ประกาศสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศ พ.ศ. ๒๕๖๒

ศูนย์เทคโนโลยีสารสนเทศ

๕ มีนาคม ๒๕๖๒

ประกาศสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ดังนั้น สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจจึงกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ครอบคลุมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

(๑) “สำนักงาน” หมายความว่า สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.)

(๒) “ผู้บริหาร” หมายความว่า ผู้อำนวยการ ที่ปรึกษา รองผู้อำนวยการ ผู้อำนวยการสำนัก ผู้อำนวยการกอง เลขานุการกรม ผู้เชี่ยวชาญ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และผู้อำนวยการกลุ่ม

(๓) “ผู้บริหารระดับสูงสุด” หมายความว่า ผู้อำนวยการสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ

(๔) “ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ” หมายความว่า ที่ปรึกษา รองผู้อำนวยการ หรือผู้ที่ได้รับมอบหมายให้เป็นผู้ดำรงตำแหน่งผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศประจำ สคร. (Chief Information Officer : CIO)

(๕) “ผู้ปฏิบัติงาน” หมายความว่า บุคลากร สคร. ซึ่งเป็นข้าราชการตั้งแต่ระดับชำนาญการพิเศษลงมา ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราว และบุคคลภายนอก

/(๖) “นโยบาย”...

(๖) “นโยบาย” หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ซึ่ง สคร. ได้กำหนดไว้ เพื่อเป็นทิศทางให้ผู้ดูแลระบบ (Administrator) ผู้ใช้งาน (User) และบุคคลภายนอกได้ถือปฏิบัติ

(๗) “แนวปฏิบัติ” หมายความว่า แนวทางหรือข้อกำหนดให้ผู้ใช้งาน (User) และบุคคลภายนอกได้ถือปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๘) “ผู้ใช้งาน” (User) หมายความว่า บุคคลที่ได้รับอนุญาตให้เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยมีบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตน (Authentication)

(๙) “บัญชีผู้ใช้งาน” (Username) หมายความว่า ชุดของตัวอักษรและอักขระที่ถูกกำหนดขึ้นเพื่อใช้ในการแสดงตัวตน และใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตน (Authentication) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๑๐) “รหัสผ่าน” (Password) หมายความว่า ชุดของตัวอักษร ตัวเลข และอักขระพิเศษ อย่างน้อย ๘ ตัวขึ้นไป และยากต่อการคาดเดา โดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตน (Authentication) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๑๑) “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบคอมพิวเตอร์และระบบสารสนเทศ

(๑๒) “สินทรัพย์” (Asset) หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งใดก็ตามที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของ สคร.

(๑๓) “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน (User) เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดแนวปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

(๑๔) “ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ รวมทั้งคุณสมบัติอื่นๆ ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non - Repudiation) และความน่าเชื่อถือ (Reliability)

/(๑๕) “เหตุการณ์”...

(๑๕) “เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information Security Event) หมายความว่า การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๖) “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบคอมพิวเตอร์และระบบสารสนเทศถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๑๗) “ผู้ดูแลระบบ” (Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากเจ้าของระบบ (System Owner) หรือจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ

(๑๘) “เจ้าของระบบ” (System Owner) หมายความว่า สำนัก/กอง/ศูนย์/กลุ่มที่เป็นผู้รับผิดชอบหลักในการพัฒนาระบบคอมพิวเตอร์และระบบสารสนเทศ โดยมีวัตถุประสงค์เพื่อสนับสนุนภารกิจการปฏิบัติงานของหน่วยงานให้เกิดประสิทธิภาพต่อ สคร. ในภาพรวม หรือตามที่ผู้อำนวยการ สคร. มอบหมาย และมีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน (User)

(๑๙) “ระบบคอมพิวเตอร์” หมายถึง ระบบคอมพิวเตอร์ลูกข่ายแบบเสมือน (Virtualization System) ที่ติดตั้งบนอุปกรณ์ในการประมวลผลข้อมูล (Process Device) โดยเข้าถึงด้วยเทคโนโลยีแบบคลาวด์คอมพิวติ้ง (Cloud Computing) และระบบปฏิบัติการ (Operating System) ที่ติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) พร้อมด้วยโปรแกรมประยุกต์ (Application Software)

(๒๐) “ระบบสารสนเทศ” หมายถึง ระบบงานคอมพิวเตอร์ เช่น เว็บพอร์ทัล (Portal Web) จดหมายอิเล็กทรอนิกส์ (E - Mail) และระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น หรืออุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับการพัฒนา หรือติดตั้ง หรือการนำมาประยุกต์ใช้ เพื่อสนับสนุนการปฏิบัติงานของ สคร.

