ประกาศสำนักงานบริหารหนี้สาธารณะ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
และการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2567

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 มาตรา 6 และมาตรา 7 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 45 กำหนดให้หน่วยงานของรัฐมีหน้าที่ดำเนินมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ 1 ในประกาศนี้

“สำนักงาน” หมายถึง สำนักงานบริหารหนี้สาธารณะ

“นโยบาย” หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่สำนักงานจัดไว้ให้บริการประชาชน ซึ่งสำนักงานประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานที่เกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับประกาศแนบท้ายพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้บังคับ

“แนวปฏิบัติ” หมายถึง ขั้นตอนวิธีการที่สำนักงานได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของเจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมีจุดมุ่งหมายเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์นั้น มีวิธีการที่มั่นคงปลอดภัย

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

“บัญชีผู้ใช้งาน” หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

/**“สินทรัพย์”** ...

“สินทรัพย์” หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

“สินทรัพย์คอมพิวเตอร์” หมายความว่า โปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดในบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“สารสนเทศ” หมายถึง ข้อมูลในรูปแบบต่างๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจ หรือใช้ประโยชน์ต่าง ๆ ตามภารกิจของสำนักงาน

“เครือข่าย” หมายความว่า ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ 2 เครื่องขึ้นไปเข้าด้วยกัน เพื่อสะดวกต่อการร่วมใช้ข้อมูล โปรแกรม หรือเครื่องพิมพ์ และอำนวยความสะดวกในการติดต่อแลกเปลี่ยนข้อมูลระหว่างเครื่องได้ตลอดเวลา

“ผู้ดูแลระบบ” หมายถึง เจ้าหน้าที่ที่มีหน้าที่รับผิดชอบในการเป็นผู้ดูแล บริหารจัดการ และรักษาสินทรัพย์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศต่าง ๆ

“หน่วยงานภายนอก” หมายถึง หน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

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

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตัวอย่างข้อมูลเกี่ยวกับบุคคลในที่นี้ เช่น ชื่อ-นามสกุล อายุ วันเดือนปีเกิด สถานภาพสมรส หรือเลขประจำตัวประชาชน เป็นต้น โดยรวมถึงข้อมูลของอุปกรณ์ทางอิเล็กทรอนิกส์ เช่น IP address, MAC address หรือ Cookie ID เป็นต้น ที่บุคคลนั้นๆ ใช้งาน

/“ไซเบอร์” ...

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ข้อ 2 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน แบ่งเป็น 2 ส่วน ได้แก่

ส่วนที่ 1 แนวนโยบาย

ส่วนที่ 2 แนวปฏิบัติ

รายละเอียดภายในของทั้งสองส่วน ประกอบด้วยเนื้อหาสาระสำคัญในประเด็นต่อไปนี้

(1) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศตามเป้าหมายครอบคลุม 4 เรื่อง ดังนี้

- การเข้าถึงสารสนเทศ
- การเข้าถึงระบบเครือข่าย
- การเข้าถึงระบบปฏิบัติการ
- การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(2) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

(4) การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจต้องมีแนวปฏิบัติในการบริหารจัดการสิทธิในแต่ละกลุ่ม รวมถึงการระงับสิทธิ

(5) การกำหนดกฎเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

/ข้อ 3 ...

ข้อ 3 ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานให้เป็นไปตามที่กำหนดไว้ในแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง พ.ศ. 2567

ข้อ 4 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ รวมถึงจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ (IT Contingency Plan) โดยกำหนดให้มีการตรวจสอบ และควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ และตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานอย่างน้อยปีละ 1 ครั้ง โดยกลุ่มตรวจสอบภายในของสำนักงาน

ข้อ 5 สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานของสำนักงาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการ ดังนี้

(1) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์สำนักงานและบอร์ดประชาสัมพันธ์ให้แก่ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

(2) จัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงโดยผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ 6 มีการควบคุมการเข้าถึงสารสนเทศและข้อมูลคอมพิวเตอร์โดยคำนึงถึงการใช้งาน ชั้นความลับและความมั่นคงปลอดภัยเป็นสำคัญ โดยการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้ทดแทน

ข้อ 7 กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่สำนักงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล ให้ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ 8 ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือที่กฎหมายอื่นกำหนดไว้

/ข้อ 9 ...

ข้อ 9 ให้ศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ รวมถึงกำหนดให้มีการปฏิบัติที่ชัดเจนและให้มีการทบทวนนโยบายและแนวปฏิบัติเป็นประจำทุกปีเพื่อให้มีความครบถ้วน สมบูรณ์ เป็นไปตามเจตนารมณ์ของกฎหมายที่กำหนดไว้และในกรณีที่มีการปรับปรุง/แก้ไขนโยบายหรือแนวปฏิบัติ ให้แจ้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ทราบด้วย

ประกาศ ณ วันที่ 31 กรกฎาคม พ.ศ. 2567

(นายพชร อนันตศิลป์)

ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง พ.ศ. 2567

ศูนย์เทคโนโลยีสารสนเทศ
สำนักงานบริหารหนี้สาธารณะ

คำนำ

สำนักงานบริหารหนี้สาธารณะ (สบน.) ได้ออกประกาศ เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล และแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567 เพื่อเป็นส่วนหนึ่งของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ และการรักษาความมั่นคงปลอดภัยไซเบอร์ ในการป้องกันภัยคุมคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้สารสนเทศมีความปลอดภัย สามารถรักษาความลับ ความถูกต้องของข้อมูล และเพื่อให้มีแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศในการให้บริการอิเล็กทรอนิกส์ภาครัฐและสอดคล้องตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยได้ทำการทบทวนและปรับปรุงเนื้อหาเพิ่มเติมให้เป็นปัจจุบัน

แนวปฏิบัติที่กำหนดต่อไปนี้ เป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติเพื่อให้การให้บริการต่าง ๆ ตามภารกิจของ สบน. ที่ดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ และเพื่อให้ง่ายต่อการนำไปปฏิบัติหรืออ้างอิง จึงแบ่งแนวปฏิบัติออกเป็น 12 หมวด ดังนี้

หมวด 1 แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ
หมวด 2 แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึงของผู้รับผิดชอบระบบ
หมวด 3 แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ
หมวด 4 แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน
หมวด 5 แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบสารสนเทศ/ผู้ดูแลระบบเครือข่าย
หมวด 6 แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย
หมวด 7 แนวปฏิบัติในการใช้งาน Token Key และ GFMIS Smart Card
หมวด 8 แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน
หมวด 9 แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
หมวด 10 แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์
หมวด 11 แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ
หมวด 12 แนวปฏิบัติในการเผยแพร่ข้อมูลต่อสาธารณะ

สารบัญ

หมวด 1
แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

ข้อ 1 ผู้รับผิดชอบระบบสารสนเทศของสำนักงานบริหารหนี้สาธารณะ (สบน.) ต้องมีหน้าที่บริหารจัดการควบคุมการเข้าถึงระบบสารสนเทศ ดังนี้

1.1 ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศได้ก็ต่อเมื่อได้รับอนุญาตจากผู้ดูแลระบบ หรือผู้รับผิดชอบระบบงานตามหน้าที่การปฏิบัติงานเท่านั้น

1.2 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบกล่าวคือในการขออนุญาตเข้าใช้งานระบบงาน ผู้ใช้จะต้องทำบันทึกและกรอกเอกสารที่ สบน. กำหนดเพื่อขอเข้าใช้งานระบบ และให้ผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาลงนามอนุมัติเอกสารดังกล่าวเพื่อจัดเก็บไว้เป็นหลักฐาน จากนั้นผู้ดูแลระบบจะสร้างบัญชีสำหรับการเข้าถึงโดยอนุญาตเฉพาะในส่วนที่จำเป็นโดยคำนึงถึงประเภทข้อมูลและชั้นความลับเป็นหลัก

1.3 ผู้ดูแลระบบต้องกำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้ หากผู้ใช้งานใส่รหัสผ่าน (Password) เพื่อเข้าใช้งานผิด 3 ครั้ง ระบบจะยกเลิกสิทธิการใช้งาน (Block) ไม่ให้ผู้ใช้งานสามารถใช้งานได้จนกว่าผู้ใช้งานจะยื่นเรื่องพร้อมหลักฐานแสดงต่อเจ้าหน้าที่ดูแลระบบ เพื่อขอรหัสใหม่อีกครั้ง

1.4 ผู้ดูแลระบบต้องกำหนดให้การเข้าใช้ระบบ (Login) เพื่อเข้าใช้งานใด ๆ จะต้องมีการตรวจจับการเปิดระบบงานไว้ เมื่อไม่มีการใช้งานก็ต้องออกจากระบบ (Logout) หรือให้ใช้งานระบบ Logout อัตโนมัติตามระยะเวลาที่เหมาะสม

1.5 ผู้ดูแลระบบต้องอนุญาตให้ผู้ใช้งานเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและระบบสารสนเทศในส่วนที่จำเป็นตามหน้าที่การปฏิบัติงานเท่านั้น 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. สามารถใช้งานได้ตลอด 24 ชั่วโมง

1.7 กรณีมีการจ้างผู้ให้บริการภายนอก (Outsource) ในการพัฒนา ดูแล และบำรุงรักษาระบบสารสนเทศ มีมาตรการควบคุม ดังนี้

(1) กำหนดเกณฑ์และคัดเลือกผู้ให้บริการภายนอกที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการ และมีขั้นตอนการปฏิบัติงานที่รอบคอบ รัดกุม และน่าเชื่อถือ

(2) กำหนดข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้ให้บริการภายนอก และต้องระบุการรักษาความลับของข้อมูล กำหนดขอบเขตงานและเงื่อนไขในการให้บริการอย่างชัดเจน

(3) กรณีใช้บริการด้านการพัฒนาระบบงาน กำหนดให้ผู้ให้บริการภายนอกเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงานเท่านั้น และหากมีความจำเป็นที่ผู้ให้บริการภายนอกเข้ามาปฏิบัติหน้าที่ภายในสำนักงาน ต้องมีเจ้าหน้าที่ของหน่วยงานควบคุมดูแลอย่างใกล้ชิด

(4) กำหนดให้ผู้ให้บริการภายนอกจัดทำคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

(5) กำหนดให้ผู้ให้บริการภายนอกรายงานแผนและผลการปฏิบัติงาน ปัญหาและอุปสรรคต่าง ๆ และแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

(6) กำหนดให้มีหลักเกณฑ์ กระบวนการ และขั้นตอนในการตรวจรับงานที่ส่งมอบโดยผู้ให้บริการภายนอกที่ชัดเจน

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

2.1 กำหนดระดับความสำคัญของพื้นที่ หรือจำแนกพื้นที่การใช้งานกับพื้นที่การควบคุม

2.2 ทดสอบระบบควบคุมการเข้าถึงพื้นที่ทางกายภาพเพื่อให้ทราบว่าระบบยังใช้งานได้ตามปกติหรือไม่

2.3 ผู้ปฏิบัติงานควรปิดประตูและหน้าต่างให้สนิทอยู่เสมอ

ข้อ 3 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องมีหน้าที่บริหารจัดการควบคุมพื้นที่การเข้า - ออกพื้นที่การควบคุม ได้แก่ ห้องปฏิบัติการคอมพิวเตอร์ (Server Room) ดังนี้

3.1 มีการบันทึกวันและเวลาการเข้า - ออกพื้นที่การควบคุมของผู้มาเยือน (Visitor)

3.2 ดูแลผู้มาเยือนในพื้นที่หรือบริเวณที่มีการควบคุมจนกระทั่งเสร็จสิ้นภารกิจและกลับไปเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

3.3 จัดให้มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของ สบน. โดยบุคคลภายนอกและควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

3.4 จัดสื่อประชาสัมพันธ์เพื่อสร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

3.5 มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

3.6 ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ ได้แก่ ห้องปฏิบัติการคอมพิวเตอร์ (Server Room) เป็นต้น เว้นแต่ได้รับอนุญาต

3.7 มีการยืนยันตัวตน ได้แก่ การแสดงบัตรผ่าน การใช้บัตรแถบแม่เหล็ก การสแกนลายนิ้วมือ เป็นต้น เพื่อควบคุมการเข้า - ออกในพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาห้องปฏิบัติการคอมพิวเตอร์ (Server Room)

3.8 จัดเก็บบันทึกการเข้า - ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะห้องปฏิบัติการคอมพิวเตอร์ (Server Room) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

3.9 บุคคลภายนอก ได้แก่ เจ้าหน้าที่บริษัท นักศึกษาฝึกงาน หรือผู้ได้รับการว่าจ้างอื่น ๆ และผู้มาเยือน ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน หรือเยี่ยมชมอยู่ภายใน สบน.

3.10 ควรจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

3.11 จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

3.12 ควบคุมบริเวณ ได้แก่ จุดรับส่งของ เป็นต้น หรือมีการแยกบริเวณดังกล่าวออกจากพื้นที่ที่มีการติดตั้ง จัดเก็บ หรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศเพื่อหลีกเลี่ยงการเข้าถึงโดยมิได้รับอนุญาตของผู้ไม่มีสิทธิเข้าถึง และ/หรือผู้ที่อาจสามารถเข้าถึงระบบสารสนเทศได้

3.13 ห้ามบันทึกภาพ/วีดิทัศน์ใด ๆ ในห้องปฏิบัติการคอมพิวเตอร์ (Server Room) โดยมิได้รับอนุญาตหรือหากจำเป็นต้องบันทึกภาพ/วีดิทัศน์ การกระทำนั้นต้องอยู่ภายใต้การควบคุมดูแลของผู้รับผิดชอบระบบสารสนเทศของ สบน.

