แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกองทุนบริหารเงินกู้เพื่อการปรับโครงสร้างหนี้สาธารณะ และพัฒนาตลาดตราสารหนี้ในประเทศ

สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง

สารบัญ

หมวด 1
การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมการเข้าถึงข้อมูลและการใช้อุปกรณ์ในการประมวลผลข้อมูล ของกองทุนบริหารเงินกู้เพื่อการปรับโครงสร้างหนี้สาธารณะและพัฒนาตลาดตราสารหนี้ในประเทศ (กปพ.) โดยให้ความสำคัญต่อการใช้งานตามภารกิจและความปลอดภัยในการอนุญาตให้เข้าถึงข้อมูล การกำหนดสิทธิ ประเภทของข้อมูล ลำดับความสำคัญหรือชั้นความลับของข้อมูล และช่องทางที่สามารถเข้าถึงได้

แนวทางปฏิบัติ

1.1 ผู้ดูแลระบบ ต้องจำแนกกลุ่มของระบบหรือการทำงาน โดยให้กำหนดผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

1.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และมีหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานสารสนเทศ รวมถึงทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้

1.2.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตกำหนดสิทธิ หรือการมอบอำนาจ

(1) กำหนดสิทธิในการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการใช้งาน ดังนี้

- สิทธิในการสร้างข้อมูล (Create)
- สิทธิในการอ่านข้อมูลหรือเรียกดูข้อมูล (Read)
- สิทธิในการเปลี่ยนแปลงหรือปรับปรุงข้อมูล (Modify/Update)
- สิทธิในการมอบหมายสิทธิในการดำเนินการแทน (Assign)
- สิทธิในการรับรองความถูกต้องครบถ้วนของข้อมูล (Approve)
- สิทธิในการรับรองการดำเนินการจัดทำ/แปลงข้อมูล (Authenticate)

(2) ผู้ใช้งานที่ต้องการใช้งานระบบสารสนเทศของหน่วยงานจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้จัดการ กปพ. หรือผู้มีอำนาจลงนาม

1.2.2 การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับ สอดคล้องกับแนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าวเป็นมาตรฐานที่มีความละเอียด รอบคอบ ถือว่าเป็นแนวทาทงที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(1) ประเภทข้อมูลหรือรูปแบบของเอกสารอิเล็กทรอนิกส์สามารถแบ่งได้ ดังนี้

- ข้อมูลและสารสนเทศสนับสนุนการตัดสินใจของผู้บริหาร (Early Indicator) ได้แก่ ข้อมูลและสารสนเทศที่มีความสำคัญหรือความจำเป็นเร่งด่วนที่ต้องมีการติดตามใกล้ชิด

เพื่อประกอบการตัดสินใจเชิงนโยบาย การกำหนดนโยบาย และการวางแผนของผู้จัดการ กปพ.

- ข้อมูลและสารสนเทศสนับสนุนเชิงยุทธศาสตร์ (Strategy Data) ได้แก่ ข้อมูลและสารสนเทศเชิงวิชาการเพื่อสนับสนุนการดำเนินงานตามพันธกิจและยุทธศาสตร์ของหน่วยงานให้บรรลุเป้าหมาย รวมทั้งข้อมูลที่เผยแพร่สู่สาธารณะ

- ข้อมูลและสารสนเทศสนับสนุนปฏิบัติงาน (Operation Data) ได้แก่ ข้อมูลและสารสนเทศเพื่อสนับสนุนการปฏิบัติงานทั่วไปของหน่วยงาน

(2) การแบ่งระดับความสำคัญของข้อมูล แบ่งเป็น 3 ระดับ ประกอบด้วย

- ข้อมูลที่มีความสำคัญมาก หมายถึง มีผลกระทบในระดับที่มีนัยสำคัญต่อการดำเนินงานตามวัตถุประสงค์ขององค์กร อาทิ รายการสินทรัพย์ลงทุนของ กปพ.