(๒๑) “ข้อมูลสารสนเทศ” หมายความว่า ข้อมูล (Data) หรือสารสนเทศ (Information) ที่อยู่ในรูปของเอกสารอิเล็กทรอนิกส์ เช่น แฟ้มข้อมูล (File) ฐานข้อมูล (Database) และเอกสารที่มีการแปลงให้อยู่ในรูปแบบอิเล็กทรอนิกส์ (E - Document)

(๒๒) “พื้นที่ปฏิบัติงานทั่วไป” (General Working Area) หมายความว่า พื้นที่สำหรับการปฏิบัติงานภายใน สคร. ซึ่งได้รับการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์ลูกข่ายเสมือน เครื่องคอมพิวเตอร์พกพา อุปกรณ์ต่อพ่วง และเครือข่ายแบบไร้สาย (Wireless LAN)

(๒๓) “ห้องศูนย์ข้อมูล” (Data Center) หมายความว่า พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะเพื่อติดตั้งอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ระบบเครือข่ายคอมพิวเตอร์ ระบบจัดเก็บข้อมูลระบบรักษาความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศ และระบบป้องกันอัคคีภัย ซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์และระบบสารสนเทศแก่ผู้ใช้งาน (User)

/ข้อ ๔...

ข้อ ๔ สคร. ได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นลายลักษณ์อักษร พร้อมทั้งได้กำหนดให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบ กำกับดูแล และติดตามให้ผู้ใช้งาน (User) ปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าวไว้อย่างชัดเจน ดังนี้

(๔.๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

(๔.๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๔.๓) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

(๔.๔) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๔.๕) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๔.๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

(๔.๗) การจัดทำระบบสำรองของระบบสารสนเทศ

(๔.๘) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

ข้อ ๕ สคร. ได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศทางเว็บไซต์ของ สคร. ระบบเครือข่ายภายใน (Intranet) และหนังสือเวียนภายใน ให้ผู้ใช้งาน (User) และบุคคลภายนอกทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามได้อย่างถูกต้อง

ข้อ ๖ สคร. ทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นปัจจุบันอยู่เสมอ โดยอย่างน้อยให้ทบทวนปรับปรุงเมื่อครบกำหนด ๒ ปี และนำเสนอคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เพื่อให้ความเห็นชอบ เพื่อนำเสนอผู้อำนวยการ สคร. ก่อนประกาศใช้ต่อไป

ข้อ ๗ สคร. กำหนดให้ผู้บริหารระดับสูงสุด (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่ สคร. หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้

ประกาศ ณ วันที่ ๕ มีนาคม พ.ศ. ๒๕๖๒

(นายประภาศ คงเอียด)

ผู้อำนวยการสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ

เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ พ.ศ. ๒๕๖๒

หมวด ๑

การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

(Business Requirements for Access Control)

วัตถุประสงค์

เพื่อให้บุคลากร สคร. และบุคคลภายนอก ให้มีความรู้ ความเข้าใจ และสามารถปฏิบัติตามแนวปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) พร้อมทั้งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ

นโยบาย

บุคลากร สคร. และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้

๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) ต้องสอดคล้องและเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ

๑.๒ ศูนย์เทคโนโลยีสารสนเทศมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน (User) สำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุมการใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๓ เจ้าของระบบ (System Owner) มีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน (User)

๑.๔ ผู้ดูแลระบบ (Administrator) มีหน้าที่กำหนดสิทธิให้แก่ผู้ใช้งาน (User) ตามที่เจ้าของระบบ (System Owner) อนุมัติ

๑.๕ ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

/๑.๖ เมื่อมี...

๑.๖ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ทั้งทางกายภาพ (Physical Access) และจากระยะไกล (Remote Access) บุคคลภายนอกดังกล่าวต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากศูนย์เทคโนโลยีสารสนเทศ และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหายบุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

๑.๗ การเข้าถึงห้องศูนย์ข้อมูล (Data Center) เพื่อปฏิบัติงานที่เกี่ยวข้องกับอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ให้ดำเนินการ ดังนี้

๑.๗.๑ ศูนย์เทคโนโลยีสารสนเทศต้องกำหนดหลักเกณฑ์สำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center)

๑.๗.๒ การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจากศูนย์เทคโนโลยีสารสนเทศก่อนเริ่มดำเนินการทุกครั้งก่อนเริ่มดำเนินการทุกครั้ง

๑.๗.๓ ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

๑.๗.๔ ผู้ใช้งาน (User) หรือบุคคลภายนอก ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน โดยมีผู้ดูแลระบบ (Administrator) ควบคุมการปฏิบัติงานของผู้ใช้งาน (User) หรือบุคคลภายนอกตลอดเวลา และต้องไม่นำอาหาร หรือเครื่องดื่มเข้าไปในห้องศูนย์ข้อมูล (Data Center) และห้ามสูบบุหรี่ในห้องศูนย์ข้อมูล (Data Center)