ข้อ 4 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดการจัดวางและการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (Hardware) ดังนี้

4.1 จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงของบุคคลภายนอก

4.2 ระบบงานที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่มีความมั่นคงปลอดภัยเพียงพอ

4.3 ไม่ให้มีการนำอาหาร เครื่องดื่ม หรือสูบบุหรี่ภายในบริเวณห้องปฏิบัติการคอมพิวเตอร์ (Server Room)

4.4 ตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว ได้แก่ การตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติอยู่เสมอ

ข้อ 5 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดให้มีระบบป้องกันและสนับสนุนการทำงาน ดังนี้

5.1 มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อความต้องการใช้งาน โดยให้มีอย่างน้อย ดังนี้

(1) ระบบสำรองกระแสไฟฟ้า (UPS)

(2) ระบบระบายอากาศ

(3) ระบบปรับอากาศ และควบคุมความชื้น

5.2 ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนอย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

5.3 ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องปฏิบัติการคอมพิวเตอร์ (Server Room) ทำงานผิดปกติหรือหยุดการทำงาน

ข้อ 6 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดและควบคุมการเดินสายไฟฟ้า สายสัญญาณการสื่อสาร และสายเคเบิ้ลอื่น ๆ ดังนี้

6.1 เครือข่ายภายใน สบน. ในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ต้องให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณ และป้องกันสัตว์ต่าง ๆ กัดสาย ได้แก่ หนู แมลงสาบ เป็นต้น ซึ่งจะทำให้เกิดความเสียหายต่อสายสัญญาณ

6.2 ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

6.3 จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

6.4 ตู้ Rack ที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

ข้อ 7 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดการบำรุงรักษาอุปกรณ์ ดังนี้

7.1 กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

7.2 ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

7.3 จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

7.4 จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

7.5 ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายใน สบน.

7.6 จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ 8 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องควบคุมการนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่น ๆ ออกจาก สบน. ดังนี้

8.1 ให้มีการขออนุญาตก่อนนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่น ๆ ออกจาก สบน.

8.2 บันทึกข้อมูลการนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่น ๆ ออกจาก สบน. เพื่อรวบรวมไว้เป็นหลักฐานป้องกันการสูญหาย และบันทึกข้อมูลเพิ่มเติมเมื่อนำส่งคืน

ข้อ 9 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องบริหารจัดการควบคุมอุปกรณ์ที่ใช้งานอยู่ภายนอก สบน. ดังนี้

9.1 กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่น ๆ ของ สบน. ออกไปใช้งานนอกสถานที่ ดังนี้

(1) ห้ามผู้ใช้งานละทิ้งเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่น ๆ ของ สบน. ไว้โดยลำพังในที่สาธารณะ

(2) ให้ผู้ใช้งานรับผิดชอบดูแลเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่น ๆ ของ สบน. เสมือนเป็นทรัพย์สินของตนเอง

ข้อ 10 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องควบคุมการจำหน่ายอุปกรณ์จัดเก็บข้อมูลเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่าย หรือการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

10.1 ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะแทงจำหน่ายอุปกรณ์ดังกล่าว ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูล ในหมวด 3 แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ข้อ 1.2 (16)

10.2 มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์จัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวด 2
แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึงของผู้รับผิดชอบระบบ

ข้อ 1 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน ดังนี้

1.1 การลงทะเบียนบุคลากร ต้องปฏิบัติตามขั้นตอนลงทะเบียนที่ สบน. กำหนดขึ้น เพื่อให้มีสิทธิในการใช้งานระบบสารสนเทศตามความจำเป็นรวมทั้งปฏิบัติตามขั้นตอนการบริหารจัดการสิทธิ์ของบุคลากรภายในและภายนอก สบน. ดังนี้

1.1.1 บุคลากรภายใน สบน.

(1) สำนัก/ศูนย์/กลุ่มของผู้ที่ต้องการใช้งานระบบ มีหนังสือถึงสำนัก/ศูนย์/กลุ่มของผู้ดูแลระบบ เพื่อแจ้งรายชื่อบุคลากรที่ได้รับมอบหมายให้เป็นผู้ใช้งานระบบ

(2) ผู้ใช้งานนำเข้าข้อมูลเพื่อขอสิทธิ์เข้าใช้งานระบบผ่าน Google Form หรือตามแบบฟอร์มที่กำหนด เมื่อผู้ดูแลระบบได้รับหนังสือจากสำนัก/ศูนย์/กลุ่มแล้ว จึงตรวจสอบความถูกต้องตรงกันกับรายชื่อผู้ใช้งานที่ขอสิทธิ์เข้าใช้งานระบบผ่าน Google Form ที่ได้รับ

(3) ผู้ดูแลระบบกำหนดรหัสผู้ใช้งาน รหัสผ่าน และสิทธิ์การใช้งานให้แก่ผู้ใช้งาน หลังจากนั้นผู้ดูแลระบบจะแจ้งข้อมูลให้ผู้ใช้งานแต่ละรายทราบโดยตรงทาง E-Mail ที่แจ้งไว้ใน Google Form หรือตามแบบฟอร์มที่กำหนด

(4) สำหรับระบบงานพื้นฐาน ให้ผู้ใช้งานนำเข้าข้อมูลการขอสิทธิ์ใช้ระบบผ่าน Google Form หรือตามแบบฟอร์มที่กำหนด เมื่อนำเข้าข้อมูลเรียบร้อยแล้ว ศทส. จะดำเนินการตรวจสอบข้อมูลให้ถูกต้องตรงกันระหว่างข้อมูลจาก Google Form หรือตามแบบฟอร์มที่กำหนด และข้อมูลจากส่วนทรัพยากรบุคคลจากนั้นจะทำการเพิ่มข้อมูลผู้ใช้งานในระบบฐานข้อมูลผู้ใช้งาน (Active Directory : AD) กำหนดรหัสผู้ใช้งาน รหัสผ่าน และสิทธิ์การใช้งานให้แก่ผู้ใช้งาน เมื่อดำเนินการแล้วเสร็จ จะแจ้งผู้ใช้งานแต่ละรายทราบทาง E-Mail

1.1.2 บุคคลภายนอก สบน.

(1) หน่วยงานของผู้ที่ต้องการใช้งานระบบ มีหนังสือถึง สบน. เพื่อแจ้งรายชื่อบุคลากรที่ได้รับมอบหมายให้เป็นผู้ใช้งานระบบ

(2) ผู้ใช้งานนำเข้าข้อมูลเพื่อขอสิทธิ์เข้าใช้งานระบบผ่าน Google Form หรือตามแบบฟอร์มที่กำหนด พร้อมแนบไฟล์เอกสารที่กำหนด เช่น สำเนาบัตรประจำตัวประชาชน เป็นต้น เมื่อผู้ดูแลระบบได้รับหนังสือจากหน่วยงานภายนอกแล้ว จึงนำมาตรวจสอบ ความถูกต้องตรงกันกับรายชื่อผู้ใช้งานที่ขอสิทธิ์เข้าใช้งานผ่าน Google Form หรือตามแบบฟอร์มที่กำหนด ที่ได้รับ

(3) ผู้ดูแลระบบกำหนดรหัสผู้ใช้งาน รหัสผ่าน และสิทธิ์การใช้งานให้แก่ผู้ใช้งาน หลังจากนั้นผู้ดูแลระบบจะแจ้งข้อมูลให้ผู้ใช้งานแต่ละรายทราบโดยตรงทาง E-Mail ที่แจ้งไว้ใน Google Form หรือตามแบบฟอร์มที่กำหนด

1.1.3 กรณีเจ้าหน้าที่ไม่ได้ปฏิบัติงานภายใน สบน หรือเปลี่ยนตำแหน่งงาน ผู้ดูแลระบบจะปรับปรุงสิทธิการใช้งาน

1.2 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ 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 หลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

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) จัดส่งรายชื่อนั้นให้ผู้บังคับบัญชาของหน่วยงานภายใน สบน. เพื่อให้ทบทวนว่ายังมีรายชื่อของผู้ที่โอน/ลาออกไปแล้ว หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้อง

(3) ผู้บังคับบัญชาของหน่วยงานภายใน สบน. แจ้งกลับว่ามีรายชื่อใดที่ต้องปรับปรุงแก้ไขให้ถูกต้อง

(4) แก้ไขข้อมูลสิทธิให้ถูกต้องตามที่ได้รับแจ้ง (ถ้ามี)

ข้อ 3 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดให้มีการยืนยันตัวตนผู้ใช้งาน โดยผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานต้องผ่านการยืนยันตัวตนจากระบบ โดยมีแนวทางปฏิบัติ ดังนี้

3.1 การแสดงตัวตนด้วยชื่อบัญชีผู้ใช้งาน (User Account)

3.2 การยืนยันตัวตนด้วยการใช้รหัสผ่าน (Password)

3.3 การเข้าใช้ระบบงานสำคัญของ สบน. ผ่านเครือข่ายอินเทอร์เน็ต จะมีการตรวจสอบผู้ใช้งานด้วย

3.4 การเข้าใช้ระบบงานสำคัญของ สบน. จากระยะไกล (Remote Access) จะมีการตรวจสอบเพื่อเพิ่มความปลอดภัยและเพื่อพิสูจน์ตัวตนของผู้ใช้งาน ได้แก่ รหัสผ่าน หรือวิธีการเข้ารหัสลับ เป็นต้น

3.5 การใช้งานระบบสารสนเทศ เมื่อมีการว่างเว้นจากการใช้งานเกินเวลา 5 นาที ระบบจะทำการยกเลิกการใช้งานและการเชื่อมต่อเข้าระบบโดยอัตโนมัติ

ข้อ 4 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดวิธีการใช้รหัสผ่านให้มีความมั่นคงปลอดภัย ดังนี้

4.1 การบริหารจัดการรหัสผ่าน มีมาตรการและการควบคุม ดังนี้

(1) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 6 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(2) มีการเก็บหรือจัดการกับรหัสผ่านที่มีความปลอดภัยจากการถูกแฮก

(3) หลีกเลี่ยงการตั้งรหัสผ่านเดียวกันหลาย ๆ ระบบ

(4) ปิดการใช้งาน “hint” หรือคำใบ้ของรหัสผ่าน

(5) กำหนดให้ต้องเปลี่ยนรหัสผ่านทุก 6 เดือน

(6) กำหนดให้การเข้าใช้งานระบบครั้งแรกมีการโต้ตอบด้วยการยืนยันตัวตนและเปลี่ยนรหัสผ่านเพื่อเพิ่มความปลอดภัย

(7) กรณีผู้ใช้งานเปลี่ยนหน้าที่ความรับผิดชอบหรือลาออกจะต้องเปลี่ยนหรือถอดถอนสิทธินั้นทันทีเมื่อได้รับแจ้ง

4.2 การใช้รหัสผ่าน มีมาตรการให้ผู้ใช้งานต้องใช้ด้วยความระมัดระวัง ดังนี้

(1) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(2) ไม่ใช้โปรแกรมสำนักงานคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

(3) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(4) กำหนดรหัสผ่านให้ยากต่อการคาดเดา

(5) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เนื่องจากความจำเป็นในการปฏิบัติงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(6) กรณีผู้ใช้งานลาออกหรือเปลี่ยนหน้าที่ความรับผิดชอบ ต้องแจ้งให้ ศทส. ทราบทันทีเพื่อระงับบัญชีผู้ใช้

ข้อ 5 การใช้รหัสผ่านให้ปลอดภัย มีมาตรการในการปฏิบัติ ดังนี้

5.1 แสดงกระบวนการมอบอำนาจหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

5.2 มีการกำหนดสิทธิการเข้าถึงตามความจำเป็น

5.3 มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

5.4 มีวิธีเลือกการใช้รหัสผ่านและการใช้งานรหัสผ่านที่มีคุณภาพ

หมวด 3
แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ข้อ 1 ผู้บังคับบัญชาหน่วยงานภายใน สบน. ต้องจัดให้มีวิธีการกำหนดประเภทข้อมูลและจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ซึ่งเบื้องต้นใช้แนวทางตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และระเบียบที่เกี่ยวข้องในการกำหนดชั้นความลับของข้อมูล จึงกำหนดให้มีแนวทางปฏิบัติ ดังนี้

1.1 ผู้ใช้งานต้องแบ่งประเภทของข้อมูลและชั้นความลับของข้อมูลตามที่ ศทส. ได้กำหนดชั้นความลับของข้อมูลเป็น 4 ระดับ ดังนี้

(1) ชั้นความลับ (Top secret/Secret/Confidential)

(2) ใช้ภายในเท่านั้น (Internal Use)

(3) ส่วนบุคคล (Personal)

(4) เปิดเผยได้ (Public)

1.2 ผู้ใช้งานต้องพิจารณาองค์ประกอบต่อไปนี้เพื่อเป็นแนวทางกำหนดชั้นความลับของข้อมูล

(1) ความสำคัญของเนื้อหา ได้แก่ เนื้อหาของข้อมูลนั้นมีความสำคัญต่อความสำเร็จของงานตามภารกิจของ สบน. มากน้อยเพียงใด หากมีความสำคัญสูง ข้อมูลนั้นจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือลับ เป็นต้น

(2) แหล่งที่มาของข้อมูล ได้แก่ หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับชั้นความลับจะต้องคงไว้ตามเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับจะเป็นประเภทเปิดเผยได้ เป็นต้น

(3) วิธีการนำไปใช้ประโยชน์ ได้แก่ หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบด้านการเงินของ สบน. ดังนั้น ข้อมูลนี้จะอยู่ในประเภทชั้นความลับ เป็นต้น

(4) จำนวนบุคคลที่ควรรับทราบ ได้แก่ หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้ เป็นต้น

(5) ผลกระทบหากมีการเปิดเผย ได้แก่ หากข้อมูลนั้นถูกเปิดเผย จะมีผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการเงิน ด้านการปฏิบัติตามกฎระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้น ข้อมูลสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในหรือลับ เป็นต้น

(6) หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่อง ได้แก่ ข้อมูลสำคัญหรือข้อมูลลับที่มาจากเจ้าของเรื่องใดจะต้องคงชั้นความลับไว้ตามเดิม การนำไปใช้งานควรขออนุญาตจากผู้ที่เป็นเจ้าของเรื่องก่อน เป็นต้น