- ข้อมูลที่มีความสำคัญปานกลาง หมายถึง มีผลกระทบต่อการดำเนินภารกิจ อาทิ อัตราผลตอบแทนของผู้บริหารสินทรัพย์แต่ละราย

- ข้อมูลที่มีความสำคัญน้อย หมายถึง ไม่มีผลกระทบใดๆ ต่อการดำเนินภารกิจ อาทิ ประกาศ คำสั่ง ที่บังคับใช้ภายในหน่วยงาน

(3) การแบ่งลำดับชั้นความลับของข้อมูล แบ่งเป็น 4 ลำดับ ประกอบด้วย

- ข้อมูลลับที่สุด หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงานอย่างร้ายแรงที่สุด

- ข้อมูลลับมาก หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงานอย่างร้ายแรง

- ข้อมูลลับ หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงาน

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(4) กำหนดเวลาการเข้าถึงสารสนเทศ ดังนี้

- ข้อมูลที่เผยแพร่บนเว็บไซต์ของ กปพ. (http://www.pddf.or.th) สำหรับผู้ใช้งานภายนอก สามารถเข้าถึงได้ตลอดเวลา

- ระบบงานภายใน (Back Office) สำหรับเจ้าหน้าที่หรือผู้ใช้งานภายใน ตามที่หน่วยงานกำหนด

(5) กำหนดช่องทางการเข้าถึง สิทธิในการเข้าถึงข้อมูลและสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น โดยมีช่องทางการเข้าถึง ดังนี้

- ระบบเครือข่ายอินเทอร์เน็ต (Internet)

- ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

1.2.3 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

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

1.2.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการเปลี่ยนแปลงสิทธิต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

1.2.6 กรณีมีการจ้างผู้ให้บริการภายนอก (Outsource) ในการพัฒนา ดูแล และบำรุงรักษาระบบสารสนเทศ มีมาตรการควบคุมดังนี้

(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

หมวด 2
การบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management)

แนวทางปฏิบัติ

2.1 สร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information security awareness training) โดยจัดให้มีการฝึกอบรมให้แก่ผู้ให้งาน ประกอบด้วย

(1) การกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับ Information security awareness training ได้แก่ โครงการยกระดับความรู้ด้านดิจิทัลสู่ไทยแลนด์ 4.0 โครงการฝึกอบรมเพื่อความปลอดภัยในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน เป็นต้น

(2) ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงความเสี่ยงและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนกให้มีมาตรการเชิงป้องกันตามความเหมาะสม โดยกำหนดให้บุคลากรของ กปพ. เข้าร่วมการอบรม online ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA) ตามหลักสูตรที่เกี่ยวข้อง และผู้ดูแลระบบจะเป็นผู้อบรมให้ความรู้เกี่ยวกับความปลอดภัยในการใช้งานคอมพิวเตอร์และเครือข่าย ให้แก่ผู้ใช้งานในหน่วยงาน

2.2 กลุ่มงานบริหารสารสนเทศ เป็นผู้กำหนดบัญชีผู้ใช้งาน (User Account) โดยมีขั้นตอนสำหรับการลงทะเบียนผู้ใช้งาน (User registeration) และการลบออกจากทะเบียนของผู้ใช้งาน โดยต้องได้รับการพิจารณาอนุมัติอย่างเป็นลายลักษณ์อักษรจากผู้จัดการ กปพ. หรือผู้มีอำนาจลงนาม ครอบคลุมประเด็นดังต่อไปนี้

(1) ให้ผู้ใช้งานแจ้งรายละเอียดเพื่อดำเนินการตามขั้นตอน

(2) มีการระบุชื่อบัญชีผู้ใช้ (Username) แยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(3) การกำหนด Username จะกำหนดจากชื่อภาษาอังกฤษ ทั้งนี้ ต้องควบคุมไม่ให้เกิดความซ้ำซ้อนกัน

(4) การกำหนดสิทธิต้องมีความเหมาะสมกับผู้ใช้งานตามความจำเป็นของภารกิจ และสอดคล้องกับหน้าที่ความรับผิดชอบ

(5) การยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการลบออกจากทะเบียนของผู้ใช้งาน ให้แจ้งแก่ผู้บังคับบัญชีทันที เมื่อมีผู้ใช้งานเกษียณอายุราชการ โอน ย้าย เปลี่ยนแปลงสังกัด ลาออก เพื่อทำการเปลี่ยนแปลงสิทธิหรือถอดถอนสิทธิการเข้าถึงระบบสารสนเทศ

(6) มีการตรวจสอบและทบทวนบัญชีผู้ใช้งาน เป็นประจำทุกปี

2.3 มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ดังนี้

(1) ต้องจัดให้มีการควบคุมและจำกัดสิทธิในการใช้งานระบบตามความจำเป็นในการใช้งานเท่านั้น