๒. การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนด ดังนี้

๒.๑ สิทธิของผู้ใช้งาน (User) ประกอบด้วย

๒.๑.๑ อ่านอย่างเดียว

๒.๒.๒ สร้างข้อมูล

๒.๒.๓ แก้ไขข้อมูล

๒.๒.๔ ลบข้อมูล

๒.๒ สิทธิผู้ดูแลระบบ (Administrator) กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การกำหนดประเภทของข้อมูล ลำดับความสำคัญ ลำดับชั้นความลับ รวมถึงระดับชั้นการเข้าถึง เวลาที่เข้าถึง และช่องทางการเข้าถึง ดังนี้

๓.๑ ประเภทของข้อมูล แบ่งเป็น ๓ ประเภท ดังนี้

๓.๑.๑ ข้อมูลสารสนเทศสำหรับการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร และข้อมูลงบประมาณรายจ่าย

๓.๑.๒ ข้อมูลสารสนเทศสำหรับการสนับสนุนการปฏิบัติงาน ได้แก่ ข้อมูลระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ - รัฐวิสาหกิจ (GFMIS - SOE)

/๓.๑.๓ ข้อมูล...

๓.๑.๓ ข้อมูลสารสนเทศสำหรับการเผยแพร่แก่ประชาชนทั่วไปและผู้ที่สนใจ ได้แก่ ข้อมูลในเว็บไซต์ของ สคร.

๓.๒ ลำดับความสำคัญของข้อมูล แบ่งเป็น ๓ ระดับ ดังนี้

๓.๒.๑ สำคัญมากที่สุด

๓.๒.๒ สำคัญมาก

๓.๓.๓ ปกติ

๓.๓ ลำดับชั้นความลับของข้อมูล แบ่งเป็น ๔ ระดับ ดังนี้

๓.๓.๑ ลับที่สุด - ความลับที่มีความสำคัญที่สุด เกี่ยวกับขาวสาร วัตถุหรือบุคคล ซึ่งถาหากความลับดังกลาวทั้งหมดหรือเพียงบางสวนรั่วไหลไปถึงบุคคลผูไมมีหนาที่ไดทราบจะทำใหเกิดความเสียหายหรือเปนภยันตรายตอความมั่นคง ความปลอดภัย หรือความสงบเรียบรอยของประเทศชาติหรือพันธมิตร หรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้องอย่างร้ายแรงที่สุด

๓.๓.๒ ลับมาก - ความลับที่มีความสำคัญมาก เกี่ยวกับขาวสาร วัตถุหรือบุคคล ซึ่งถาหากความลับดังกลาวทั้งหมดหรือเพียงบางสวนรั่วไหลไปถึงบุคคลที่ไมมีหนาที่ไดทราบจะทำใหเกิดความเสียหายหรือเปนภยันตรายตอความมั่นคง ความปลอดภัยของประเทศชาติหรือพันธมิตร หรือความสงบเรียบรอยภายในราชอาณาจักร หรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้องไดอยางรายแรง

๓.๓.๓ ลับ - ความลับที่มีความสำคัญเกี่ยวกับ ขาวสาร วัตถุ หรือบุคคล ซึ่งถาหากความลับดังกลาวทั้งหมด หรือเพียงบางสวนรั่วไหลไปถึงบุคคลผูไมมีหนาที่ไดทราบจะทำใหเกิดความเสียหายต่อราชการหรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้องได

๓.๓.๔ ปกปิด - ความลับซึ่งไมพึงเปดเผยใหผูไมมีหนาที่ไดทราบ โดยสงวนไวใหทราบเฉพาะบุคคลที่มีหนาที่ตองทราบเพื่อประโยชนในการปฏิบัติภารกิจองค์กรเทานั้น

๓.๔ ระดับชั้นการเข้าถึง แบ่งเป็น ๓ ระดับ ดังนี้

๓.๔.๑ กลุ่มผู้บริหาร

๓.๔.๒ กลุ่มผู้ปฏิบัติงาน

๓.๔.๓ กลุ่มประชาชนทั่วไปและผู้ที่สนใจ

๓.๕ เวลาที่เข้าถึง

ระบบคอมพิวเตอร์และระบบสารสนเทศสามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง ๗ วัน

๓.๖ ช่องทางการเข้าถึง

ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศได้ ๒ ช่องทาง ดังนี้

๓.๖.๑ ระบบเครือข่ายภายใน (Intranet)

๓.๖.๒ ระบบเครือข่ายภายนอก (Internet)

/๔. การใช้งาน...