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

- ลับที่สุด หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงานอย่างร้ายแรงที่สุด
- ลับมาก หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงานอย่างร้ายแรง
- ลับ หมายความถึง 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 ได้แก่ จัดทำภายใน สบน. ไม่จัดทำในสถานที่สาธารณะซึ่งบุคคลภายนอกสามารถเห็นข้อมูลที่จัดทำได้ และจำกัดบุคคลเฉพาะผู้ที่เกี่ยวข้องในการเข้าถึงข้อมูล

- ในการจัดทำข้อมูลลับซึ่งใช้กระดาษหรือวัสดุชั่วคราว ได้แก่ กระดาษร่าง กระดาษคาร์บอน ต้องทำลายกระดาษหรือวัสดุนั้นทันทีที่จัดทำเสร็จเรียบร้อย ถ้าเป็นการจัดทำโดยใช้เครื่องคอมพิวเตอร์ จะต้องลบหรือทำลายสื่อบันทึกข้อมูลจนไม่สามารถนำไปใช้ประโยชน์ได้ (ดูวิธีการทำลายในตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูลในข้อ (16) ที่จะกล่าวต่อไป) หากไม่ทำลายต้องเก็บรักษาไว้ในสถานที่ที่ปลอดภัย

- จัดทำข้อมูลโดยแสดงเลขที่หน้าของจำนวนหน้าทั้งหมดไว้ในทุกหน้าของข้อมูลลับ และแสดงไว้ในส่วนที่สามารถเห็นได้ชัดเจน ได้แก่ มุมขวาด้านบนของเอกสาร (การบันทึกเลขหน้ามีจุดประสงค์ เพื่อให้ทราบว่าข้อมูลลับนั้นเป็นหน้าใดของจำนวนทั้งหมด หากมีการสูญหายไปหน้าใดหน้าหนึ่งจะได้ทราบและสามารถติดตามหาผู้ละเมิดและหาทางลดหรือแก้ไขความเสียหายที่เกิดขึ้นได้)

(11) ในการแสดงชั้นความลับบนข้อมูลลับ ให้ปฏิบัติ ดังนี้

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

- แสดงชั้นความลับบนเอกสารลับในทุกหน้าของเอกสารให้ปรากฏเห็นอย่างเด่นชัด

(12) ในการทำสำเนาหรือแจกจ่ายข้อมูลลับให้ปฏิบัติ ดังนี้

- ทำสำเนาหรือแจกจ่ายข้อมูลลับให้แก่ผู้รับปลายทางซึ่งเป็นผู้ที่มีสิทธิ ในการเข้าถึงข้อมูลตามที่ระบุไว้ในทะเบียนข้อมูลลับ หรือสามารถแจกจ่ายให้ได้ตามความจำเป็นในการเข้าถึงข้อมูลนั้น

- แจ้งให้หน่วยงานภายนอกที่อนุญาตให้เข้าถึงข้อมูลลับนั้นได้ ว่าไม่อนุญาตให้ทำสำเนาเพิ่มเติม เว้นเสียแต่ได้รับอนุญาตจากผู้มีอำนาจลงนามอนุญาตก่อน

(13) ในการเก็บรักษาเอกสารลับให้ปฏิบัติ ดังนี้

- จัดเก็บเอกสารลับไว้ในแฟ้มข้อมูลลับ และนำไปเก็บไว้ในตู้เก็บเอกสารลับโดยแยกเก็บเป็นแต่ละเรื่องหรือแต่ละหัวข้อ

- ไม่จัดเก็บเอกสารลับร่วมกับเอกสารที่อยู่ในชั้นความลับอื่น ๆ ได้แก่ ข้อมูลใช้ภายในเท่านั้น ข้อมูลส่วนบุคคล หรือข้อมูลที่เปิดเผยได้

- จัดเก็บแฟ้มข้อมูลลับไว้ในตู้และปิดล็อคด้วยกุญแจที่แข็งแรงและมั่นคง

(14) ในการยืมหรือขอเข้าถึงข้อมูลลับให้ปฏิบัติ ดังนี้

- เมื่อมีการขอยืมหรือขอเข้าถึงข้อมูลลับโดยผู้อื่นที่ไม่ได้เป็นผู้มีสิทธิในการเข้าถึงข้อมูลตามทะเบียนข้อมูลลับ ให้หัวหน้าของส่วนงานที่รับผิดชอบเป็นผู้พิจารณาตรวจสอบคุณสมบัติของผู้ยืมหรือขอเข้าถึงก่อนว่าเป็นผู้มีอำนาจหน้าที่ที่เกี่ยวข้องหรือไม่ หรือมีความจำเป็นในการเข้าถึงข้อมูลนั้นหรือไม่พร้อมทั้งต้องทำบันทึกหลักฐานการยืมหรือการขอเข้าถึงข้อมูลนั้นด้วย และแจ้งให้ผู้ยืมหรือขอเข้าถึงทราบว่าห้ามทำสำเนาเพิ่มเติม

- เมื่อหมดความจำเป็นในการใช้งานแล้ว หัวหน้าของส่วนงานที่รับผิดชอบกำหนดให้ผู้ขอยืมจัดส่งข้อมูลนั้นกลับคืนมาโดยทันที สำหรับกรณีการเข้าถึงระบบเทคโนโลยีสารสนเทศให้ยกเลิกบัญชีผู้ใช้งานที่ขอเข้าถึงข้อมูลลับโดยทันที

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

(16) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ

ตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูล

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

(17) ในการจัดการกับไฟล์ข้อมูลลับให้ปฏิบัติ ดังนี้

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

- การสำเนา E-File ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูง ต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล

- ระมัดระวังการเผยแพร่ หรือแจกจ่าย E-File ที่เป็นความลับของ สบน. ไปยังกลุ่มผู้รับ ต้องเฉพาะกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

- ผู้เป็นเจ้าของ E-File ต้องตรวจสอบความถูกต้องของ E-File ก่อนนำไปใช้งาน

- ห้ามผู้เป็นเจ้าของ E-File ที่เป็นความลับ หรือที่มีระดับความสำคัญสูง ส่งข้อมูลดังกล่าวไปทางไปรษณีย์ เว้นแต่จะได้ใช้วิธีเข้ารหัสลับที่ สบน. กำหนดไว้

- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัยและไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์

- ห้ามแบ่งปัน (Share) ไฟล์ข้อมูลลับบนเครือข่ายสาธารณะ (Internet) ของ สบน. เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

- ตรวจสอบการทำงานของระบบป้องกันไวรัสในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับเป็นประจำทุก 30 วัน ว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมสำนักงานเพื่อแก้ไขช่องโหว่ของโปรแกรมในเครื่องตามปกติหรือไม่

- สำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ประจำทุก 30 วัน หรือตามความจำเป็น

- ต้องทำลาย E-File บนหน่วยความจำหลัก (Hard disk) ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

หมวด 4
แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

ข้อ 1 การใช้เครื่องคอมพิวเตอร์ภายใน สบน. ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

1.1 ห้ามใช้เครื่องคอมพิวเตอร์จนกว่าจะได้รับการอนุมัติให้ใช้งาน โดยให้กรอกข้อมูลขอใช้งานเครื่องคอมพิวเตอร์และเข้าถึงระบบงานของ สบน. ตามแบบฟอร์มพนักงานใหม่ผ่านระบบเครือข่ายภายใน (Intranet)

1.2 การใช้งานเครื่องคอมพิวเตอร์ต้องตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสและการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) ก่อนใช้งานทุกครั้ง หากพบว่าโปรแกรมดังกล่าวทำงานผิดปกติให้รีบแจ้ง ศทส. เพื่อดำเนินการแก้ไขโดยเร็ว

1.3 เครื่องคอมพิวเตอร์ที่ใช้ภายใน สบน. ให้ติดตั้งโปรแกรมมาตรฐานตามที่กำหนดไว้ท้ายระเบียบนี้ ห้ามเปลี่ยนแปลงหรือติดตั้งโปรแกรมเพิ่มเติม เว้นแต่จะได้รับความเห็นชอบจากหัวหน้าหน่วยงานภายใน สบน. เท่านั้น

ความในวรรคหนึ่ง ไม่ใช้บังคับแก่การเปลี่ยนแปลงหรือการติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมเพื่อทดลองการใช้งานซึ่งดำเนินการโดย ศทส. หรือผู้ที่ได้รับการว่าจ้างให้มาจัดทำหรือดูแลระบบเทคโนโลยีสารสนเทศของ สบน.

1.4 การติดตั้งซอฟต์แวร์ทุกครั้งต้องใช้สิทธิ์ผู้ดูแลระบบเสมอ

1.5 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์เพื่อไม่ให้บุคคลภายนอกสามารถใช้งานเครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ของ สบน. ได้

1.6 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกจากโปรแกรมตามมาตรฐานที่กำหนดไว้ (ในภาคผนวก ข)

1.7 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ในทรัพย์สินทางปัญญาของบุคคลอื่น

1.8 ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟท์แวร์ที่มีลิขสิทธิ์ถูกต้องของ สบน.

1.9 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่ายคอมพิวเตอร์

1.10 ต้องระมัดระวังการใช้งานและดูแลเครื่องคอมพิวเตอร์ รวมทั้งระบบเครือข่ายตามที่วิญญูชนทั่วไปจะพึงปฏิบัติ

1.11 เอกสารหรือข้อมูลต่าง ๆ ไม่ว่าจะอยู่ในรูปแบบใดก็ตามที่ได้มีการกำหนดเงื่อนไขการใช้งานไว้ต้องใช้งานด้วยความระมัดระวัง และต้องปฏิบัติตามเงื่อนไขอย่างเคร่งครัด เพื่อป้องกันมิให้เกิดการละเมิดตามกฎหมาย

1.12 ต้องลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์เพื่อประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

1.13 ต้องออกจากระบบ (Log off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์ รวมทั้งปิดเครื่องคอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

1.14 การติดตั้งโปรแกรมเพิ่มเติมที่มีลิขสิทธิ์และใช้ในการทำงาน โดยผ่านการกรอกแบบฟอร์มคำขอในระบบ

1.15 การนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้กับระบบเครือข่ายคอมพิวเตอร์ของ สบน. ต้องได้รับการตรวจสอบและอนุญาตจาก ศทส.

1.16 ตรวจสอบ (Scan) อุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable Media) ก่อนการใช้งานด้วยโปรแกรมป้องกันไวรัสเพื่อป้องกันโปรแกรมที่ไม่พึงประสงค์

ข้อ 2 การใช้เครื่องคอมพิวเตอร์แบบพกพา (Notebook) ของ สบน. นอกจากต้องปฏิบัติตามที่กำหนดไว้ในข้างต้นแล้ว ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

2.1 ต้องตรวจสอบเครื่องคอมพิวเตอร์แบบพกพาที่นำไปใช้ว่าได้ติดตั้งโปรแกรมคอมพิวเตอร์ตามมาตรฐานที่กำหนดไว้ท้ายระเบียบนี้แล้วหรือไม่ หากพบว่ายังไม่ได้ติดตั้งให้แจ้งผู้รับผิดชอบระบบสารสนเทศของ สบน. เพื่อขอรับการติดตั้งก่อนการใช้งาน

2.2 ต้องระมัดระวังไม่ให้บุคคลภายนอกมองเห็นหรือคัดลอกข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาที่นำไปใช้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

2.3 เมื่อหมดความจำเป็นที่ต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาแล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ผู้รับผิดชอบทันที ทั้งนี้ให้เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมในการใช้งานของเครื่องคอมพิวเตอร์ที่รับคืนไว้ดังกล่าวด้วย

ข้อ 3 ในกรณีที่เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนเครื่องคอมพิวเตอร์แบบพกพาตรวจพบความเสียหาย ให้แจ้งผู้บังคับบัญชาทราบโดยเร็ว และหากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทเลินเล่ออย่างร้ายแรงของผู้นำไปใช้ ต้องให้ผู้นำไปใช้รับผิดชอบต่อความเสียหายที่เกิดขึ้นดังกล่าว

ข้อ 4 การควบคุมการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

4.1 ผู้ใช้งานจะต้องยืนยันตัวตนด้วย User Account ของตนเองก่อนเข้าใช้งานระบบปฏิบัติการเครื่องคอมพิวเตอร์ทุกครั้ง

4.2 ผู้ใช้งานต้องไม่อนุญาตให้บุคคลอื่นใช้ User Account ของตนเองในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

4.3 ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมเพื่อล็อคหน้าจอโดยอัตโนมัติ หลังจากที่ไม่ได้ใช้งานเกินกว่า 15 นาที

4.4 ผู้ใช้งานควรทำการลงบันทึกออก (Log Off) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าเครื่องคอมพิวเตอร์ รวมทั้งปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเลิกใช้งาน

4.5 ผู้ใช้งานต้องไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

4.6 ผู้ใช้งานต้องกำหนดรหัสผ่านไม่น้อยกว่า 6 ตัวอักษร โดยไม่นำชื่อหรือนามสกุลของตนเองหรือคำที่ง่ายต่อการคาดเดามาตั้ง และต้องเปลี่ยนรหัสผ่านทุก 6 เดือน

ข้อ 5 การเข้าถึงระบบงานเทคโนโลยีสารสนเทศ เจ้าหน้าที่ใช้งานต้องปฏิบัติตามข้อกำหนด ดังนี้

5.1 กรอกแบบเพื่อขออนุมัติใช้งานคอมพิวเตอร์และเข้าสู่ระบบงานของ สบน. โดยผ่านการลงทะเบียนตามแบบฟอร์มพนักงานใหม่ในระบบ Intranet

5.2 ต้องไม่เข้าถึงระบบงานอื่นที่ไม่ได้รับอนุญาตให้ใช้งาน

5.3 ต้องออกจากระบบงานโดยทันที เมื่อใช้งานเสร็จสิ้น

5.4 ห้ามให้สิทธิการเข้าถึงระบบแก่ผู้อื่นที่มิได้รับมอบหมายให้ปฏิบัติงานแทน

ข้อ 6 การใช้งานอินเทอร์เน็ต ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

6.1 ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

(1) การพนัน

(2) การประมูล

(3) วิพากษ์วิจารณ์ที่เกี่ยวข้องกับชาติ ศาสนา และพระมหากษัตริย์

(4) ลามก อนาจาร

(5) อื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

6.2 ห้ามเล่นเกมส์ หรือดาวน์โหลดเกมส์ ภาพยนตร์ เพลง หรือสื่อลามกอนาจารผ่านทางอินเทอร์เน็ต

6.3 ห้ามใช้อินเทอร์เน็ตเพื่อเผยแพร่หรือแจกจ่าย ดังต่อไปนี้

(1) สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของ

(2) ข้อมูลประเภทสื่อลามกอนาจาร

(3) ข้อมูลที่เป็นความลับของ สบน. ไปยังบุคคลที่ไม่ได้รับอนุญาต

(4) ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

6.4 ห้ามใช้งานข้อมูลที่ได้รับโดยผ่านทางอินเทอร์เน็ตที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของข้อมูลนั้น

6.5 ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ หรือชื่อเสียงของ สบน.