(2) กำหนดสิทธิการใช้ระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) ระบบเครือข่ายไร้สาย (Wireless LAN) Internet และ E-mail เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบ รวมทั้งต้องทบทวนสิทธิดังกล่าวสม่ำเสมอ

(3) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ กล่าวคือ ผู้ใช้งานที่มีสิทธิสูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้สิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ และควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้นๆ โดยมีกำหนดระยะเวลาการใช้งาน และต้องระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากการดำรงตำแหน่ง

2.4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

(1) กำหนดให้รหัสผ่านมีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยอาจมีการผสมระหว่างตัวอักษรที่เป็นตัวพิมพ์เล็กและพิมพ์ใหญ่ ตัวเลข และตัวอักขระพิเศษหรือสัญลักษณ์

(2) ไม่ใช้รหัสส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(3) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

(4) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลกำหนดไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของผู้อื่น

(5) จะต้องเก็บรักษารหัสผ่านสำหรับการใช้งานเครื่องคอมพิวเตอร์และเครือข่ายที่ได้มาโดยถือว่าเป็นความลับเฉพาะบุคคล และต้องไม่เปิดเผยหรือกรพะทำการใดให้ผู้อื่นทราบรหัสผ่านดังกล่าว

(6) ผู้ใช้งานที่เป็นเจ้าของรหัสผ่านต้องใช้งานอย่างระมัดระวัง ไม่เปิดเผยรหัสผ่านให้ผู้อื่นทราบ และต้องรับผิดชอบในกรณีที่หน่วยงานได้รับความเสียหายซึ่งเกิดขึ้นจาก User Account ดังกล่าว

(7) ผู้ดูแลระบบ ต้องกำหนดรหัสผ่านแบบชั่วคราวที่ยากต่อการคาดเกา และกำหนดให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านผู้ใช้งานใหม่ได้ภายหลัง

(8) ควรเปลี่ยนรหัสผ่านทุกรอบระยะเวลา 6 เดือน หรือตามความเหมาะสม ซึ่งขึ้นอยู่กับความสำคัญของระบบงาน

2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access right)

(1) ต้องจัดให้มีการทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานเป็นประจำทุกปี

(2) ผู้ดูแลระบบ ต้องมีการสอบทานและระงับการใช้งาน User Account ที่ไม่ได้ใช้งานเกิน 1 ปี และต้องจัดส่งรายชื่อของผู้ใช้งานที่ถูกระงับไปยังผู้จัดการ กปพ. เพื่อยืนยันการยกเลิก User Account ดังกล่าว

หมวด 3
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

แนวทางปฏิบัติ

3.1 การใช้งานรหัสผ่าน (Password use)

(1) ผู้ใช้งานที่เป็นเจ้าของ User Account ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันเกิดขึ้นจากการใช้ User Account ของเครื่องคอมพิวเตอร์และเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

(2) ผู้ใช้งานต้องเก็บรักษา User Account ไว้เป็นความลับและห้ามเปิดเผยต่อผู้อื่น ห้ามถ่ายโอน จำหน่าย หรือแจกจ่ายให้แก่ผู้อื่นโดยมิได้รับอนุญาตจากผู้จัดการ กปพ.

(3) ผู้ใช้งานต้องเข้าระบบ (Liog in) โดยใช้ User Account ของตนเอง และต้องออกจากระบบ (Log out) ทุกครั้งที่ไม่ได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์หรือสิ้นสุดการใช้งาน

(4) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้อุปกรณ์คอมพิวเตอร์หรือระบบสารสนเทศของตนเอง โดยต้องใส่รหัสผ่านให้ถูกต้องก่อนใช้งานอุปกรณ์คอมพิวเตอร์

(5) ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์คอมพิวเตอร์ทุกเครื่องตั้งเวลาการพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย 10 นาที และมีการใช้รหัสในการเข้าถึงใหม่ทุกครั้ง

3.2 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy)

(1) ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต และห้ามใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใดๆ

(2) ผู้ใช้งานต้องไม่ทิ้งหรือปล่อยให้ทรัพย์สินที่มีความสำคัญของหน่วยงาน อาทิ เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย ที่สาธารณะ หรือที่ถูกพบเห็นได้ง่าย โดยต้องเก็บไว้ในตู้ที่มีการล็อคกุญแจเท่านั้น