๔. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) แบ่งเป็น ๒ ส่วน ดังนี้

๔.๑ การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้สอดคล้องตามภารกิจ

๔.๑.๑ เจ้าของระบบ (System Owner) อนุมัติสิทธิให้ผู้ใช้งาน (User) ตามภารกิจเพื่อให้สามารถเข้าถึงข้อมูลในระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะในส่วนที่ได้รับมอบหมายตามความจำเป็นในการใช้งาน

๔.๑.๒ ผู้ดูแลระบบ (Administrator) กำหนดสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน (User) ตามที่เจ้าของระบบ (System Owner) อนุมัติ

๔.๒ การปรับปรุงการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศให้สอดคล้องตามภารกิจและการรักษาความมั่นคงปลอดภัย

ผู้ดูแลระบบ (Administrator) ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้างเพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัยตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

/หมวด ๒...

หมวด ๒

การบริหารจัดการการเข้าถึงของผู้ใช้งาน

(User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งาน (User) ที่ได้รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศ และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนบุคลากรใหม่ (User Registration) เพื่อรับสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

๒. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อบุคลากรไม่ได้ปฏิบัติงานที่ สคร. แล้ว

๓. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการควบคุม จำกัด และเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๔. กำหนดให้มีการบริหารจัดการรหัสผ่าน (User Password Management) อย่างรัดกุม โดยเริ่มตั้งแต่กระบวนการสร้างรหัสผ่านชั่วคราว (Temporary Password) ตามสิทธิที่ได้รับของผู้ใช้งาน (User) การส่งมอบรหัสผ่านชั่วคราว (Temporary Password) การเปลี่ยนรหัสผ่าน เงื่อนไขการเปลี่ยนรหัสผ่าน และการกำหนดรหัสผ่านใหม่ในกรณีลืมรหัสผ่าน

๕. กำหนดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง

๖. กำหนดให้มีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักและความเข้าใจเรื่องภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

๗. กำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

แนวปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน (User Registration) ให้ดำเนินการ ดังนี้

๑.๑ ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคลากร สคร. และบุคคลภายนอก อย่างน้อยประกอบด้วยชื่อ นามสกุล ตำแหน่งสังกัด หมายเลขโทรศัพท์ และจดหมายอิเล็กทรอนิกส์ (E - Mail) ที่ใช้งานในปัจจุบันเพื่อเป็นจดหมายอิเล็กทรอนิกส์ (E - Mail) สำรองของผู้ขอใช้งาน

/๑.๒ การขออนุญาต...

๑.๒ การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

๑.๒.๑ กรณีบุคลากร สคร.

(๑) ให้บุคลากรใหม่กรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคลากรของ สคร. ในวันรายงานตัว

(๒) ให้สำนักงานเลขานุการกรมส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคลากรของ สคร. ให้ศูนย์เทคโนโลยีสารสนเทศ เพื่อสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านชั่วคราว (Temporary Password)

(๓) ให้เจ้าของระบบ (System Owner) อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคลากรใหม่

(๔) ให้ผู้ดูแลระบบ (Administrator) กำหนดสิทธิให้บุคลากรใหม่ ตามที่เจ้าของระบบ (System Owner) อนุมัติ พร้อมทั้งแจ้งให้บุคลากรใหม่ได้รับทราบ

๑.๒.๒ กรณีบุคคลภายนอก

(๑) ให้สำนัก/กอง/ศูนย์/กลุ่ม แจ้งความประสงค์พร้อมเหตุผลในการให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคคลภายนอก

(๒) ให้ศูนย์เทคโนโลยีสารสนเทศพิจารณาเหตุผลดังกล่าวก่อนดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านชั่วคราว (Temporary Password)

(๓) ให้เจ้าของระบบ (System Owner) อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคคลภายนอก

(๔) ให้ผู้ดูแลระบบ (Administrator) กำหนดสิทธิให้ผู้ใช้งาน (User) ตามที่เจ้าของระบบ (System Owner) อนุมัติ พร้อมทั้งแจ้งให้บุคคลภายนอกได้รับทราบ

๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และการกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้ใช้ชื่อภาษาอังกฤษตามบัตรประจำตัวประชาชนตามด้วยเครื่องหมาย “_” และอักษรนามสกุลตัวแรก

๑.๓.๒ การกำหนดรหัสผ่าน (Password) ชุดของตัวอักษร ตัวเลข และอักขระพิเศษอย่างน้อย ๘ ตัวขึ้นไป และยากต่อการคาดเดา โดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตน (Authentication) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๓.๓ ให้ผู้ดูแลระบบ (Administrator) แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่านชั่วคราว (Temporary Password) ให้ผู้ใช้งาน (User) ทราบโดยตรง

๑.๓.๔ เมื่อบุคลากร สคร. มีการเปลี่ยนชื่อหรือนามสกุลให้แจ้งศูนย์เทคโนโลยีสารสนเทศเพื่อเปลี่ยนบัญชีผู้ใช้งาน (Username)

/๑.๔ บัญชี...