ข้อ 7 การใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ผู้ใช้งานต้องปฏิบัติตามข้อกำหนด ดังต่อไปนี้

7.1 ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ตามที่ สบน. กำหนดเท่านั้น

7.2 ห้ามใช้ E-Mail Address ที่ สบน. กำหนดให้ ลงทะเบียนตามเว็บไซต์ที่ไม่เกี่ยวข้องกับงานของ สบน.

7.3 ห้ามเข้าถึง E-Mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต

7.4 ห้ามปลอมแปลง รับหรือส่ง E-Mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต

7.5 ห้ามส่ง E-Mail ที่มีลักษณะดังต่อไปนี้

(1) จดหมายขยะ (Spam Mail)

(2) จดหมายลูกโซ่ (Chain Letter)

(3) จดหมายที่ละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

(4) จดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

(5) จดหมายที่มีขนาดใหญ่เกินกว่าที่กำหนด

7.6 ต้องระบุชื่อเรื่อง (Subject) และชื่อผู้ส่งใน E-Mail ทุกฉบับที่ส่งไป

7.7 ต้องใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับ E-Mail เท่าที่มีความจำเป็นต้องรับรู้เท่านั้น

7.8 ต้องใช้คำที่สุภาพในการส่ง E-Mail

7.9 ต้องสำรองข้อมูล E-Mail Address ตามความจำเป็น เป็นประจำทุก 30 วัน

ข้อ 8 ห้ามมิให้เจ้าหน้าที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของ สบน. กระทำการในลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้

8.1 กระทำผิดกฎหมายหรือก่อให้เกิดความเสียหายแก่บุคคลอื่นหรือขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือละเมิดทรัพย์สินทางปัญญาของ สบน. และของบุคคลอื่น

8.2 เปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน ทั้งที่เป็นข้อมูลของ สบน. หรือบุคคลภายนอก

8.3 การเข้าถึงข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาต

8.4 ขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของ สบน. หรือเจ้าหน้าที่คนอื่นของ สบน.

8.5 แสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับ สบน. ไปยังที่อยู่เว็บไซต์ใด ๆ ในลักษณะที่ก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง และก่อให้เกิดความเสียหายแก่ สบน.

8.6 กระทำการอื่นใดที่อาจขัดต่อการดำเนินงานตามอำนาจหน้าที่ของ สบน. หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่ สบน.

8.7 จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

8.8 กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์

ข้อ 9 เอกสารที่เป็นความลับหรือมีระดับความสำคัญซึ่งพิมพ์ออกมาจากเครื่องพิมพ์ (Printer) เจ้าหน้าที่ต้องปฏิบัติให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการ ดังต่อไปนี้

9.1 จัดหมวดหมู่เอกสารที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก

9.2 จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ

9.3 การสำเนาเอกสารที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูง ต้องได้รับอนุญาตจากผู้เป็นเจ้าของ

9.4 ระมัดระวังการเผยแพร่ หรือแจกจ่ายเอกสารที่เป็นความลับของ สบน. 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

(1) ชื่อผู้ส่งจะไม่สามารถค้นหาที่มาได้ และ/หรือเป็นชื่อที่ผู้ใช้งานไม่รู้จัก/ไม่คุ้นเคย

(2) ชื่อเรื่องของ E-Mail จะเป็นข้อความที่โน้มน้าวให้น่าสนใจ เพื่อต้องการให้ผู้ใช้งานเปิดอ่าน ตัวอย่างได้แก่ “นี่คือคำตอบที่คุณได้ร้องขอจากเราไป” หรือ “ผมได้ส่งไฟล์มาแล้วตามที่ร้องขอ” หรือ“คุณได้รับอนุมัติบัตรเครดิตแล้ว” เป็นต้น

11.2 ตรวจสอบเนื้อหาของ E-Mail โดยมีจุดสังเกต ดังนี้

(1) E-Mail ที่ไม่มีเนื้อหา

(2) E-Mail ที่มีเนื้อหาเกี่ยวกับการโฆษณาสินค้า ผลิตภัณฑ์ หรือบริการ

(3) E-Mail ที่มีลักษณะหลอกลวงโดยสอบถามข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ควรเปิดเผยสู่สาธารณะ

(4) E-Mail ที่ใช้เนื้อหาในลักษณะของรูปภาพแทนตัวอักษร

(5) E-Mail ที่แนบไฟล์ที่อาจเป็น Virus หรือ Trojan และมีเนื้อหาเชิญชวนให้ผู้ใช้งานดาวน์โหลดหรือติดตั้งไฟล์ดังกล่าว

ข้อ 12 ในกรณีที่ผู้ใช้งานได้รับจดหมายขยะ (Spam Mail) ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดดังนี้

12.1 ห้ามเปิดอ่าน E-Mail ฉบับนั้นโดยเด็ดขาด และให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีและสารสนเทศทราบทันที

12.2 ในกรณีที่เปิดอ่านแล้ว ห้ามคลิกที่ Link ข้อมูล หรือดาวน์โหลดไฟล์ที่แนบมากับ E-Mail ฉบับนั้น และให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีและสารสนเทศทราบทันที

ข้อ 13 หากผู้ใช้งานละเมิดหรือฝ่าฝืนแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางสารสนเทศใด ๆ ในหมวดนี้ ที่มีเนื้อหาเกี่ยวข้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ซึ่งเกิดจากความจงใจหรือประมาทเลินเล่อก็ตาม ให้ถือว่าผู้นั้นต้องเป็นผู้รับโทษตามกฎหมาย เว้นแต่การกระทำดังกล่าวก่อให้เกิดผลกระทบตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ข้อ 8

ข้อ 14 จัดกิจกรรมการสร้างความตระหนักในการใช้งาน ระบบสารสนเทศอย่างปลอดภัย (Information Security Awareness)

14.1 จัดอบรมเพื่อเพิ่มความรู้ให้แก่บุคลากรในเรื่อง การสร้างความตระหนักและกำกับการใช้งานระบบสารสนเทศอย่างปลอดภัย โดยให้วิทยากรที่มีความรู้ความชำนาญ มีประสบการณ์ทางด้านความปลอดภัยทางเทคโนโลยีสารสนเทศมาเป็นผู้บรรยาย พร้อมจัดทำเอกสารประกอบการบรรยายให้กับผู้รับฟังบรรยาย ณ สบน. ระยะเวลาอย่างน้อยปีละ 2 ครั้ง ครั้งละไม่น้อยกว่า 30 นาที

14.2 จัดอบรมเพื่อเพิ่มความรู้ให้แก่ผู้ดูแลระบบ ในเรื่อง การสร้างความตระหนักและกำกับการใช้งานระบบสารสนเทศอย่างปลอดภัย โดยให้วิทยากรที่มีความรู้ความชำนาญ มีประสบการณ์ทางด้านความปลอดภัยทางเทคโนโลยีสารสนเทศมาเป็นผู้บรรยาย พร้อมจัดทำเอกสารประกอบการบรรยายให้กับผู้รับฟังบรรยาย ณ สบน. ระยะเวลาอย่างน้อยปีละ 2 ครั้ง ครั้งละไม่น้อยกว่า 1 ชั่วโมง

หมวด 5
แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบสารสนเทศ/ผู้ดูแลระบบเครือข่าย

ข้อ 1 ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศ ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) และระบบเครือข่ายของ สบน. ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์ ระบบงานสารสนเทศ และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้นในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นกับ สบน. ให้ผู้ดูแลระบบ (System Administrator) พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าวได้ทันที

ข้อ 2 ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่ายให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

ข้อ 3 ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) ระบบงานสารสนเทศ และระบบเครือข่าย

ข้อ 4 ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

ข้อ 5 บริหารจัดการบัญชีผู้ใช้งานและควบคุมการเข้าถึงตามอำนาจหน้าที่เท่านั้น

ข้อ 6 บริหารจัดการระบบงานสารสนเทศ และระบบเครือข่ายตามอำนาจหน้าที่รับผิดชอบเท่านั้น

ข้อ 7 บริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามอำนาจหน้าที่รับผิดชอบเท่านั้น

ข้อ 8 ไม่ใช้อำนาจหน้าที่ของตนเองในการเข้าถึงข้อมูลของผู้ใช้งาน บนระบบคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่าย โดยไม่มีเหตุผลอันสมควร

ข้อ 9 ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานเครื่องคอมพิวเตอร์ 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 (Server Room) ได้แก่ สายไฟฟ้า และสายสัญญาณ เป็นต้น ทุก 30 วัน หากพบความชำรุดให้ติดต่อหน่วยงานที่รับผิดชอบเพื่อให้แก้ไขอย่างทันการณ์

ข้อ 14 จัดทำมาตรฐานการพัฒนาซอฟต์แวร์ (ในภาคผนวก ง)

หมวด 6
แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

ข้อ 1 กำหนดมาตรการทางเครือข่ายและการสื่อสารข้อมูลเพื่อป้องกันข้อมูลในเครือข่ายคอมพิวเตอร์ ระบบงานสารสนเทศ หรือบริการต่างๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

1.1 กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกลแบบเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN)

1.2 การปฏิบัติงานขององค์กรจากภายนอก สบน. ในการเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกลจะต้องปฏิบัติ ดังนี้

(1) ติดต่อ ศทส. เพื่ออธิบายเหตุผลความจำและกำหนดช่วงเวลาที่สิ้นสุดในการใช้งานและลงทะเบียนเป็นลายลักษณ์อักษร

(2) ศทส. จะกำหนดสิทธิให้เข้าใช้งานเฉพาะระบบที่จำเป็นต้องใช้เท่านั้น

1.3 กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ ได้แก่ เครือข่ายอินเทอร์เน็ต เครือข่ายไร้สาย เป็นต้น

1.4 การเข้าสู่ระบบงานสารสนเทศภายในองค์กร สำหรับผู้ใช้นอกองค์กร (Guest) ต้องมีการ Login และต้องมีการยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง ด้วยการใช้รหัสผ่านโดยจะต้องลงทะเบียนและขอรับได้ที่ ศทส.

1.5 กำหนดข้อปฏิบัติในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์พกพาและโทรศัพท์มือถือต้องมีการยืนยันตัวตนในการเข้าใช้งานทุกครั้งด้วยการใช้รหัสผ่านที่ออกให้โดย ศทส. ซึ่งสิทธิที่ได้จะแตกต่างและมีข้อกำหนดการใช้งานที่จำกัด

1.6 มีการบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์เครือข่าย เพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

ข้อ 2 ผู้รับผิดชอบหรือผู้ดูแลระบบสารสนเทศภายใน สบน. จะต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

2.1 ผู้ดูแลระบบต้องออกแบบการแบ่งระบบเครือข่าย (Segregation in Networks) ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน ดังนี้ (1) เขตภายใน (Internal Zone) (2) เขตภายนอก (External Zone) เพื่อเป็นการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

2.2 การเข้าสู่ระบบเครือข่ายภายใน สบน. โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาก่อนที่จะสามารถใช้งานได้ในทุกกรณี

2.3 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายและระบบสารสนเทศที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

2.4 ผู้ดูแลระบบจะต้องตรวจสอบและจำกัดเส้นทางการเข้าถึงเครือข่าย โดยการปิดเส้นทางของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นออกจากระบบ

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

2.6 กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต่าง ๆ ของระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์อย่างชัดเจนและมีการทบทวนการกำหนดค่าตัวแปร (Parameter) ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

2.7 ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก สบน. จะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมป้องกันการบุกรุกในการทำ Packet Filtering เป็นต้น

2.8 มีการติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายภายใน สบน. ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

2.9 การเข้าสู่ระบบงานเครือข่ายภายใน สบน. ผ่านทางอินเทอร์เน็ตจะต้องมีการยืนยันตัวตน (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 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2.13 ผู้ดูแลระบบกำหนดอุปกรณ์บนเครือข่ายเป็น IP Address แยกตาม สำนัก/ศูนย์/กลุ่ม แต่ละสิทธิของผู้ใช้งาน โดยให้ควบคุมการใช้งานอย่างเหมาะสมและมีการยืนยันตัวตนทุกครั้งที่ใช้อุปกรณ์

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

2.15 มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานทุก 90 วัน

ข้อ 3 ผู้รับผิดชอบระบบสารสนเทศของ สบน. จะต้องควบคุมการเข้าใช้งานจากภายนอก สบน. เพื่อดูแลรักษาความปลอดภัยโดยมีแนวทางการปฏิบัติ ดังนี้

3.1 การเข้าถึงระบบจากระยะไกลแบบเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) เพื่อเข้าถึงระบบเครือข่ายคอมพิวเตอร์ของ สบน. ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรจะต้องขออนุญาตก่อนการใช้งานทุกครั้ง