(3) ผู้ใช้งานต้องจัดการทรัพย์สินไว้ในที่ที่กำหนดหลังจากการใช้งานเรียบร้อยแล้ว ในกรณีที่เป็นงานระบบสารสนเทศต้องทำการ Log out ทุกครั้ง

(4) ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับลงบันข้อมูลที่มีความสำคัญหรือชั้นความลับสูงในอุปกรณ์สำหรับจัดเก็บข้อมูลนั้นๆ ก่อนที่จะนำอุปกรณ์ไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำบานข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูลที่ปรากฏ

ตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูล

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลายสื่อและข้อมูล
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ใช้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

3.3 การนำการเข้ารหัสลับมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 และต้องใช้วิธีการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น โพรโทคอล TLS ในการรับส่งข้อมูลผ่านเครือข่าย และ AES สำหรับข้อมูลที่จัดเก็บ

หมวด 4
การควบคุมการใช้อินเทอร์เน็ต (Internet)

แนวทางปฏิบัติ

4.1 ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Firewall, Proxy, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นที่เหมาะสม และต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

4.2 ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเบราว์เซอร์ (Web browser) ผ่านเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาของ กปพ. ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

4.3 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

4.4 ไม่ใช้ระบบ Internet ของ กปพ. เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และ/หรือกระทำการใดที่ไม่เหมาะสม เช่น เข้าเว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อให้เกิดความเสียหายแก่หน่วยงาน

4.5 ห้ามเปิดเผยข้อมูลสำคัญอันเป็นความลับเกี่ยวกับงานหรือภารกิจของหน่วยงานที่ยังไม่มีประกาศอย่างเป็นทางการผ่านระบบ Internet

4.6 การดาวน์โหลดโปรแกรมการใช้งานจากระบบ Internet การอัปเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดสิขสิทธิ์

4.7 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

4.8 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้ายผู้อื่น อันทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน หรือการทำลายความสัมพันธ์กับบุคลากรหน่วยงานอื่นๆ

4.9 ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะลามกอนาจาร และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านระบบ Internet ของ กปพ.

4.10 หลังจากใช้ระบบ Internet ของ กปพ. เสร็จแล้ว ให้ปิด Web browser และ Log out จากระบบเพื่อป้องกันไม่ให้บุคคลอื่นเข้าใช้งานได้

4.11 ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้านการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

หมวด 5
การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-mail)

แนวทางปฏิบัติ

5.1 ในการลงทะเบียนบัญชีผู้ใช้งาน E-mail ต้องทำการกรอกข้อมูล พร้อมกับยื่นคำขอแก่ กปพ. ก่อนขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์

5.2 ไม่บันทึกหรือเก็บรหัสผ่านไว้ในคอมพิวเตอร์ และควรเปลี่ยนรหัสผ่านทุก 6 เดือน

5.3 หลังจากการใช้งานระบบ E-mail เสร็จสิ้น ต้อง Log out จากระบบทุกครั้ง

5.4 ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ตามที่ กปพ. กำหนดเท่านั้น

5.5 ห้ามใช้ E-Mail Address ที่ กปพ. กำหนดให้ ลงทะเบียนตามเว็บไซต์ที่ไม่เกี่ยวข้องกับงานหลักของหน่วยงาน

5.6 ห้ามเข้าถึง E-Mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต

5.7 ห้ามปลอมแปลง รับหรือส่ง E-Mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต

5.8 ห้ามส่ง E-Mail ที่มีลักษณะดังต่อไปนี้

(1) จดหมายขยะ (Spam Mail)

(2) จดหมายลูกโซ่ (Chain Letter)

(3) จดหมายที่ละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

(4) จดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

5.9 ต้องระบุชื่อเรื่อง (Subject) และชื่อผู้ส่งใน E-Mail ทุกฉบับที่ดำเนินการส่งออก

5.10 การส่งข้อมูลที่เป็นความลับของ กปพ. ไม่ควรระบุความสำคัญของข้อมูลลงใน Subject เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสลับข้อมูล E-mail ที่หน่วยงานกำหนดไว้ ให้ใช้ความระมัดระวังในการระบุ E-mail Address ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