๑.๔ บัญชีผู้ใช้งาน (Username) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศได้จนกว่าบุคลากร สคร. หรือบุคคลภายนอกสิ้นสุดการปฏิบัติหน้าที่ใน สคร. และศูนย์เทคโนโลยีสารสนเทศดำเนินการยกเลิกสิทธิการใช้งาน

๒. การยกเลิกสิทธิการใช้งานของบุคลากร สคร. หรือบุคคลภายนอกให้ดำเนินการ ดังนี้

๒.๑ กรณีบุคลากร สคร.

๒.๑.๑ ให้สำนักงานเลขานุการกรมแจ้งศูนย์เทคโนโลยีสารสนเทศ เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร สคร. เมื่อมีการลาออก ให้โอน หรือสิ้นสุดการจ้าง

๒.๑.๒ ศูนย์เทคโนโลยีสารสนเทศจะปิดบัญชีผู้ใช้งาน (Username) ชั่วคราว เป็นเวลา ๙๐ วัน หากบุคลากร สคร. ที่มีความประสงค์จะใช้ข้อมูลในบัญชีผู้ใช้งาน (Username) ดังกล่าว ให้แจ้งความประสงค์พร้อมเหตุผลต่อศูนย์เทคโนโลยีสารสนเทศ เพื่อขอเปิดใช้งานบัญชีผู้ใช้งาน (Username) ดังกล่าวชั่วคราว พร้อมทั้งกำหนดรหัสผ่านชั่วคราว (Temporary Password) ทั้งนี้ เมื่อครบกำหนด ๙๐ วัน นับจากมีคำสั่งเป็นลายลักษณ์อักษร ศูนย์เทคโนโลยีสารสนเทศจะยกเลิกสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศและลบข้อมูลสารสนเทศของบัญชีผู้ใช้งาน (Username) ดังกล่าว เป็นการถาวร

๒.๒ กรณีบุคคลภายนอก

๒.๒.๑ ให้สำนัก/กอง/ศูนย์/กลุ่ม แจ้งความประสงค์ยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศต่อศูนย์เทคโนโลยีสารสนเทศทันทีที่หมดความจำเป็น

๒.๒.๒ ศูนย์เทคโนโลยีสารสนเทศจะยกเลิกสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ และลบข้อมูลสารสนเทศเป็นการถาวร

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้ใช้งาน (User) ให้ดำเนินการ ดังนี้

๓.๑ ผู้ดูแลระบบ (Administrator) ตรวจสอบสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคลากร สคร. หรือบุคคลภายนอก ให้สอดคล้องกับคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ หรือเหตุผลความจำเป็นของสำนัก/กอง/ศูนย์/กลุ่ม ที่ได้แจ้งความประสงค์ในการให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ แล้วแต่กรณี

๓.๒ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้สำนักงานเลขานุการกรมแจ้งศูนย์เทคโนโลยีสารสนเทศ เพื่อเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว

๓.๓ ในกรณีที่ผู้ใช้งาน (User) ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศที่สูงกว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อศูนย์เทคโนโลยีสารสนเทศ ทั้งนี้ ต้องมีการกำหนดระยะเวลาการใช้งาน และยกเลิกสิทธิการใช้งานทันทีที่หมดความจำเป็น

/๔. การบริหาร...

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๔.๑ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่านชั่วคราว (Temporary Password) ทันทีที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในครั้งแรก

๔.๒ การเปลี่ยนรหัสผ่านใหม่ (Password) ให้ดำเนินการผ่านระบบบริหารจัดการรหัสผ่าน (Password Management System) โดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เดิม

๔.๓ ในกรณีที่ผู้ใช้งาน (User) ลืมรหัสผ่าน (Password) ให้ขอรับรหัสผ่านใหม่ผ่านระบบบริหารจัดการรหัสผ่าน (Password Management System) โดยเลือกใช้วิธีการตอบคำถาม หรือเลือกรับ Link / URL สำหรับการตั้งรหัสผ่านใหม่ผ่านระบบจดหมายอิเล็กทรอนิกส์ (E - Mail) สำรองของผู้ใช้งาน (User)

๔.๔ กรณีผู้ใช้งาน (User) ไม่สามารถเปลี่ยนรหัสผ่านใหม่ได้ ให้แจ้งศูนย์เทคโนโลยีสารสนเทศเพื่อขอรับรหัสผ่านชั่วคราว (Temporary Password)

๔.๕ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๙ เดือน และรหัสผ่าน (Password) ใหม่ ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

