นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(Information Security Policy)
ISM-PL-001

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

การควบคุมเอกสาร (**Document Control**)

การอนุมัติเอกสาร (**Document Approvals**)

เอกสารฉบับนี้ได้รับการทบทวนและอนุมัติโดย

จัดเตรียมเอกสารโดย (Prepared by)	**ทบทวนโดย (Reviewed by)**	**อนุมัติโดย (Approved by)**
มติคณะกรรมการความปลอดภัยด้านสารสนเทศ ครั้งที่ 2/2558	มติคณะกรรมการจัดการ ครั้งที่ 11/2558	มติคณะกรรมการธนาคาร ครั้งที่ 8/2558
วัน-เดือน-ปี 13 พฤษภาคม 2558	วัน-เดือน-ปี 15 มิถุนายน 2558	วัน-เดือน-ปี 26 มิถุนายน 2558

ประวัติการแก้ไขเอกสาร

ครั้งที่ (Version)	**วัน-เดือน-ปี**	**รายละเอียด**	**แก้ไขโดย**
1.0	27/01/54	อนุมัติโดยคณะกรรมการธนาคาร ครั้งที่ 1/2554	คณะกรรมการความปลอดภัยด้านสารสนเทศ
2.0	29/02/55	อนุมัติโดยคณะกรรมการธนาคาร ครั้งที่ 2/2555	คณะกรรมการความปลอดภัยด้านสารสนเทศ
2.1	27/08/55	แก้ไขรหัส และชื่อเอกสาร	คณะทำงานความปลอดภัยด้านสารสนเทศ
2.2	06/12/55	ปรับปรุงตามความเห็นกระทรวง ICT และปรับ Bullet เป็นหัวข้อ เพื่อให้สะดวกในการอ้างอิง	คณะทำงานความปลอดภัยด้านสารสนเทศและผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ
2.3	1/02/56	ปรับปรุงตามความเห็นกระทรวง ICT และเปลี่ยนหรือตัดคำว่า “ เช่น/เป็นต้น”	คณะทำงานความปลอดภัยด้านสารสนเทศและผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ
2.4	17/06/56	ปรับปรุงตามความเห็นกระทรวง ICT เช่น เปลี่ยนจาก CFO เป็น CEO ที่รับผิดชอบกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายฯ และระบุการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศให้ชัดเจน เป็นต้น	คณะทำงานความปลอดภัยด้านสารสนเทศและผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ
2.4	26/07/56	อนุมัติโดยคณะกรรมการธนาคาร ครั้งที่ 7/2556	คณะกรรมการความปลอดภัยด้านสารสนเทศ

ครั้งที่ (Version)	วัน-เดือน-ปี	รายละเอียด	แก้ไขโดย
3.0 – 4.0	20/04/58	ปรับปรุงเวอร์ชั่น	คณะกรรมการความปลอดภัยด้านสารสนเทศ
5.0	26/06/58	การทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปี 2557 อนุมัติโดยคณะกรรมการธนาคาร ครั้งที่ 8/2558	คณะกรรมการความปลอดภัยด้านสารสนเทศ

สารบัญ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ธสน.

1. วัตถุประสงค์

ธสน. ได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้สอดคล้องกับวิสัยทัศน์ ภารกิจ และยุทธศาสตร์ ของ ธสน. ในการเพิ่มศักยภาพในการบริหารจัดการ โดยมีวัตถุประสงค์เพื่อรักษาความมั่นคงปลอดภัยให้แก่สินทรัพย์ของธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย (ธสน.) โดยเฉพาะอย่างยิ่งสินทรัพย์ที่เป็นข้อมูลสำคัญในการดำเนินธุรกิจ โดยการปกป้องให้พ้นจากภัยคุกคามและความเสี่ยงทั้งจากภายในและภายนอก ธสน. ไม่ว่าจะเกิดขึ้นโดยเจตนาหรือไม่เจตนาก็ตาม รวมถึงเพื่อลดความเสียหายต่างๆ ที่อาจเกิดขึ้นจากเหตุละเมิดความมั่นคง และเพื่อรักษาไว้ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง โดยอ้างอิงจากกฎหมายและมาตรฐานที่สำคัญ