3.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบและข้อมูลอย่างเคร่งครัด

3.3 ก่อนการขอเข้าใช้งานระบบสื่อสารจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับ สบน. และต้องได้รับอนุมัติจากผู้บังคับบัญชาทุกครั้ง

3.4 มีการควบคุมช่องทางติดต่อ (Port) ที่ใช้ในการเข้าถึงระบบอย่างรัดกุม การเข้าถึงระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

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

ข้อ 4 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless) ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดแนวปฏิบัติตามข้อกำหนด ดังต่อไปนี้

4.1 ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายใน สบน. จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน

4.2 ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

4.3 ผู้ดูแลระบบควรใช้ Software หรือ Hardware ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

หมวด 7
แนวปฏิบัติในการใช้งาน Token Key และ GFMIS Smart Card

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

(1) ระบบ GFMIS-SOE

(2) 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) และใส่รหัสผ่าน (Password) ก่อนเข้าใช้งาน

1.6 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ทุก ๆ 3 เดือน เพื่อความปลอดภัยในการเข้าใช้งานระบบ

1.7 ผู้ใช้งานต้องรับผิดชอบต่อการปฏิบัติงานที่เกิดจากการใช้งานตามสิทธิที่ได้รับในการปฏิบัติงานเข้าใช้งานระบบทุกรายการ

ข้อ 2 การดูแลและการเก็บรักษา Token Key ให้ปลอดภัย

2.1 ผู้ใช้งานต้องมีหน้าที่ในการจัดเก็บรักษา Token Key ให้มีความปลอดภัย ดังนี้

(1) ควรระมัดระวังไม่ให้ Token Key ตกน้ำ หรือแช่น้ำเป็นเวลานาน อาจทำให้ Token Key ไม่สามารถใช้งานได้

(2) ห้ามงัดแงะ ทุบหรือกระแทกอย่างรุนแรง จะทำให้ Token Key เสียรูปทรงจนไม่สามารถใช้งานได้

(3) ต้องไม่อนุญาตให้บุคคลอื่นนำ Token Key ไปใช้งานนอกจากจะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 3 ข้อปฏิบัติในกรณีที่ Token Key สูญหาย หรือชำรุด ต้องดำเนินงานตามขั้นตอน ดังนี้

3.1 ผู้ใช้งานต้องโทรศัพท์แจ้งผู้ดูแลระบบเพื่อระงับการใช้งาน Token Key กรณีที่ผู้ใช้งานไม่แจ้งการสูญหายและมีผู้อื่นนำ Token Key ไปใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นตามแต่กรณี

3.2 ทำหนังสือแจ้งผู้ดูแลระบบภายใน 3 วัน นับจากที่ผู้ใช้งานโทรแจ้งระงับการใช้งาน Token Key เพื่อรับ Token Key อันใหม่สำหรับการใช้งาน

3.3 กรณีที่เป็นผู้ใช้งานคนเดิมไม่ต้องส่งเอกสารข้อมูลส่วนบุคคลอีก

ข้อ 4 ข้อปฏิบัติในกรณีที่มีการย้ายหรือเปลี่ยนแปลงผู้ใช้งาน Token Key ต้องดำเนินงานตามขั้นตอน ดังนี้

4.1 ทำหนังสือแจ้งพร้อมแบบฟอร์มลงทะเบียนผู้ใช้งาน (แบบลงทะเบียน GFMIS-SOE)

4.2 ทำหนังสือคำสั่งแต่งตั้งให้ดำรงตำแหน่งผู้ใช้งาน ภายใน 15 วัน นับจากมีคำสั่งย้ายหรือเปลี่ยนแปลงผู้ใช้งาน

4.3 ต้องแนบรายละเอียดข้อมูลส่วนบุคคล ได้แก่ บัตรประจำตัวประชาชนหรือบัตรข้าราชการ เพื่อให้สามารถระบุตัวตนผู้ใช้งานได้

ข้อ 5 กรณีที่ต้องเพิกถอนการใช้งาน Token Key

5.1 การเพิกถอนการใช้งาน คือ การทำให้ใบรับรองอิเล็กทรอนิกส์หรือ Token Key ไม่สามารถนำมาใช้ได้อีกต่อไป โดยผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ หรือผู้ใช้งานสามารถเพิกถอนการใช้งานได้ในกรณีดังต่อไปนี้

(1) มีผู้อื่นสามารถเข้าถึง หรือนำ Token Key ไปใช้งานโดยไม่ได้รับอนุญาต

(2) 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

ข้อ 7 ข้อกำหนดในการใช้งาน GFMIS Smart Card

7.1 ผู้ใช้งานต้องรับผิดชอบต่อการปฏิบัติงานที่เกิดจากการใช้สิทธิในการปฏิบัติงานทั้งหมด

7.2 ผู้ใช้งานต้องถือว่าบัตร GFMIS Smart Card ภายใต้รหัสของผู้ใช้งาน (User Login) และรหัสผ่านนั้นเป็นสิ่งใช้แทนเครื่องหมายเฉพาะประจำตัวหรือเสมือนลายมือชื่อของผู้ใช้งาน

7.3 กรณีที่บัตร GFMIS Smart Card สูญหาย ถูกขโมย หรือชำรุดเสียหาย ผู้ใช้งานต้องขอระงับใช้งานบัตร GFMIS Smart Card ชั่วคราว โดยผู้ใช้งานต้องปฏิบัติ ดังนี้

(1) แจ้งกรมบัญชีกลางทราบด้วยวาจาหรือลายลักษณ์อักษรทันทีที่ทราบเหตุ เพื่อระงับการใช้งานบัตร GFMIS Smart Card หากผู้ใช้งานมิได้ดำเนินการดังกล่าวข้างต้นและมีผู้อื่นนำสิทธิการใช้งานไปใช้เข้าสู่ระบบ ให้ถือว่าผู้ใช้งานเจ้าของบัตร GFMIS Smart Card นั้นเป็นผู้รับผิดชอบต่อความเสียหายทั้งหมด

(2) แจ้งความที่สถานีตำรวจท้องที่เกิดเหตุ และส่งสำเนาใบแจ้งความแก่กรมบัญชีกลางเพื่อออกบัตร GFMIS Smart Card รหัสผู้ใช้งาน (User Login) และรหัสผ่านชุดใหม่

7.4 ให้เก็บรักษาบัตร GFMIS Smart Card เสมือนเอกสารแทนตัวเงิน โดยนำหลักเกณฑ์การเก็บรักษาเงินตามระเบียบการเบิกจ่ายจากเงินคลัง การเก็บรักษาเงินและการนำเงินส่งคลัง พ.ศ. 2551 มาบังคับใช้โดยอนุโลม และถือปฏิบัติ ดังนี้

(1) เปลี่ยนรหัสผ่านบัตร GFMIS Smart Card เมื่อได้รับบัตรมาครั้งแรก และควรเปลี่ยนรหัสผ่านทุก 90 วัน

(2) ห้ามเขียนรหัสผ่านบนบัตร GFMIS Smart Card

(3) เก็บรักษาบัตร GFMIS Smart Card ไว้ในสภาพที่เหมาะสมคือไม่เก็บไว้ในที่อุณหภูมิสูงเกินหรือเก็บไว้ในสภาพที่บิดงอเพื่อป้องกันบัตร GFMIS Smart Card ชำรุด

หมวด 8
แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

ข้อ 1 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล เมื่อมีระบบงานใหม่ เกิดข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่ ควรกำหนดให้ใช้แนวทางการสำรองและกู้คืนข้อมูล ดังนี้

1.1 กำหนดระบบงานที่มีความจำเป็นต้องสำรองข้อมูลไว้

1.2 กำหนดผู้รับผิดชอบในการสำรองข้อมูลและกรณีเกิดเหตุฉุกเฉิน (ในภาคผนวก จ)

1.3 กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อยต้องประกอบด้วย ข้อมูลในฐานข้อมูลของระบบ ข้อมูลสำหรับตัวระบบ ได้แก่ โปรแกรมระบบปฏิบัติการ (Operation Software) และโปรแกรมอื่น ๆ ที่เกี่ยวข้อง

1.4 กำหนดความถี่ในการสำรองข้อมูลของระบบงาน ได้แก่ ระบบงานที่มีการเปลี่ยนแปลงบ่อย ควรมีความถี่ในการสำรองข้อมูลมากขึ้น เป็นต้น

1.5 กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งโปรแกรมที่ใช้ในการสำรองข้อมูล

1.6 ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย 1 ชุด

1.7 ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วนหรือไม่

1.8 ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ 1 ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่

1.9 จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด โดยแผนฯ ควรมีรายละเอียดอย่างน้อยดังต่อไปนี้

(1) การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

(2) การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(3) การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน

(4) การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

(5) การกำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอกได้แก่ ผู้ให้บริการเครื่องคอมพิวเตอร์ โปรแกรมและระบบเครือข่าย เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่าง ๆ ได้แก่ เกิดอัคคีภัย การก่อวินาศกรรม เป็นต้น

1.10 ให้ทำการปรับปรุงแผนฯ ดังกล่าวอย่างน้อยปีละ 1 ครั้ง

1.11 ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนฯ รวมทั้งเมื่อมีการปรับปรุงแผนใหม่จะต้องจัดประชุมใหม่และแจ้งให้ผู้ที่เกี่ยวข้องทราบได้แก่เดียวกัน

หมวด 9
แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ 1 การแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย (เพิ่มเติมจากประกาศของ ICT)

1.1 ให้เจ้าหน้าที่หรือผู้ปฏิบัติงานแจ้ง ศทส. ทันทีที่พบเห็นเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของ สบน. ได้แก่

(1) มีโปรแกรมสำนักงานไม่ประสงค์ดีเข้ามาในระบบคอมพิวเตอร์

(2) มีการบุกรุกเข้ามาในระบบเครือข่าย

(3) ข้อมูลสำคัญเปลี่ยนแปลง หรือสูญหาย

(4) มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(5) มีการนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์

(6) มีการใช้ระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์

(7) พบจุดอ่อนในเครื่องคอมพิวเตอร์ โปรแกรมและระบบเครือข่ายที่ใช้งาน

(8) มีการโจมตีเข้ามาในระบบจนไม่สามารถให้บริการได้

(9) ระบบเทคโนโลยีสารสนเทศชำรุดหรือสูญหาย

(10) บุคคลภายนอกเข้าใช้ระบบงานของ สบน. โดยไม่ได้รับอนุญาต

(11) มีการติดตั้งโปรแกรมเพื่อขโมยข้อมูลหรือเข้าถึงข้อมูลในระบบเครือข่าย

(12) เหตุการณ์อื่น ๆ ที่เป็นการละเมิดความมั่นคงปลอดภัยของ สบน.

1.2 ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชาหรือ ศทส. ในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้น รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชาหรือ ศทส. ด้วย

ข้อ 2 ผู้รับผิดชอบระบบสารสนเทศของ สบน. เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่พบ ให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

2.1 ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบในระดับใด (สูง กลาง หรือต่ำ)

2.2 แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบตามระดับของผลกระทบ กล่าวคือ รายงานไปสู่ระดับชั้นของผู้บังคับบัญชาที่สูงขึ้นตามลำดับสำหรับเหตุการณ์ที่มีผลกระทบสูงกว่า

2.3 วิเคราะห์และแก้ไขสถานการณ์ตามความจำเป็นกรณีการบุกรุก การโจมตีระบบหรือระบบได้รับความเสียหาย ประสานงานขอความช่วยเหลือจากผู้รู้ ได้แก่ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT)

2.4 กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ ให้ผู้ที่ผ่านการอบรมหรือฝึกฝนเป็นผู้ดำเนินการเพื่อป้องกันไม่ให้หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัย และจำกัดการเข้าถึงหลักฐานนั้น

2.5 จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลาง ขึ้นไปและแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีข้อมูลอย่างน้อยในรายงาน ดังนี้

(1) รายละเอียดเหตุการณ์

(2) วันเวลาที่เกิดขึ้น

(3) ชื่อผู้แจ้ง/หน่วยงานผู้แจ้ง

(4) สถานะของเหตุการณ์ในแต่ละช่วงเวลา

(5) ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา

(6) สาเหตุและวิธีการแก้ไข

(7) ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

ข้อ 3 ความรับผิดชอบของผู้บังคับบัญชากรณีที่มีการละเมิดการปฏิบัตินี้

3.1 ให้แจ้งรายงานตามสายการบังคับบัญชาให้หน่วยที่เกี่ยวข้องทราบ

3.2 สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

3.3 พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์นี้ได้อุบัติซ้ำอีก

3.4 ให้พิจารณาการลงโทษทางวินัยตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิดและผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้โดยเจตนาหรือไม่เจตนา และการละเมิดนั้นก่อให้เกิดความเสียหายหรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

ข้อ 4 ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบงานสารสนเทศ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของระบบสารสนเทศดำเนินการ ดังนี้

4.1 พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่าง ๆ ประมวลลับ หรือรหัสผ่านที่จำเป็นในการใช้เครือข่ายสื่อสารข้อมูลสารสนเทศมีผลกระทบกระเทือนเสียหายอย่างใดหรือไม่

4.2 ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันที ในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นสมควร

ข้อ 5 ความรับผิดชอบของผู้ใช้งานต่อประกาศฉบับนี้มี 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 10
แนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์

ข้อ 1 การปฏิบัติเมื่อเกิดฟิชชิ่ง (Phishing) ที่เว็บเซิร์ฟเวอร์ของ สบน.