๕. ผู้ดูแลระบบ (Administrator) ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง

๖. ให้ศูนย์เทคโนโลยีสารสนเทศจัดฝึกอบรมให้แก่ผู้ใช้งาน (User) เพื่อให้มีความรู้ ความเข้าใจ และเกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ อย่างน้อยปีละ ๑ ครั้ง หรือจัดให้ผู้ใช้งาน (User) เข้าร่วมการฝึกอบรมที่หน่วยงานอื่นจัดขึ้น

๗. ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศตามความเหมาะสม ได้แก่ การไม่เปิดจดหมายอิเล็กทรอนิกส์ (E - Mail) ที่ไม่ระบุที่มาหรือชื่อผู้ส่งที่น่าสงสัย โดยให้ลบจดหมายอิเล็กทรอนิกส์ (E - Mail) ทันที หรือการแจ้งเตือนผู้ใช้งาน (User) เมื่อมีไวรัสแพร่ระบาด

/หมวด ๓...

หมวด ๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

๑. กำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)

๒. กำหนดแนวปฏิบัติในการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) ดูแล

๓. กำหนดแนวปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ได้แก่ เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศ เพื่อไม่ให้สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งาน (User) ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔. กำหนดให้ผู้ใช้งาน (User) อาจนำการเข้ารหัสข้อมูล (Encryption) มาใช้กับการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับของ สคร. โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

แนวปฏิบัติ

๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้

๑.๑ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่านชั่วคราว (Temporary Password) ทันทีที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในครั้งแรก

๑.๒ ผู้ใช้งาน (User) ต้องกำหนดรหัสผ่าน (Password) ตามหมวด ๒ ข้อ ๑.๓ (๒)

๑.๓ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๙ เดือน และรหัสผ่าน (Password) ใหม่ ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

๑.๔ ผู้ใช้งาน (User) ต้องไม่ใช้รหัสผ่าน (Password) ร่วมกับบุคคลอื่น และไม่ควรให้ระบบคอมพิวเตอร์หรือระบบสารสนเทศจำรหัสผ่าน (Password) ในการเข้าใช้งานโดยอัตโนมัติ

/๑.๕ ผู้ใช้งาน...

๑.๕ ผู้ใช้งาน (User) ต้องไม่เปิดเผยรหัสผ่าน (Password) สำหรับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเก็บเป็นความลับเสมือนเป็นสมบัติส่วนตัว ห้ามจดหรือเขียนรหัสผ่าน (Password) ที่ใช้งานไว้ในที่เปิดเผย

๑.๖ หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็นในการเข้าถึง หลังจากดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

๑.๗ หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของบัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดในเอกสารฉบับนี้แล้ว

๑.๘ ผู้ดูแลระบบ (Administrator) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๓ เดือน และรหัสผ่าน (Password) ใหม่ ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

๒. การป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) ผู้ใช้งาน (User) ต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๓.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ในการประมวลผลข้อมูล (Process Device) มีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานของ สคร. เท่านั้น

๓.๒ ระบบคอมพิวเตอร์และระบบสารสนเทศ เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์ประมวลผลข้อมูล ต้องถูกติดตั้งด้วยซอฟต์แวร์ที่มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมายเท่านั้น

๓.๓ ระบบคอมพิวเตอร์และระบบสารสนเทศ ต้องได้รับการป้องกันด้วยรหัสผ่านของระบบพิสูจน์ตัวตนจากส่วนกลาง (Active Directory : AD) ทุกครั้งเมื่อเข้าใช้งาน และออกจากระบบ (Log out) ทันทีทุกครั้งเมื่อเลิกใช้งาน

๓.๔ ผู้ใช้งาน (User) ต้องรับผิดชอบต่อสินทรัพย์ (Asset) ของ สคร. และให้ใช้งานด้วยความระมัดระวังเสมือนเป็นทรัพย์สินของตน

๓.๕ ผู้ใช้งาน (User) ต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใดๆ ที่เครื่องคอมพิวเตอร์ลูกข่ายหรือเครื่องคอมพิวเตอร์พกพา หรือระบบคอมพิวเตอร์หรือระบบสารสนเทศ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลต่อศูนย์เทคโนโลยีสารสนเทศ

๓.๖ ผู้ใช้งาน (User) ต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา หรือการ์ดความจำในโทรศัพท์มือถือ เพื่อป้องกันการรั่วไหลของข้อมูล

๓.๗ บุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานระบบคอมพิวเตอร์และระบบสารสนเทศ ต้องขออนุมัติศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร ก่อนเข้าปฏิบัติงาน และต้องได้รับการอนุมัติจากศูนย์เทคโนโลยีสารสนเทศก่อนเริ่มปฏิบัติงาน

/๓.๘ การทำลาย...

