIS)	×	×	×		
7	ระบบบริหารหนี้สาธารณะ (GFMIS-TR)	×	×	×		
8	ระบบบริหารจัดการข้อมูลการบริหารการชำระหนี้ (DMTR)	×		×		
9	ระบบงานสร้างแบบจำลองความเสี่ยงด้านหนี้สาธารณะ (Risk Model)	×	×	×		
10	ระบบการคำนวณค่าธรรมเนียมการค้ำประกันและการให้กู้ต่อ (Credit Fee)	×	×	×		
11	ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)	×	×	×	×	
12	ระบบสำนักงานอัจฉริยะ (Smart Office)	×	×	×	×	×

ที่	ระบบเทคโนโลยีสารสนเทศ	ครุฑ	ตำรวจ	อรรณ	พิวั	หฤ
13	ระบบประชุมทางไกล Video Conference	×		×		
14	3.5 ระบบติดต่อสื่อสารภายในองค์กร (Microsoft Lync)	×		×	×	×
15	ระบบลงเวลาปฏิบัติงานด้วยนิ้วมือ	×		×		
16	ระบบบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (EFS)	×	×	×	×	
17	ระบบเว็บไซต์สำนักงานบริหารหนี้สาธารณะ (www.pdmo.go.th)	×	×	×	×	×
18	ระบบเว็บไซต์กองทุนบริหารเงินกู้เพื่อการปรับโครงสร้างหนี้ สาธารณะและพัฒนาตลาดตราสารหนี้ในประเทศ (กปพ.) (www.pddf.or.th)	×				×
19	ระบบสารสนเทศเชิงบูรณาการด้านการตรวจสอบภายใน (Internal Audit) และการจัดการความรู้ (KM)	×	×	×	×	×
20	ระบบสารสนเทศเพื่อการพัฒนากระบวนการและข้อมูล ด้านหนี้สาธารณะให้รองรับเทคโนโลยีที่เกี่ยวข้องกับการเงิน (Financial Technology : FIN-TECH)	×	×	×	×	×
21	ระบบอิเล็กทรอนิกส์ เพื่อเข้าสู่ Mobile Platform	×				
22	ระบบเว็บไซต์ภายใน (Intranet)	×	×	×	×	×
23	ระบบ PDMO Channel	×	×	×		×
24	ระบบติดตามการเตือนภัยการบริหารผลการดำเนินงาน ตัวชี้วัด (KPI)	×	×			×
25	ศูนย์ข้อมูลข่าวสาร	×	×	×		×
26	ศูนย์รับเรื่องร้องเรียน	×	×	×		×

ที่	ระบบสำรอง	ครุฑ	ตำรวจ	อรรณ	พิวั	หฤ
1	ระบบไฟฟ้าสำรอง	×	×	×	×	
2	ระบบสำรองข้อมูล	×	×	×	×	

ผู้รับผิดชอบการจัดทำแผนและทบทวนแผน

ส่วนนโยบายและแผนสารสนเทศ

ภาคผนวก จ

ข้อปฏิบัติและหลักเกณฑ์ในการควบคุมการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่มีขั้นตอนการปฏิบัติดังนี้

1. ผู้ใช้งานต้องลงทะเบียนตามแบบ ศทส. 03 โดยจะได้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งาน
2. ผู้ใช้งานต้องทำการ Log-out ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
3. ผู้ใช้งานมีหน้าที่รับผิดชอบในการ Update โปรแกรมป้องกันไวรัสอย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
4. ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่
5. หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้
6. ผู้ใช้งานควรจะทำสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล
7. ผู้ใช้งานไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่
8. หากผู้ใช้งานลาออกจะต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบทันที เพื่อป้องกันการสวมสิทธิ