1.1 เมื่อผู้ดูแลระบบเครือข่ายได้รับแจ้งหรือตรวจพบว่าเว็บเซิร์ฟเวอร์ ของ สบน. ถูกผู้ไม่หวังดีทำ Phishing ผู้ดูแลระบบจะดำเนินการ ดังนี้

(1) บล็อก IP Address ของเว็บเซิร์ฟเวอร์ที่ถูก Phishing หรือแจ้งผู้ให้บริการเส้นทางเครือข่ายของหน่วยงานดำเนินการโดยเร่งด่วน

(2) แจ้งผู้ดูแลเว็บเซิร์ฟเวอร์ที่ถูก Phishing ทาง E-Mail หรือ โทรศัพท์ เพื่อให้ดำเนินการแก้ไขปัญหา

1.2 เมื่อดำเนินการแก้ไขปัญหาเรียบร้อยแล้ว ให้ประสานผู้ดูแลระบบเครือข่าย หรือผู้ให้บริการเส้นทางเครือข่ายของหน่วยงานเพื่อปลดบล็อก IP Address

1.3 ผู้ดูแลระบบต้องตรวจสอบเว็บเซิร์ฟเวอร์, เว็บไซต์ของ สบน. และเว็บไซต์ภายในของ สบน. รวมทั้งติดตั้งโปรแกรมปรับปรุงช่องโหว่ (Patch) อย่างสม่ำเสมอ เพื่อป้องกันผู้ที่ไม่หวังดีในการเข้ามาทำ Phishing

ข้อ 2 การปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์เกี่ยวกับมัลแวร์เรียกค่าไถ่ (Ransomware)

2.1 ระบุเครื่องคอมพิวเตอร์ทุกเครื่อง โดยแยกเป็นกลุ่มตามระดับผลกระทบหากถูกโจมตีจาก Ransomware ระบุผู้รับผิดชอบเครื่องแต่ละเครื่อง เช่น สำนัก/ศูนย์/กลุ่ม ข้อมูลติดต่อเจ้าหน้าที่ ศทส. และเจ้าหน้าที่ Outsource

2.2 วางแผนการจัดการ การตรวจสอบเครื่องแต่ละกลุ่ม และดำเนินการป้องกัน

2.3 สำรองข้อมูลที่สำคัญออกจากเครื่องไว้ในอุปกรณ์สำรองภายนอก (External Hard Disk) อย่างน้อย 3 แหล่ง (ที่ไม่ต่อเชื่อมกับระบบเครือข่าย เพื่อป้องกันการถูกเข้ารหัสไฟล์ข้อมูล)

2.4 สื่อสารให้ความรู้เกี่ยวกับการป้องกัน/ลดความเสี่ยงแก่ผู้ใช้งาน มิให้เป็นพาหะนำมัลแวร์เข้าสู่เครือข่าย เช่น ไม่เปิดอีเมลที่ไม่รู้จัก ไม่คลิกเปิดหรือ Download ไฟล์แนบที่ไม่ระบุแหล่งที่มาที่รู้จัก รวมถึงไฟล์น่าสงสัยอื่น ๆ

2.5 ดำเนินการป้องกัน (ติดตั้ง/Update Patch OS) และสื่อสารให้ความแก่ผู้ใช้ และให้ผู้ดูแลระบบติดตามสถานะอย่างใกล้ชิด

2.6 ผู้ดูแลระบบ

(1) ระบบเครือข่ายของ สบน. ต้องมีการติดตั้งระบบป้องกันเครือข่าย (Firewall)

(2) ต้องมีการพิสูจน์ตัวตน (Authentication) ในการใช้งานระบบสารสนเทศหรือระบบเครือข่ายของ สบน. และมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อย่างเหมาะสม

(3) จัดตารางการสำรองข้อมูล เช่น ฐานข้อมูล โปรแกรมที่มีความจำเป็นเพื่อเป็นการป้องกันข้อมูลสูญหาย และสามารถนำกลับมาใช้ได้โดยไม่เกิดผลกระทบต่อระบบที่ต้องการใช้งาน

(4) จัดทำแผนการทดสอบและการกู้คืนข้อมูลที่สำคัญหลังจากสำรองข้อมูลแล้ว

(5) จัดให้มีเครื่องคอมพิวเตอร์แม่ข่ายสำรองสำหรับระบบที่จำเป็นใช้งาน หลังจากระบบหลักมีปัญหาสามารถใช้งานได้โดยไม่เกิดผลกระทบต่อการบริการหรือมีผลกระทบน้อยที่สุด

(6) หลังจากสำรองข้อมูลแล้วให้ตัดการเชื่อมต่อกับระบบเครือข่ายเพื่อป้องกันการถูกโจมตี

2.7 ผู้ใช้งานระบบ

(1) ผู้ใช้งานระบบสารสนเทศต้องไม่ติดตั้งโปรแกรมที่ไม่ได้รับอนุญาตจากผู้ดูแลระบบ

(2) ไม่เปิดไฟล์ที่ไม่ทราบแหล่งที่มาที่ชัดเจน

(3) ไม่ใช้งานเว็บไซต์ที่มีความเสี่ยง

หมวด 11
แนวปฏิบัติในการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศ

ข้อ 1 ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องควบคุมการพัฒนาหรือจัดหาระบบงานเพื่อให้ระบบงานที่ได้รับมีความมั่นคงปลอดภัยเพียงพอ ดังนี้

1.1 ให้ประเมินความเสี่ยงและระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษร ข้อกำหนดดังกล่าวอย่างน้อยควรมีคุณสมบัติของการเข้าสู่ระบบงาน (Login) ที่มีความมั่นคงปลอดภัย ดังนี้

(1) ไม่มีหรือไม่แสดงรูปแบบการใช้งาน (Function) ให้การช่วยเหลือในระหว่างที่ Login

(2) บันทึกความพยายามในการ Login ทั้งที่สำเร็จและไม่สำเร็จ และแสดงประวัติการ Login 3 ครั้งล่าสุด

(3) ตัดการเชื่อมต่อหลังจากที่ทำการ Login ไม่สำเร็จเกินกว่า 3 ครั้ง

(4) เมื่อใส่ข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้อง ให้แสดงข้อความปรากฏ ได้แก่ “ข้อมูลการ Login ไม่ถูกต้อง”

(5) ให้แสดงข้อความเตือนที่หน้าจอภายหลังจากการ Login เสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ “ระบบนี้เป็นระบบที่เป็นทรัพย์สินของ สบน. การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้น จึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงานหากมีการตรวจพบและเป็นความผิด จะดำเนินการลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม สิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้งานใช้ระบบงานนี้โดยไม่ถือว่าเป็นการละเมิดความเป็นส่วนตัว”

(6) ไม่แสดงรายละเอียดของระบบใด ๆ จนกว่าจะ Login สำเร็จ

(7) การกำหนดหรือตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับเข้าถึงระบบงาน

(8) การเข้ารหัสลับข้อมูลสำคัญที่มีการรับส่งระหว่างเครื่องคอมพิวเตอร์ลูกข่ายกับเครื่องคอมพิวเตอร์ที่ให้บริการ

(9) การเข้ารหัสข้อมูลสำคัญ ได้แก่ ข้อมูลลับ ที่จัดเก็บไว้ในฐานข้อมูล

(10) การตัดและหมดเวลาการใช้งานหลังจากที่ไม่ได้ใช้ระบบงานเกินกว่าระยะเวลาตามที่กำหนดไว้ ได้แก่ 15 - 30 นาที

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

1.2 พัฒนาหรือจัดหาระบบงานให้ได้ตามข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ระบุไว้

1.3 พัฒนาหรือจัดหาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลระบบเพื่อทำการบันทึกและปรับปรุงสิทธิของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

1.4 กำหนดให้มีการจัดทำแผนการทดสอบโดยผู้พัฒนาระบบ นำเสนอแผนฯ ดังกล่าวเพื่อพิจารณาอนุมัติโดยผู้มีอำนาจ ดำเนินการทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการทดสอบให้ผู้มีอำนาจได้รับทราบเพื่อให้คำแนะนำในการปรับปรุงต่าง ๆ ที่จำเป็นแผนการทดสอบที่จัดทำอย่างน้อยประกอบด้วย

(1) แผนการทดสอบความยอมรับของผู้ใช้ (User Acceptance Test : UAT)

(2) แผนการทดสอบความสอดคล้องของระบบ (System Integration Test)

(3) แผนการทดสอบข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Test)

1.5 ไม่อนุญาตให้นำข้อมูลสำคัญของ สบน. ไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นแต่ได้รับการอนุมัติจากผู้บังคับบัญชาระดับสูงก่อน และหากเป็นไปได้ให้ตัดข้อมูลส่วนที่สำคัญทิ้งไป ให้เหลือเฉพาะส่วนที่เพียงพอต่อการนำไปใช้ในการทดสอบ

1.6 การส่งข้อมูลผ่านระบบสารสนเทศต้องไม่สามารถถูกเปลี่ยนแปลงพร้อมทั้งยังคงความถูกต้องครบถ้วน (Integrity) และความถูกต้องแท้จริง (Authenticity)

1.7 หากระบบงานที่พัฒนาต้องจัดเก็บข้อมูลส่วนบุคคล ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยระบบงานนั้น ๆ ต้องมีคุณลักษณะอย่างน้อยดังต่อไปนี้

(1) ต้องมีหน้าจอแสดงข้อความขอความยินยอมและจุดประสงค์ในการเก็บใช้หรือเปิดเผยข้อมูลส่วนบุคคลและข้อมูลการใช้งานในการเยี่ยมชมเว็บไซต์ (Cookies)

(2) การเก็บ ใช้ เปิดเผย หรือถ่ายโอนข้อมูลข้อมูลส่วนบุคคลต้องอยู่ในขอบเขตของการอนุญาตของเจ้าของข้อมูลนั้น

(3) มีช่องทางให้เจ้าของข้อมูลเข้าถึง ปรับปรุง รวมถึงลบข้อมูลส่วนบุคคลและการยินยอมในการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตนเองได้

ข้อ 2 ภายหลังจากที่ได้มีการตรวจรับระบบที่พัฒนาขึ้นใหม่แล้ว ผู้รับผิดชอบระบบสารสนเทศของ สบน. ต้องกำหนดการควบคุมการติดตั้งโปรแกรมลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการ ดังนี้

2.1 ให้มีการควบคุมการเปลี่ยนแปลงระบบงานภายใน สบน. เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

2.2 ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงระบบงานภายใน สบน.

2.3 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

2.4 กำหนดให้มีการจัดเก็บรหัสโปรแกรม (Source Code) และบรรณานุกรมคำศัพท์ (Library) สำหรับโปรแกรมของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

2.5 กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน ได้แก่ โปรแกรมระบบปฏิบัติการ โปรแกรมระบบงาน เป็นต้น

2.6 ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

2.7 ทำการปรับปรุงคลังโปรแกรมหรือที่รวบรวมชุดคำสั่ง (Library) สำหรับโปรแกรมระบบงานให้มีความทันสมัยและสอดคล้องกับระบบทั้งหมดที่ทำการติดตั้ง

2.8 ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิมให้ทำการสำรองข้อมูลที่จำเป็น ได้แก่ ฐานข้อมูล โปรแกรม ค่าปรับแต่งและติดตั้งระบบ หรืออื่น ๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จจะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้ (Rollback)

2.9 ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่ทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ให้ถ่ายโอนข้อมูลตามแผน และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

2.10 ให้กำหนดแผนการติดตั้งสำหรับระบบงานซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า ได้แก่ แผนการติดตั้งเครื่องคอมพิวเตอร์ โปรแกรมระบบเครือข่าย และอื่น ๆ

2.11 สำหรับโปรแกรมที่จะทำการติดตั้ง ให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตโปรแกรมนั้น

2.12 ให้อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานโปรแกรมที่จะทำการติดตั้งอย่างเคร่งครัด

2.13 สำหรับการติดตั้งโปรแกรมอเนกประสงค์ (Utility Software) ต้องตรวจสอบก่อนว่าเป็นโปรแกรมที่มีการทำงานที่ถูกต้องและเชื่อถือได้

2.14 ติดตั้งโปรแกรมสำนักงานแก้ไขช่องโหว่ (Patch) ที่เกี่ยวข้องกับระบบงานตามความจำเป็น ได้แก่ 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 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

3.2 พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่ สบน. ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

ข้อ 4 การดำเนินงานโครงการ/แผนงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ หรือวัสดุอุปกรณ์อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ต้องผ่านการพิจารณากลั่นกรองความเหมาะสมเบื้องต้นจาก ศทส. และนำเสนอคณะกรรมการพัฒนาระบบเทคโนโลยีของสำนักงานบริหารหนี้สาธารณะ หรือ คกก. DCIO เพื่อพิจารณาเห็นชอบโครงการ/แผนงาน และบรรจุในแผนปฏิบัติการดิจิทัลก่อนเสนอให้ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะเห็นชอบหรือผู้ซึ่งผู้อำนวยการสำนักงานบริหารหนี้สาธารณะมอบหมายเพื่อดำเนินการหรือเพื่อส่งให้คณะกรรมการคอมพิวเตอร์ของกระทรวงการคลัง (คคค.) พิจารณาอนุมัติ/รับทราบ แล้วแต่กรณี ตามระเบียบราชการต่อไป

หมวด 12
แนวปฏิบัติในการเผยแพร่ข้อมูลต่อสาธารณะ

ข้อ 1 การเผยแพร่ข้อมูลในความรับผิดชอบของ สบน. ต่อสาธารณะโดยผ่านระบบเทคโนโลยีสารสนเทศของ สบน. หน่วยงานเจ้าของข้อมูลจะต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำออกเผยแพร่ และหากข้อมูลที่นำออกเผยแพร่เกี่ยวข้องกับเรื่องนโยบายจะต้องได้รับความเห็นชอบจากผู้อำนวยการสำนักงานบริหารหนี้สาธารณะหรือผู้ซึ่งผู้อำนวยการสำนักงานบริหารหนี้สาธารณะมอบหมายก่อนนำออกเผยแพร่ ในกรณีที่ข้อมูลที่นำออกเผยแพร่มีความผิดพลาด และมีความเสียหายเกิดขึ้น โดยความเสียหายนั้นเกิดจากความจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ให้เป็นความรับผิดชอบของเจ้าหน้าที่ผู้นำข้อมูลดังกล่าวออกเผยแพร่