2. คำนิยาม

คำ	ความหมาย
ผู้ใช้งาน	บุคคลผู้ได้รับอนุญาตในการเข้าถึงข้อมูลหรือระบบเทคโนโลยีสารสนเทศ โดยอาจเป็นเจ้าหน้าที่ของ ธสน. หรือบุคคลภายนอก ทั้งนี้สิทธิของผู้ใช้งานจะอนุญาตโดยผู้มีอำนาจอนุมัติของ ธสน. และมีหน้าที่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้องอย่างเคร่งครัด
สิทธิของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับข้อมูลหรือระบบเทคโนโลยีสารสนเทศของ ธสน.
สินทรัพย์	สิ่งใดก็ตามที่มีมูลค่าแก่ ธสน. อันประกอบไปด้วย ข้อมูล ระบบงานเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ อุปกรณ์เครือข่ายสื่อสาร และซอฟต์แวร์
การเข้าถึงหรือการควบคุมการใช้งานเทคโนโลยีสารสนเทศ	การอนุญาต การกำหนดสิทธิ หรือมอบอำนาจในการเข้าถึง หรือใช้งานเครือข่าย หรือระบบเทคโนโลยีสารสนเทศ ทั้งทางกายภาพและทางอิเล็กทรอนิกส์ รวมทั้งการอนุญาตในลักษณะเดียวกันกับบุคคลภายนอก
ความมั่นคงปลอดภัยด้านสารสนเทศ	การรักษาไว้ซึ่งคุณสมบัติทางด้านความมั่นคงปลอดภัยต่อสินทรัพย์ของ ธสน. อันประกอบไปด้วย การรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้ (Availability) ของสินทรัพย์สารสนเทศ รวมทั้งคุณสมบัติอื่น คือ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
ระบบเทคโนโลยีสารสนเทศ	อุปกรณ์หรือชุดอุปกรณ์ทางด้านเทคโนโลยีสารสนเทศที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลให้เป็นสารสนเทศ

คำ	ความหมาย
เหตุการณ์ด้านความมั่นคงปลอดภัย (Event)	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศของ ธสน. ถูกบุกรุกหรือโจมตี และคุกคาม
คณะกรรมการความปลอดภัยด้านสารสนเทศ	ตัวแทน ธสน. ที่ได้รับการแต่งตั้ง ซึ่งประกอบด้วย ฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายงานที่เกี่ยวข้องกับธุรกิจสินเชื่อและรับประกันฯ สำนักกฎหมาย และสำนักบริหารความเสี่ยง โดยมีสำนักตรวจสอบ และสำนักกำกับการปฏิบัติงาน เป็นผู้สังเกตการณ์ โดยคณะกรรมการความปลอดภัยด้านสารสนเทศ มีหน้าที่ดังนี้ ● ดูแล และสอบทานเนื้อหาของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้อง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงและแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความปลอดภัยทางด้านสารสนเทศของ ธสน. รวมทั้งการขออนุมัติข้อยกเว้น และนำเสนอขออนุมัติจากคณะกรรมการธนาคาร โดยผ่านความเห็นชอบจากคณะกรรมการจัดการ ● จัดให้มีขั้นตอนการปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้องที่ได้รับอนุมัติ ● จัดให้มีการตรวจสอบสถานภาพปัจจุบันของความปลอดภัยสารสนเทศของ ธสน. ● จัดให้มีการตรวจสอบเหตุการณ์ที่กระทบด้านความปลอดภัยสารสนเทศของ ธสน. ● จัดให้มีการประเมินความมีประสิทธิผลและประสิทธิภาพในการปกป้องข้อมูล ● จัดให้มีการประเมินและบริหารความปลอดภัยของข้อมูลใน ธสน. ในภาพรวม ● นำเสนอการทบทวนนโยบาย แนวปฏิบัติ และชุดเอกสารที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศต่อคณะกรรมการจัดการ และคณะกรรมการธนาคาร เพื่อพิจารณาอนุมัติ ● อื่นๆ ตามที่ได้รับมอบหมาย
คณะกรรมการจัดการ	ผู้บริหารระดับสูงของ ธสน. ที่ได้รับการแต่งตั้ง ซึ่งคณะกรรมการจัดการมีหน้าที่ดังนี้ ● กลั่นกรองนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งนโยบายและแนวปฏิบัติงานด้านสารสนเทศอื่นๆ ที่เกี่ยวข้อง ● อนุมัติขั้นตอนการปฏิบัติงานด้านสารสนเทศต่างๆ ที่เกี่ยวข้อง ● มอบหมายให้คณะกรรมการความปลอดภัยด้านสารสนเทศทำหน้าที่สื่อสารนโยบายและแนวปฏิบัติด้านสารสนเทศ (Policy) ขั้นตอนการปฏิบัติงานด้านสารสนเทศ (Procedure) ข้อปฏิบัติด้านสารสนเทศ (Work Instruction) และแบบฟอร์มด้านสารสนเทศ (Form) ให้ผู้ที่เกี่ยวข้อง