๓.๘ การทำลายอุปกรณ์บันทึกข้อมูลหรือการนำอุปกรณ์บันทึกข้อมูลกลับมาใช้งานใหม่ ให้ดำเนินการ ดังนี้

๓.๘.๑ การทำลายอุปกรณ์บันทึกข้อมูล ได้แก่ Flash Drive CD/DVD ฮาร์ดดิสก์ และเทป เป็นต้น ให้ใช้วิธีการทุบ หรือบดให้เสียหาย หรือเผาทำลาย

๓.๘.๒ การนำอุปกรณ์บันทึกข้อมูลไปใช้งานใหม่ ให้ฟอร์แมต (Format) อุปกรณ์บันทึกข้อมูลนั้น โดยใช้วิธีการฟอร์แมต (Format) ตามมาตรฐานสากล หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

๔. ผู้ใช้งาน (User) อาจนำการเข้ารหัสข้อมูล (Encryption) ที่ได้รับรองมาตรฐานสากลหรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด ได้แก่ HTTPS, SSL, LDAPS, VPN, XML และ ebXML มาใช้ในกรณีมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับของ สคร. โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

/หมวด ๔...

หมวด ๔

การควบคุมการเข้าถึงเครือข่าย

(Network Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๒. กำหนดแนวปฏิบัติในการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่าย ระบบคอมพิวเตอร์และระบบสารสนเทศของ สคร. ได้

๓. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดยต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๔. กำหนดแนวปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) โดยต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕. กำหนดแนวปฏิบัติในการแบ่งแยกเครือข่าย (Segregation in Networks) โดยต้องแบ่งแยกเครือข่ายตามกลุ่มของการให้บริการสารสนเทศ กลุ่มการใช้งาน กลุ่มของอุปกรณ์สารสนเทศ และกลุ่มประเภทของเครือข่าย

๖. กำหนดแนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

๗. กำหนดแนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศและการส่งข้อมูลสารสนเทศสอดคล้องกับแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

/แนวปฏิบัติ...

แนวปฏิบัติ

๑. การเข้าถึงเครือข่ายของผู้ใช้งาน (User)

๑.๑ การใช้งานระบบเครือข่ายภายนอก (Internet) ให้ดำเนินการ ดังนี้

๑.๑.๑ กำหนดให้ใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองสำหรับเข้าใช้งานระบบเครือข่ายภายนอก (Internet)

๑.๑.๒ ห้ามใช้งานระบบเครือข่ายภายนอก (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) สูงที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ ได้แก่ Youtube หนังออนไลน์ หรือรายการบันเทิงต่างๆ ในเวลาราชการ

๑.๑.๓ ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์ เสื่อมเสีย

๑.๑.๔ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของ สคร. ผ่านระบบเครือข่ายภายนอก (Internet) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๕ ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม โดยเคร่งครัด ได้แก่ ห้ามเผยแพร่ภาพหรือข้อมูลใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือที่มีลักษณะลามกอนาจาร และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านระบบเครือข่ายภายนอก (Internet) ห้ามเผยแพร่ภาพของผู้อื่นที่เกิดจากการสร้างขึ้น ตัดต่อ ต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่จะทำให้ผู้นั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑.๑.๖ ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่างๆ จากระบบเครือข่ายภายนอก (Internet) เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุกโจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๑.๗ หลังจากใช้งานระบบเครือข่ายภายนอก (Internet) แล้วให้ปิดเว็บบราวเซอร์ (Web Browser) เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

๑.๒ การใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ให้ดำเนินการ ดังนี้

๑.๒.๑ ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม โดยเคร่งครัด และห้ามใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ในทางที่ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศีลธรรม

๑.๒.๒ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจด้วยการใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ที่ส่งโดยโดเมนเนม (Domain Name) ของ สคร. (@sepo.go.th)

/๑.๒.๓ ต้องตรวจ...

๑.๒.๓ ต้องตรวจสอบชื่อผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender) ก่อนเปิดจดหมายอิเล็กทรอนิกส์ (E - Mail) เพื่อป้องกันการเปิดไฟล์อันตรายที่อาจมีไวรัสคอมพิวเตอร์ โดยเฉพาะ Executable File ได้แก่ ไฟล์ที่มีนามสกุล .exe, .com, .bat และ .inf

๑.๒.๔ หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ต้องออกจากระบบ (Log Out) ทันที เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

๑.๓ การใช้งานเครือข่ายไร้สาย (WiFi) ให้ดำเนินการ ดังนี้

๑.๓.๑ ผู้ดูแลระบบ (Administrator) ต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดเป็นค่ามาตรฐานมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Acess Point) มาติดตั้งเพื่อใช้งาน