5.11 ไม่ใช้ E-mail Address ของผู้อื่น เพื่ออ่าน หรือรับ-ส่งข้อความ ยกเว้นได้รบการยินยอมจากเจ้าของผู้ใช้งาน และให้ถือว่าเจ้าของ E-mail Address เป็นผู้รับผิดชอบต่อการใช้งานนั้นๆ

5.12 ต้องใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับ E-Mail เท่าที่มีความจำเป็นต้องรับรู้เท่านั้น

5.13 ผู้ใช้งานต้องไม่เปิดหรือส่งต่อ E-mail หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

5.14 ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจาก E-mail ก่อนการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe เป็นต้น

5.15 ต้องสำรองข้อมูล E-Mail Address ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าหน่วยงานจะทำการสำรองข้อมูล E-mail ไว้ให้ แต่เป็นเพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้น E-mail ที่มีความจำเป็น ผู้ใช้งานต้องเก็บสำรองด้วยตนเอง)

5.16 ผู้ใช้งานห้ามใช้ข้อความที่ไม่สุภาพ หรือรับ-ส่ง E-mail ที่ไม่เหมาะสม ข้อมูลอันอาจก่อให้เกิดความเสียหายแก่หน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน

5.17 ผู้ใช้งานต้องตรวจสอบกล่องข้อความของ E-mail ทุกวัน และควรจัดเก็บแฟ้มข้อมูลและ E-mail ของตนเองให้เหลือจำนวนน้อยที่สุด รวมถึงลบ E-mail ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ของระบบสารสนเทศดังกล่าว

หมวด 6
การใช้งานคอมพิวเตอร์แบบพกพา (Notebook)

แนวทางปฏิบัติ

6.1 แนวทางปฏิบัติการใช้งานทั่วไป

(1) คอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน ถือเป็นทรัพย์สินของหน่วยงาน เพื่อใช้ในงานของหน่วยงานเท่านั้น

(2) โปรแกรมที่ได้ถูกติดตั้งบนคอมพิวเตอร์แบบพกพาของ กปพ. ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(3) ไม่ดัดแปลง แก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์แบบพกพาของ กปพ. และรักษาให้คงอยู่ในสภาพเดิม

(4) ในกรณีที่ต้องการเคลื่อนย้ายคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าเฉพาะเครื่องเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

(5) หลีกเลี่ยงการใช้ของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือก่อให้เกิดความเสียหายแก่ทรัพย์สินของ กปพ.

(6) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(7) การเคลื่อนย้ายคอมพิวเตอร์แบบพกพาขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามเคลื่อนย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

6.2 ความปลอดภัยทางด้านกายภาพ

(1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(2) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น หรือมีฝุ่นละอองสูง และต้องระวังการตกกระทบของตัวเครื่อง

6.3 การควบคุมการเข้าถึงระบบปฏิบัติการ

(1) ผู้ใช้งานต้องกำหนด Username และ Password ในการเข้าใช้งานระบบปฏิบัติการของเครื่อง

(2) ผู้ใช้งานต้องกำหนด Password ให้มีคุณภาพ อย่างน้อยให้สอดคล้องตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

(3) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 15 นาที เพื่อให้เครื่องทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นต้องมีการใช้ใส่รหัสผ่านเพื่อเข้าใช้งาน

(4) ผู้ใช้งานต้องทำการ Log out จากระบบทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

6.4 การใช้งานรหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสารหัวข้อ “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

6.5 การสำรองข้อมูลและการกู้คืน

(1) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่อง โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูลของหน่วยงาน

(2) ผู้ใช้งานต้องจัดเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

(3) แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้ ต้องมีการทดสอบการกู้คืนอย่างสม่ำเสมอ

(4) แผ่นสื่อสำรองข้อมูลที่ไม่ได้ใช้งานแล้ว ต้องทำลายให้ไม่สามารถนำไปใช้งานอีกได้

(5) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรเป็นข้อมูลสำคัญของหน่วยงาน เนื่องจากหากเกิดการเสียหายขึ้นกับ Hard Disk ก็จะไม่เกิดผลกระทบต่อการดำเนินการของหน่วยงาน

ผู้รับผิดชอบการจัดทำแผนและทบทวนแผน

คณะทำงานเพื่อช่วยปฏิบัติงานของกองทุนบริหารเงินกู้
เพื่อการปรับโครงสร้างหนี้สาธารณะและพัฒนาตลาดตราสารหนี้ในประเทศ (คณะทำงานฯ กปพ.)