	● ประกาศและบังคับใช้นโยบายและแนวปฏิบัติด้านสารสนเทศและชุดเอกสารต่างๆ ที่เกี่ยวข้อง ● กำกับ ดูแล และควบคุมการบังคับใช้นโยบายและแนวปฏิบัติด้านสารสนเทศและชุดเอกสารต่างๆ ที่เกี่ยวข้อง ● ทบทวนขั้นตอนการปฏิบัติงานด้านสารสนเทศ (Procedure) และชุดเอกสารต่างๆ ที่เกี่ยวข้อง ● อื่นๆ ตามที่ได้รับมอบหมาย
ผู้บริหารสูงสุดของ ธสน.	กรรมการผู้จัดการซึ่งเป็นผู้บริหารสูงสุดขององค์กรรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่ ธสน. หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมอบหมายให้คณะกรรมการความปลอดภัยด้านสารสนเทศ เป็นผู้รักษาการให้เป็นไปตามนโยบายฯ นี้
เจ้าของสารสนเทศ (Information Owner)	ผู้บริหารของหน่วยงานที่สร้างข้อมูลขึ้น หรือใช้งานข้อมูลมากที่สุด โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย และยังเป็นผู้รับผิดชอบในการอนุมัติสิทธิในการเข้าใช้สารสนเทศ
ผู้ดูแลระบบ	พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และสามารถเข้าถึงซอฟต์แวร์คอมพิวเตอร์หรือข้อมูลอื่นเพื่อจัดการระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายสื่อสารได้
มาตรฐาน	บรรทัดฐานที่บังคับใช้ในการปฏิบัติงานจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
รหัสผ่าน	ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นส่วนหนึ่งในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
ระบบเครือข่าย	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ ดังต่อไปนี้ ● ระบบแลน (Local Area Network : LAN) ● ระบบแวน (Wide Area Network : WAN) ● ระบบอินทราเน็ต (Intranet) ● ระบบอินเทอร์เน็ต (Internet)
ระบบแลน (Local Area Network) และ ระบบอินทราเน็ต (Intranet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายใน ธสน. เข้าด้วยกัน เป็นระบบเครือข่ายที่มีวัตถุประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายใน ธสน.
ระบบอินเทอร์เน็ต	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล
ลงบันทึกเข้า (Login)	กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

ลงบันทึกออก (Logout)	กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย
สื่อบันทึกพกพาและอุปกรณ์เคลื่อนที่ต่างๆ	สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูลที่มีขนาดกะทัดรัด ติดตั้ง หรือถอดได้ง่ายและสะดวกต่อการพกพา ดังต่อไปนี้ ● Flash Drive หรือ Handy Drive หรือ Thumb Drive ● External Hard Disk ● Floppy Disk ● PDA หรือ Smart Phone หรือ Tablet หรือ Phablet ● CD-Rom
หน่วยงานภายนอก	องค์กรหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่างๆ ของ ธสน. โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
อัพเดท (Update)	ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันตามกรอบเวลาที่กำหนด