ข้อ 2 การเผยแพร่ข้อมูลต่อสาธารณะโดยผ่านระบบเทคโนโลยีสารสนเทศของ สบน. ให้ดำเนินการโดยหน่วยงานเจ้าของข้อมูล เว้นแต่กรณีที่ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะหรือผู้ซึ่งผู้อำนวยการสำนักงานบริหารหนี้สาธารณะมอบหมาย สั่งการ หรือเห็นชอบไว้เป็นอย่างอื่น

ประกาศ ณ วันที่ 31 กรกฎาคม พ.ศ. 2567

(นายพชร อนันตศิลป์)
ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ

ภาคผนวก ก
ขั้นตอนการลงทะเบียนผู้ใช้งานสำนักงานบริหารหนี้สาธารณะ

มีขั้นตอนการปฏิบัติ ดังนี้

1 การลงทะเบียนขอเข้าใช้งานเครื่องคอมพิวเตอร์ E-Mail ระบบงานภายใน (Intranet) และอินเทอร์เน็ตผ่านเครือข่าย สบน. ให้ใช้แบบฟอร์มสำหรับลงทะเบียนพนักงานใหม่ผ่านระบบ Intranet

2 การติดตั้งโปรแกรมเพิ่มเติมในเครื่องคอมพิวเตอร์ สบน. ให้ส่งคำขอติดตั้งพร้อมเหตุผลความจำเป็นโดยใช้แบบฟอร์มคำขอผ่านระบบ Intranet

ภาคผนวก ข
มาตรฐานการติดตั้งโปรแกรมและตั้งค่าเครื่องคอมพิวเตอร์ ของ สำนักงานบริหารหนี้สาธารณะ

มีขั้นตอนการปฏิบัติดังนี้

1. ติดตั้งเครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง และเครื่องสำรองไฟเครื่องใหม่ ณ สถานที่ที่ สบน. กำหนดไว้

2. ตั้งค่าการเชื่อมต่อสัญญาณเครือข่ายภายในของ สบน.เพื่อ Join Domain

3. ตั้งค่าเครื่องคอมพิวเตอร์ (Computer Name) ตามชื่อย่อ สำนัก/ศูนย์/กลุ่ม - ชื่อจริง เช่น IT-Orrawon, IT-Anuchit เป็นต้น

หมายเหตุ : ชื่อย่อ สำนัก/ศูนย์/กลุ่ม (สจน.1= DMB1, สจน.2=DMB2, สนผ.=PPB, สบช.= PAB, สลก.=OOS, กบส.= IAG, กม. = LAW, กบส.= RMG)

4. ติดตั้งโปรแกรมมาตรฐานในการใช้งานคอมพิวเตอร์ตามที่ สบน. กำหนด ดังนี้

4.1 ชุดโปรแกรมระบบปฏิบัติการ Microsoft Windows

4.2 ชุดโปรแกรมสำนักงาน Microsoft Office

4.3 โปรแกรมประเภท Anti-Virus

4.4 โปรแกรมติดต่อสื่อสารภายในองค์กร (Skype for Business)

4.5 โปรแกรมสำหรับประชุมทางไกล (Cisco Webex)

4.6 โปรแกรมประเภท Zip File

4.7 โปรแกรม Acrobat Reader

4.8 โปรแกรมประเภท Browser (Firefox, Chrome, Edge)

ภาคผนวก ค
ข้อปฏิบัติและหลักเกณฑ์ในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

มีขั้นตอนการปฏิบัติ ดังนี้

1 ผู้ใช้งานต้องทำการ Log-out ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

2 ผู้ใช้งานมีหน้าที่รับผิดชอบในการ Update โปรแกรมป้องกันไวรัสอย่างน้อยทุก 30 วัน เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

3 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่

4 หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

5 ผู้ใช้งานควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

6 ผู้ใช้งานไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

7 หากผู้ใช้งานลาออกจะต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบทันที เพื่อป้องกันการสวมสิทธิ

ภาคผนวก ง
มาตรฐานการพัฒนาซอฟต์แวร์

การจัดหาระบบสารสนเทศเพื่อมาสนับสนุนการทำงานในหน่วยงานมี 2 ลักษณะ ได้แก่ 1. หน่วยงานพัฒนาระบบสารสนเทศขึ้นใช้เอง 2. จัดซื้อจัดจ้างตามระเบียบพัสดุ เพื่อจัดหาผู้พัฒนาระบบสารสนเทศตามที่หน่วยงานต้องการ ซึ่งทั้ง 2 ลักษณะ สามารถนำเอากระบวนการในการพัฒนาซอฟต์แวร์ตามมาตรฐาน ISO/IEC 29110 มาประยุกต์ใช้ เพื่อให้ระบบสารสนเทศมีคุณภาพตามมาตรฐานสากล รวมถึงการจัดทำเอกสารที่เป็นระบบทำให้เจ้าหน้าที่สามารถปรับปรุงดูแลระบบต่อได้

1. หน่วยงานที่พัฒนาระบบสารสนเทศขึ้นใช้เองกรณีหน่วยงานมีความพร้อมด้านบุคลากรที่มีความสามารถในการพัฒนาระบบงานสารสนเทศขึ้นมาสนับสนุนในการทางานภายในหน่วยงานของตนเอง โดยหน่วยงานเหล่านี้ให้ความสำคัญต่อการปรับปรุงกระบวนการทำงาน จึงนำมาตรฐาน ISO/IEC 29110 มาประยุกต์ใช้ในการบริหารจัดการโครงการทางด้านสารสนเทศขององค์กร มีขั้นตอน ดังนี้

1.1 ศึกษาและจัดทำขอบเขตของโครงการ (Statement of Work) หน่วยงานดำเนินศึกษาความต้องการของหน่วยงานหรือผู้ใช้ที่ต้องการนำระบบสารสนเทศมาใช้ เพื่อจัดทำเป็นขอบเขตของการดำเนินโครงการ และกำหนดระยะเวลาที่ใช้ในการดำเนินโครงการรายการสิ่งที่ต้องส่งมอบให้กับผู้ใช้

1.2 จัดทำแผนการดำเนินโครงการ (Project Plan) ผู้บริหารโครงการต้องดำเนินการวางแผนในการดำเนินโครงการ โดยอ้างอิงจากขอบเขตของโครงการ (Statement of Work) มีการกำหนดบุคลากรในโครงการกำหนดพื้นที่จัดเก็บของโครงการมีการประเมินความเสี่ยงในการดำเนินโครงการและนำเสนอแผนในการดำเนินโครงการให้ผู้ที่เกี่ยวข้องได้รับทราบ

1.3 จัดเตรียมพื้นที่สำหรับโครงการ (Project Repository) ผู้บริหารโครงการต้องประสานกับผู้ดูแลเครื่อง Server เพื่อขอพื้นที่ที่ใช้ในการจัดเก็บเอกสารและโปรแกรมที่พัฒนา

1.4 รวบรวมและวิเคราะห์ความต้องการ (Requirement Gathering) นักวิเคราะห์และออกแบบระบบงานจะดำเนินการรวบรวมความต้องการจากผู้ใช้งาน แล้วนำความต้องการที่ได้มาศึกษาทำความเข้าใจและวิเคราะห์เพื่อสรุปเป็นความต้องการของระบบและซอฟต์แวร์

1.5 ยืนยันความต้องการกับผู้ใช้ (Validation Results) นักวิเคราะห์และออกแบบระบบงานจะนำความต้องการที่สรุปได้กลับไปยืนยันความต้องการกับผู้ใช้ เพื่อให้เกิดความเข้าใจที่ตรงกัน

1.6 จัดทำเอกสารสรุปความต้องการของระบบ (Requirements Specification) นักวิเคราะห์และออกแบบระบบงานจะนำความต้องการที่ผ่านการยืนยันมาจัดทำเอกสารสรุปความต้องการของระบบ และนำไปให้ผู้ใช้งานพิจารณาเห็นชอบ

1.7 ออกแบบระบบและซอฟต์แวร์ (System and Software Design) นักวิเคราะห์และออกแบบระบบงานดำเนินการออกแบบระบบและซอฟต์แวร์ตามเอกสารสรุปความต้องการของระบบ เช่น การออกแบบสถาปัตยกรรมของระบบและซอฟต์แวร์ (System & Software Architecture) การออกแบบรายละเอียดของหน้าจอ (Screens Design) การออกแบบรายละเอียดของรายงาน (Reports Design) การออกแบบโครงสร้างฐานข้อมูล (E-R Diagram and Data Dictionary) ขั้นตอนการทำงาน (Work Flow Diagram) ฯลฯ โดยให้สอดคล้องตามความต้องการของเอกสารสรุปความต้องการของระบบ

1.8 ออกแบบเอกสารแสดงตัวอย่างข้อมูลที่ใช้ทดสอบนักวิเคราะห์และออกแบบระบบงานจะดำเนินการออกแบบตัวอย่างข้อมูลที่จะใช้ในการทดสอบการใช้งานซอฟต์แวร์ เพื่อให้ครอบคลุมตามความต้องการของเอกสารสรุปความต้องการของระบบ และถูกต้องตามเอกสารการออกแบบระบบและซอฟต์แวร์

1.9 เอกสารบันทึกการตรวจสอบย้อนกลับของระบบนักวิเคราะห์และออกแบบระบบงานดำเนินการบันทึกข้อมูลลงในเอกสารเพื่อดูความสัมพันธ์จากความต้องการ (Requirements) เชื่อมไปยังการออกแบบ (Design) เชื่อมไปยังโปรแกรม(Components) และเชื่อมไปยังชุดข้อมูลที่ใช้ทดสอบ (Test Cases)

1.10 พัฒนาระบบงานนักพัฒนาโปรแกรมดำเนินการพัฒนาตามเอกสารการออกแบบระบบและซอฟต์แวร์ (Software Design) และการทดสอบการใช้งานเบื้องต้น (Unit Test)

1.11 ทดสอบระบบงาน (Test Report) ผู้ทดสอบระบบดำเนินการทดสอบการใช้งานโดยใช้ข้อมูลที่ใช้ทดสอบ (Test Cases) และบันทึกผลลัพธ์ของการทดสอบในเอกสารการทดสอบระบบงาน (Test Report) หากพบปัญหาในการใช้งานจะรายงานผลต่อผู้ที่เกี่ยวข้องเพื่อดำเนินการแก้ไขให้ระบบใช้งานได้สมบูรณ์

1.12 จัดทำคู่มือการใช้งานสำหรับผู้ใช้ (Software User Document) นักวิเคราะห์และออกแบบระบบงานจะเริ่มจัดทำคู่มือการใช้งานสำหรับผู้ใช้ (Software User Document) หลังจากที่ผ่านการทดสอบการใช้งานเป็นที่เรียบร้อย

1.13 จัดทำคู่มือปฏิบัติงานสำหรับผู้ดูแลระบบ (Product Operation Guide) ผู้ดูแลระบบงานเริ่มจัดทำคู่มือปฏิบัติงานสำหรับผู้ดูแลระบบ (Product Operation Guide) เพื่ออธิบายถึงวิธีการในการดูแลรักษาระบบงานให้สามารถใช้งานได้อย่างต่อเนื่องรวมถึงการสำรองข้อมูล (Database Backup)

1.14 จัดทำคู่มือการบำรุงรักษาระบบงาน (Maintenance Document) ผู้ดูแลระบบงานเริ่มจัดทำคู่มือการบำรุงรักษาระบบงาน (Maintenance Document) ซึ่งเป็นการอธิบายถึงการเตรียมสภาพแวดล้อมในการพัฒนาระบบ และการทดสอบระบบ รวมถึงการสรุปเวอร์ชันสุดท้ายของเอกสารต่าง ๆ ณ วันส่งมอบงาน

1.15 ส่งมอบงาน (Acceptance Record) ผู้บริหารโครงการจัดทำเอกสารประกอบการส่งมอบงาน (Acceptance Record) ให้กับผู้ใช้งานได้ลงนามรับมอบระบบงานที่พัฒนาขึ้น

1.16 รายงานการประชุม (Meeting Record) การบริหารโครงการจำเป็นต้องมีการบันทึกรายงานการประชุม (Meeting Record) ทุกครั้ง ไม่ว่าจะเป็นการประชุมภายในทีมงาน และประชุมร่วมกับผู้ใช้งาน

1.17 รายงานความก้าวหน้าของโครงการ (Progress Status Record) การบริหารโครงการผู้บริหารโครงการจะต้องจัดทำรายงานความก้าวหน้าของโครงการ (Progress Status Record) เป็นระยะตามข้อตกลงของโครงการเพื่อใช้ในการติดตามความก้าวหน้าในการดำเนินโครงการรวมทั้งปัญหาและอุปสรรคที่พบระหว่างดำเนินโครงการ

1.18 สรุปปัญหาที่พบระหว่างดำเนินโครงการ (Correction Register) การบริหารโครงการผู้บริหารโครงการจะต้องบันทึกปัญหาที่พบระหว่างดำเนินโครงการ (Correction Register) โดยเฉพาะปัญหาที่ส่งผลกระทบกับแผนการดำเนินโครงการทำให้จำเป็นต้องมีการปรับเปลี่ยนแผนการดำเนินโครงการ (Project Plan) และผู้บริหารโครงการจะต้องติดตามปัญหาให้มีการดำเนินการแก้ไขปัญหาให้เรียบร้อย

1.19 การตรวจสอบตามข้อกำหนดของมาตรฐาน (Verification Result) การบริหารโครงการผู้ควบคุมคุณภาพจะดำเนินการตรวจสอบผลการดำเนินการของบุคลากรของโครงการตลอดระยะเวลาของโครงการ และเป็นไปตามที่แผนการดำเนินโครงการ (Project Plan) ได้กำหนดไว้