3. ขอบข่าย

1) ข้อมูลทั้งหมด (ทั้งที่อยู่ในรูปเอกสาร และอิเล็กทรอนิกส์ไฟล์) ที่ได้รับการจัดเก็บ ได้รับการใช้งาน หรือใช้ในการสื่อสารเพื่อดำเนินกิจการของ ธสน.
2) บุคคลทั้งหมดที่มีส่วนเกี่ยวข้องในการใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศของ ธสน. (คณะกรรมการธนาคาร ฝ่ายจัดการ ผู้บริหาร พนักงานประจำ ลูกจ้าง บุคคลภายนอกที่ถูกว่าจ้างโดย ธสน. บริษัทคู่ค้า บริษัทหรือบุคคลที่เป็นคู่สัญญา และผู้ให้บริการ)
3) สินทรัพย์ทั้งหมดที่เกี่ยวข้องกับข้อมูลและที่ใช้ในการจัดเก็บ ส่งผ่าน หรือประมวลผลข้อมูล ดังต่อไปนี้ อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ ซอฟต์แวร์ โปรแกรมประยุกต์ เอกสารอิเล็กทรอนิกส์ เอกสารตีพิมพ์ เครื่องมือ สิ่งอำนวยความสะดวก ตลอดจนบริการที่ได้รับ

3.1 นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.1.1 เพื่อคุ้มครองผลประโยชน์และชื่อเสียงของ ธสน. พนักงานทุกคนจะต้อง

1) ปกป้องข้อมูล (ไม่ว่าจะถูกเก็บอยู่ในรูปแบบใดก็ตาม) ให้พ้นจากเหตุละเมิดต่างๆ ซึ่งอาจส่งผลกระทบต่อความลับของข้อมูล (Confidentiality) ความถูกต้องและสมบูรณ์ครบถ้วนของข้อมูล (Integrity) หรือความมีพร้อมใช้งานของข้อมูล (Availability)
2) ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ ธสน. กำหนด เพื่อความมั่นคงปลอดภัยด้านสารสนเทศ
3) ปฏิบัติตามข้อกฎหมายอื่นๆ ที่เกี่ยวข้องทั้งหมด

3.1.2 ธสน. มีนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังต่อไปนี้

1) ข้อมูลที่สำคัญของ ธสน. จะต้องได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต
2) ข้อมูลที่สำคัญของ ธสน. จะต้องได้รับการรักษาความลับอย่างเหมาะสม
3) ข้อมูลที่สำคัญของ ธสน. จะต้องมีความถูกต้องและสมบูรณ์ครบถ้วน
4) ข้อมูลที่สำคัญของ ธสน. จะต้องมีพร้อมใช้งานอยู่เสมอ

5) กฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้องต่างๆ จะต้องได้รับการปฏิบัติตามอย่างถูกต้องครบถ้วน
6) นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศรวมถึงแนวปฏิบัติและเอกสารที่เกี่ยวข้องจะต้องถูกสื่อสารไปยังบุคคลทั้งหมดที่มีส่วนเกี่ยวข้องในการใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศของ ธสน. อย่างเหมาะสม
7) พนักงานทุกคนจะต้องได้รับการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม
8) จัดให้มีการตรวจสอบ (Internal Audit) และบริหารความเสี่ยง (Risk Management) ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
9) จัดทำแผนการบริหารความต่อเนื่องทางธุรกิจเพื่อให้ธุรกิจดำเนินได้อย่างต่อเนื่อง พร้อมทั้งทำการดูแลรักษา และทดสอบแผนฯ อย่างเหมาะสม
10) จัดให้มีชุดเอกสารนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้อง เพื่อกำหนดระเบียบปฏิบัติ ตลอดจนแนวทางการปฏิบัติงานและการใช้งานข้อมูลอย่างมั่นคงปลอดภัย ดังต่อไปนี้
    1. แนวปฏิบัติสำหรับผู้ใช้งานเทคโนโลยีสารสนเทศ (Acceptable Use Guideline)
       ผู้รับผิดชอบ คือ คณะกรรมการจัดการ ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายทรัพยากรบุคคล
    2. แนวปฏิบัติ เรื่อง ระดับชั้นความลับของข้อมูล (Information Classification and Handling Guideline)
       ผู้รับผิดชอบ คือ คณะกรรมการจัดการ สำนักบริหาร และสำนักกำกับการปฏิบัติงาน
    3. แนวปฏิบัติ เรื่อง การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (System Access Control Guideline)
       ผู้รับผิดชอบ คือ คณะกรรมการจัดการ ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายทรัพยากรบุคคล
    4. แนวปฏิบัติ เรื่อง การบริหารจัดการเครือข่ายคอมพิวเตอร์ (Network Management Guideline)
       ผู้รับผิดชอบ คือ คณะกรรมการจัดการ และฝ่ายเทคโนโลยีสารสนเทศ
    5. แนวปฏิบัติ เรื่อง การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control Guideline)
       ผู้รับผิดชอบ คือ คณะกรรมการจัดการ และฝ่ายเทคโนโลยีสารสนเทศ
    6. แนวปฏิบัติ เรื่อง การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Information Access Control Guideline)
       ผู้รับผิดชอบ คือ คณะกรรมการจัดการ และฝ่ายเทคโนโลยีสารสนเทศ
    7. นโยบายและแนวปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Policy)