1.20 การขอเปลี่ยนแปลงความต้องการ (Change Request) การบริหารโครงการต้องบันทึกการขอเปลี่ยนแปลงความต้องการ (Change Request) ของผู้ใช้งานหลังจากที่ผู้ใช้งานได้พิจารณาเห็นชอบเอกสารสรุปความต้องการของระบบ (Requirement Specification) ซึ่งนักวิเคราะห์และออกแบบระบบงานจะต้องวิเคราะห์หาผลกระทบที่ได้จากการขอเปลี่ยนแปลง และประเมินระยะเวลาที่ใช้ในการดำเนินการ

2. สำหรับหน่วยงานที่ใช้ตรวจรับการจัดซื้อจัดจ้างกรณีหน่วยงานต้องการจัดซื้อจัดการโครงการในการพัฒนาระบบงานสารสนเทศ และมีความต้องการที่จะนำมาตรฐานมาควบคุมกระบวนการในการพัฒนาซอฟต์แวร์ให้สอดคล้องกับมาตรฐาน ISO/IEC 29110 เพื่อที่จะได้นำมาใช้กำกับติดตามโครงการเพื่อให้เกิดประสิทธิภาพและประสิทธิผล ซึ่งตามกระบวนการในการจัดซื้อจัดจ้างจะต้องมีการกำหนดขอบเขตของระบบงาน (Term of Reference : TOR) จำเป็นต้องมีการกำหนดรายละเอียดของเอกสารต่างๆ ที่จำเป็นตามข้อกำหนดของมาตรฐาน ISO/IEC 29110 มีขั้นตอน ดังนี้

2.1 ศึกษารายละเอียดความต้องการระบบและซอฟต์แวร์เพื่อจัดทำ TOR

2.2 จัดหาผู้รับจ้างตามระเบียบราชการ

2.3 เชิญผู้รับจ้างมาลงนามในสัญญา เพื่อเริ่มดำเนินโครงการตาม TOR

2.4 คณะกรรมการตรวจรับการจ้างต้องตรวจสอบ :

- แผนการดำเนินโครงการ (Project Plan) ว่ามีความเหมาะสมและสอดคล้องกับTOR
- เอกสารยืนยันความต้องการกับผู้ใช้งาน (Validation Result) ว่ามีการยืนยันความต้องการครบถ้วนตามเอกสาร TOR
- เอกสารสรุปความต้องการของระบบ (Requirements Specification) ว่าเอกสารได้ผ่านการพิจารณาเห็นชอบ

- เอกสารการออกแบบระบบและซอฟต์แวร์ (System & Software Design) ว่าสอดคล้องกับเอกสารสรุปความต้องการของระบบ (Requirements Specification)

- เอกสารแสดงตัวอย่างข้อมูลที่ใช้ทดสอบ (Test Cases and Test Procedures) ว่าสอดคล้องกับเอกสารการออกแบบระบบและซอฟต์แวร์ (System & Software Design)

- เอกสารบันทึกการตรวจสอบย้อนกลับของระบบ (Traceability Record) เพื่อดูว่ามีความสัมพันธ์จากความต้องการ (Requirements) เชื่อมไปยังการออกแบบ (Design) โปรแกรม (Components) และข้อมูลที่ใช้ทดสอบ (Test Cases) ครบถ้วน

- เอกสารผลการทดสอบระบบงาน (Test Report) เพื่อดูว่าระบบงานทั้งหมดได้ผ่านการทดสอบครบถ้วนพร้อมที่จะนำไปใช้งาน

2.5 คณะกรรมการตรวจรับการจ้างดำเนินการจัดหาตัวแทนของผู้ใช้งานเพื่อให้ทดสอบการใช้งานเพื่อให้แน่ใจว่าระบบงานที่ส่งมอบมีความพร้อมที่จะนาไปใช้จริง (User Acceptance Test : UAT)

2.6 ผู้รับจ้างดำเนินการจัดฝึกอบรมการใช้งานให้แก่ตัวแทนของหน่วยงาน เพื่อให้เกิดทักษะและพร้อมในการใช้งานจริง

2.7 คณะกรรมการตรวจรับการจ้างต้องตรวจสอบ :

- คู่มือการใช้งานสำหรับผู้ใช้งาน (Software User Document) ว่ามีเนื้อหาเหมาะสมเพียงพอที่ผู้ใช้งานนำไปศึกษาการใช้ระบบงาน

- คู่มือปฏิบัติงานสำหรับผู้ดูแลระบบ (Product Operation Guide) ว่ามีเนื้อหาที่เหมาะสมเพียงพอที่ผู้ดูแลระบบงานของหน่วยงานสามารถนำไปปฏิบัติในการดูแลการใช้งาน

- คู่มือการบำรุงรักษาระบบงาน (Maintenance Document) ว่ามีรายละเอียดเพียงพอต่อการเตรียมสภาพแวดล้อมในการพัฒนาระบบ และการทดสอบระบบ

- รายงานการประชุมว่ามีความถูกต้อง

- รายงานความก้าวหน้าของโครงการ (Progress Status Record) เพื่อติดตามความก้าวหน้าของโครงการ หากพบปัญหาระหว่างดำเนินโครงการที่เกี่ยวข้องกับทางหน่วยงาน จะได้ประสานไปยังผู้ที่เกี่ยวข้องในการแก้ไขปัญหาเพื่อที่จะได้ไม่ส่งผลกระทบการการดำเนินโครงการ

2.8 คณะกรรมการตรวจรับการจ้างต้องจัดทำรายงานผลการตรวจสอบ ที่ได้ตรวจสอบตามข้อกำหนดของมาตรฐาน (Verification Results)

2.9 คณะกรรมการตรวจรับการจ้างดำเนินการตรวจรับงานที่ผู้รับจ้างส่งมอบ

ภาคผนวก จ
ผู้รับผิดชอบดูแลอุปกรณ์และระบบเทคโนโลยีสารสนเทศ

ที่	อุปกรณ์	ครรชิต	มนัสวี	ดำรัส	ชานนท์	นรเดช	วรินทร
1	ระบบงานห้องศูนย์ปฏิบัติการเครื่องคอมพิวเตอร์ (Server Room)	✓	✓		✓	✓	✓
	1.1 ระบบปรับอากาศ (Air)	✓	✓		✓	✓	✓
	1.2 ระบบตรวจจับน้ำรั่ว (Water Leak)	✓	✓		✓	✓	✓
	1.3 ระบบสำรองไฟฟ้า (UPS 20 K)	✓	✓		✓	✓	✓
	1.4 ระบบดับเพลิงอัตโนมัติ (FM 200)	✓	✓		✓	✓	✓
	1.5 ระบบเปิด - ปิดห้องศูนย์ปฏิบัติการเครื่องคอมพิวเตอร์ (Server Room)	✓	✓		✓	✓	✓
2	โปรแกรมตรวจสอบความปลอดภัยสำหรับ Server, Client และ Gateway	✓	✓		✓	✓	✓
3	เครื่องแม่ข่ายชนิด Blade	✓	✓		✓	✓	✓
4	อุปกรณ์จัดเก็บข้อมูล Storage Area Network (SAN Storage)	✓	✓		✓	✓	✓
5	อุปกรณ์สื่อสารไร้สายความเร็วสูง	✓	✓		✓	✓	✓
6	อุปกรณ์ป้องกันด้านรักษาความปลอดภัย UNIFIED THREAT MANAGEMENT (UTM)	✓	✓		✓	✓	✓
7	อุปกรณ์ควบคุมอุปกรณ์กระจายสัญญาณแบบไร้สาย (Wireless Controller)	✓	✓		✓	✓	✓
8	อุปกรณ์กระจายสัญญาณสำหรับห้องศูนย์ปฏิบัติการเครื่องคอมพิวเตอร์ (Server Room)	✓	✓		✓	✓	✓
9	อุปกรณ์กระจายสัญญาณสำหรับ Server	✓	✓		✓	✓	✓
10	อุปกรณ์กระจายสัญญาณสำหรับ Client	✓	✓		✓	✓	✓
11	ใบรับรองความปลอดภัยทางอิเล็กทรอนิกส์สำหรับเว็บไซต์ (SSL Certificates)	✓	✓		✓	✓	✓

ภาคผนวก จ (ต่อ)
ผู้รับผิดชอบดูแลอุปกรณ์และระบบเทคโนโลยีสารสนเทศ

ที่	ระบบเทคโนโลยีสารสนเทศ	ครรชิต	มนัสวี	ดำรัส	ชานนท์	นรเดช	วรินทร
1	ระบบงานสร้างแบบจำลองความเสี่ยงด้านหนี้สาธารณะ (Risk Model)	✓	✓	✓	✓	✓	✓
2	ระบบการคำนวณค่าธรรมเนียมการค้ำประกันและให้กู้ต่อ (Credit Fee)	✓	✓	✓	✓	✓	✓
3	ระบบฐานข้อมูลการวิเคราะห์ความเสี่ยงทางเครดิต (Credit Scoring)	✓	✓	✓	✓	✓	✓
4	ระบบบริหารจัดการข้อมูลการบริหารการชำระหนี้ ภายใต้ระบบ GFMIS-TR (Data Management TR : DMTR)	✓	✓	✓	✓	✓	✓
5	ระบบบริหารจัดการโครงการลงทุนด้านโครงสร้างพื้นฐาน (Infrastructure Investment Project Management : IIPM)	✓	✓	✓	✓	✓	✓
6	ระบบสารสนเทศเพื่อจัดทำแผนการบริหารหนี้สาธารณะ (DDPlan)	✓	✓	✓	✓	✓	✓
7	ระบบบริหารหนี้สาธารณะ (PDM)	✓	✓	✓	✓	✓	✓
8	ระบบสำนักงานอัจฉริยะ (Smart Office)	✓	✓	✓	✓	✓	✓
9	ระบบแอปพลิเคชันของ สบน. (PDMO Mobile APP)	✓	✓	✓	✓	✓	✓
10	ระบบเว็บไซต์ภายใน (Intranet)	✓	✓	✓	✓	✓	✓
11	ระบบประชาสัมพันธ์ภายในองค์กร (PDMO TV Channel)	✓			✓	✓	✓
12	ระบบติดต่อสื่อสารภายในองค์กร (Skype for Business)	✓	✓	✓	✓	✓	✓
13	ระบบเว็บไซต์สำนักงานบริหารหนี้สาธารณะ (www.pdmo.go.th)	✓	✓	✓	✓	✓	✓
14	ระบบ SmartBond 4D	✓	✓	✓	✓	✓	✓
15	ระบบเว็บไซต์กองทุนบริหารเงินกู้เพื่อการปรับโครงสร้างหนี้สาธารณะและพัฒนาตลาดตราสารหนี้ในประเทศ (กปพ.) (www.pddf.or.th)	✓	✓	✓	✓	✓	✓
16	ระบบนายทะเบียนตั๋วระบบนายทะเบียนตั๋วสัญญาใช้เงินของกระทรวงการคลัง	✓	✓	✓	✓	✓	✓
17	ระบบลงเวลาปฏิบัติราชการ	✓	✓	✓	✓	✓	✓
18	ระบบประเมินผลการปฏิบัติราชการ (PMS)	✓	✓	✓	✓	✓	✓
19	ศูนย์ข้อมูลข่าวสาร	✓	✓	✓	✓	✓	✓

ภาคผนวก จ (ต่อ)
ผู้รับผิดชอบดูแลอุปกรณ์และระบบเทคโนโลยีสารสนเทศ

ที่	ระบบเทคโนโลยีสารสนเทศ	ครรชิต	มนัสวี	ดำรัส	ชานนท์	นรเดช	วรินทร
20	ศูนย์รับเรื่องร้องเรียน	✓	✓	✓	✓	✓	✓
21	ระบบการค้นหาข้อมูลที่ปรึกษา (Matching CDC)	✓	✓	✓	✓	✓	✓
22	ระบบจับคู่ที่ปรึกษาอัตโนมัติ	✓	✓	✓	✓	✓	✓
23	ระบบศูนย์ข้อมูลที่ปรึกษา (www.consultant.pdmo.go.th)	✓	✓	✓	✓	✓	✓
24	ระบบสารสนเทศด้านการตรวจสอบภายใน (Internal Audit)	✓	✓	✓	✓	✓	✓
25	ระบบฐานข้อมูลความเสี่ยงเพื่อการตรวจสอบภายใน	✓	✓	✓	✓	✓	✓
26	ระบบการจัดการความรู้ (KM)	✓	✓	✓	✓	✓	✓
27	ระบบบัญชีข้อมูลสารสนเทศ (PDMO Data Catalog)	✓	✓	✓	✓	✓	✓
28	ระบบสารสนเทศทรัพยากรบุคคลระดับกรม (DPIS)	✓	✓	✓	✓	✓	✓
29	ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)	✓	✓	✓	✓	✓	✓
30	ระบบประชุมทางไกล (Cisco Web)	✓	✓	✓	✓	✓	✓
31	ระบบบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ของ ธปท. (Electronic Financial Services : EFS)	✓	✓	✓	✓	✓	✓
32	ระบบการจำหน่ายพันธบัตรรัฐบาลและพันธบัตรออมทรัพย์ (สบม.)	✓	✓	✓	✓	✓	✓

ที่	ครุภัณฑ์คอมพิวเตอร์	ครรชิต	มนัสวี	ดำรัส	ชานนท์	นรเดช	วรินทร
1	คอมพิวเตอร์ส่วนบุคคล (PC)	✓	✓	✓	✓	✓	✓
2	คอมพิวเตอร์แบบพกพา (Notebook)	✓	✓	✓	✓	✓	✓
3	คอมพิวเตอร์หน้าจอสัมผัส (Tablet)	✓	✓	✓	✓	✓	✓
4	สแกนเนอร์ (Scanner)	✓	✓	✓	✓	✓	✓
5	เครื่องพิมพ์ (Printer)	✓	✓	✓	✓	✓	✓

ผู้รับผิดชอบการจัดทำแผนและทบทวนแผน

ศูนย์เทคโนโลยีสารสนเทศ ส่วนนโยบายและแผนสารสนเทศ