ผู้รับผิดชอบ คือ คณะผู้บริหารความเสี่ยง และคณะทำงานพัฒนาแผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM)

8. นโยบายและแนวปฏิบัติ เรื่อง การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing Policy)
   ผู้รับผิดชอบ คือ คณะกรรมการธนาคาร

11) จัดให้มีกระบวนการในการรายงาน สอบข้อเท็จจริง รับมือ และจัดการกับเหตุละเมิดความมั่นคงปลอดภัยอย่างเหมาะสม โดยเหตุละเมิดความมั่นคงปลอดภัย ตลอดจนสิ่งผิดปกติ และเหตุการณ์ที่น่าสงสัยอื่นๆ จะต้องได้รับการรายงานไปที่คณะกรรมการจัดการหรือผู้ได้รับมอบหมาย เพื่อดำเนินการตรวจสอบและแก้ไข

12) กรรมการผู้จัดการ ซึ่งเป็นผู้บริหารสูงสุดขององค์กร รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่ ธสน. หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมอบหมายให้คณะกรรมการความปลอดภัยด้านสารสนเทศเป็นผู้รักษาการให้เป็นไปตามนโยบายฯ นี้

13) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

3.2 การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการตรวจสอบภายใน

3.2.1 พนักงานและบุคคลที่เกี่ยวข้องทุกคนจะต้องลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) และ/หรือ เอกสารอื่นๆ ที่เกี่ยวข้อง เพื่อเป็นการยอมรับว่าข้อมูลต่างๆ ที่ได้รับทราบและใช้งานในระหว่างการจ้างงาน เป็นสินทรัพย์ของ ธสน. และไม่สามารถนำไปใช้เพื่อการอื่นโดยมิได้รับอนุญาต ทั้งนี้ ในการใช้งานข้อมูลทั้งหลายใน ธสน. จะถือว่าทุกคนรับทราบและยินยอมปฏิบัติตามเงื่อนไขของนโยบายฯ นี้ทุกประการ

3.2.2 การเจตนาเข้าถึงระบบโดยไม่ได้รับอนุญาต การจงใจใส่ข้อมูลที่ผิดพลาด และการเจตนาเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต ถือเป็นสิ่งต้องห้ามทั้งสิ้น และเพื่อให้มั่นใจได้ว่ามีการปฏิบัติตามนโยบายนี้อย่างเคร่งครัด การไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลนี้ถือว่ามีความผิดทางวินัย

3.2.3 ธสน. ต้องจัดให้มีการตรวจติดตามการปฏิบัติงานตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน ตลอดจนบุคคลอื่นที่เกี่ยวข้องเป็นระยะๆ ผ่านการตรวจสอบจากสำนักตรวจสอบ (Internal Audit) อย่างน้อยปีละ 1 ครั้ง และต้องให้การสนับสนุนผู้ตรวจสอบจากภายนอกในการตรวจสอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามความเหมาะสม

3.2.4 เพื่อเป็นแนวทางในการขออนุญาตให้มีข้อยกเว้นสำหรับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้อง ในกรณีที่พนักงานหรือหน่วยงานใน ธสน. ไม่สามารถปฏิบัติตามนโยบาย แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้องได้และจำเป็นต้องยกเว้นการบังคับใช้ในบางข้อ ทั้งนี้ เพื่อช่วยให้การปฏิบัติงานสามารถดำเนินการต่อไปได้ โดยแนวทางของการขออนุญาตยกเว้นจะประกอบด้วย การจัดทำเอกสารเกี่ยวกับเรื่องที่ต้องการยกเว้น การอนุมัติเพื่อ

ยกเว้นนโยบาย แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้อง ตามอำนาจที่ได้รับอนุมัติ และการสร้างมาตรการความคุมชดเชยเพื่อรองรับการยกเว้นดังกล่าว

ข้อพิจารณาในการยกเว้นนโยบาย แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้อง ต้องจัดทำเอกสารประกอบดังนี้

1) การขอยกเว้นของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้องนั้น ต้องมีเหตุผลอันควรทางธุรกิจและมีเอกสารประกอบ ตลอดจนต้องได้รับการอนุมัติก่อนจึงจะอนุญาตให้มีการยกเว้นได้
2) ข้อยกเว้นต่างๆ ต้องได้รับการกลั่นกรองจากคณะกรรมการความปลอดภัยด้านสารสนเทศ ก่อนนำเสนอตามลำดับชั้นไป
3) คณะกรรมการความปลอดภัยด้านสารสนเทศต้องตรวจทานและประเมินข้อยกเว้นของนโยบาย แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้องต่างๆ นั้นอย่างน้อยปีละ 1 ครั้ง
4) เจ้าของเรื่องต้องขออนุมัติใหม่หากยังไม่สามารถแก้ไขให้เป็นไปตามนโยบาย แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้องได้ภายในระยะเวลาที่กำหนด
5) หากข้อยกเว้นของนโยบาย แนวปฏิบัติ และเอกสารสนับสนุนที่เกี่ยวข้องนั้น มีผลกระทบต่อการควบคุมภายในที่มีอยู่เดิม ต้องมีการสร้างมาตรการควบคุมชดเชยขึ้นมารองรับสำหรับข้อยกเว้นดังกล่าว เพื่อให้มั่นใจได้ว่าความเสี่ยงที่เหลืออยู่ของ ธสน.อยู่ในระดับที่สามารถยอมรับได้
6) หลังจากที่ได้พิจารณาใช้มาตรการควบคุมดังกล่าวต้องถือปฏิบัติตามมาตรการควบคุมนั้น
7) การควบคุมชดเชยต้องได้รับการตรวจสอบโดยสำนักตรวจสอบ

3.3 การทบทวนและปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.3.1 นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของข้อมูลนี้ ต้องได้รับการทบทวน และประเมินผล เพื่อปรับปรุงเนื้อหา หรือยืนยันเนื้อหาเดิม โดยคณะกรรมการธนาคารอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้มั่นใจได้ว่าเนื้อหาของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ยังคงไว้ซึ่งความสมบูรณ์ มีประสิทธิภาพ และสามารถนำไปใช้งานได้อย่างเหมาะสม

3.4 บทลงโทษ

3.4.1 การละเมิด ฝ่าฝืน ละเลย หรือไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนวิธีการปฏิบัติงาน และเอกสารสนับสนุนต่างๆ ที่เกี่ยวข้องถือเป็นความผิดทางวินัย ซึ่งต้องถูกพิจารณาลงโทษทางวินัยตามระเบียบ ธสน. ที่เกี่ยวข้อง และหากการละเมิดหรือฝ่าฝืนนโยบายนั้นเข้าข่ายการกระทำที่ผิดกฎหมาย ผู้ละเมิดก็ต้องได้รับการดำเนินคดีตามที่กฎหมายระบุไว้

4. เอกสารอ้างอิง

4.1 ขั้นตอนการปฏิบัติงานเรื่อง การตรวจสอบภายใน ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Internal Audit Procedure for Information Security : MSP-PC-004)

4.2 ขั้นตอนการปฏิบัติงาน เรื่อง การประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Risk Assessment Procedure for Information Security : MSP-PC-001)