๑.๓.๒ ผู้ใช้งาน (User) ต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (WiFi)

๑.๓.๓ ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายไร้สาย (WiFi) ผู้ใช้งาน (User) จะสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะที่ได้รับอนุญาตตามสิทธิของเครือข่ายไร้สาย (Wifi) เท่านั้น

๑.๓.๔ ผู้ใช้งาน (User) ต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ที่เป็นทรัพย์สินของ สคร. ไปใช้งานเครือข่ายไร้สาย (WiFi) ที่ไม่น่าเชื่อถือ

๑.๓.๕ ผู้ใช้งาน (User) ไม่ควรทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ ระหว่างการใช้งานเครือข่ายไร้สาย (WiFi) เนื่องจากอาจเกิดความไม่ปลอดภัยและอาจขาดการเชื่อมต่อของสัญญาณ

๑.๓.๖ ห้ามผู้ใช้งาน (User) ติดตั้งและเปิดการทำงานโปรแกรมประเภทดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายของ สคร. และมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๔ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

๑.๔.๑ การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ (Social Network) ในนามของ สคร. ผู้รับผิดชอบต้องแสดงตำแหน่ง หน้าที่ สังกัด ให้ชัดเจน เพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์หรือเครื่องหมายแสดงสังกัดได้

๑.๔.๒ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ควรนำเสนอเกี่ยวกับภารกิจงานของ สคร. ได้แก่ วิสัยทัศน์ พันธกิจ ผลการดำเนินงาน และข่าวสารที่เป็นประโยชน์ มีความถูกต้อง ใช้ภาษาที่สุภาพ และมีรูปแบบที่น่าสนใจ โดยเนื้อหาต้องผ่านความเห็นชอบจากผู้บังคับบัญชาก่อนทุกครั้ง

๑.๔.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของ สคร. ผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

/๑.๔.๔ กรณี...

๑.๔.๔ กรณีประชาชนหรือหนวยงานอื่นมีความคิดเห็นแตกตาง ต้องชี้แจงดวยเหตุผล งดเว้นการโต่ตอบด่วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใชในการพัฒนาปรับปรุงในเรื่องที่เกี่ยวข้องต่อไป

๑.๔.๕ ห่ามแสดงความคิดเห็นที่อาจทำให่เข่าใจว่าเป่นความคิดเห็นจาก สคร. และต่องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) วาเปนความคิดเห็นสวนตัว

๑.๔.๖ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที

๒. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections)

การระบุและยืนยันตัวตนของผู้ใช้งานอยู่ภายนอกองค์กร (User Authentication for External Connections) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง เพื่อตรวจสอบความถูกต้องในการพิสูจน์ยืนยันตัวตน (Authentication) ก่อนเข้าถึงเครือข่าย ระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ให้ดำเนินการ ดังนี้

๓.๑ ศูนย์เทคโนโลยีสารสนเทศต้องจัดทำผังระบบเครือข่าย (Network Diagram) พร้อมรายละเอียดอุปกรณ์บนเครือข่ายที่เห็นว่าจำเป็นต่อการใช้งาน ได้แก่ กลุ่มอุปกรณ์ เลขที่อยู่ไอพี (IP Address) และหมายเลขเฉพาะอุปกรณ์ (MAC Address) โดยให้ปรับปรุงทุก ๒ ปี หรือตามความเหมาะสม

๓.๒ การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ มาใช้งานบนเครือข่ายต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ให้ดำเนินการ ดังนี้

๔.๑ ศูนย์เทคโนโลยีสารสนเทศต้องจัดทำแนวทางหรือคู่มือในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

๔.๒ ศูนย์เทคโนโลยีสารสนเทศต้องเปิดใช้งานเฉพาะพอร์ตที่จำเป็นสำหรับการใช้งานเท่านั้น และต้องตรวจสอบพอร์ตที่เปิดให้บริการสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

๕. การแบ่งแยกเครือข่าย (Segregation in Networks) แบ่งเป็น ๔ กลุ่ม ดังนี้

๕.๑ กลุ่มของการให้บริการสารสนเทศ ได้แก่ ระบบสารสนเทศเพื่อการสนับสนุนภารกิจหลัก และระบบสารสนเทศเพื่อการสนับสนุนการปฏิบัติงาน

๕.๒ กลุ่มการใช้งาน ได้แก่ เจ้าของระบบ (System Owner) ผู้ดูแลระบบ (Administrator) และผู้ใช้งาน (User)

/๕.๓ กลุ่มของ...

๕.๓ กลุ่มของอุปกรณ์สารสนเทศ ได้แก่ อุปกรณ์รักษาความมั่นคงปลอดภัยสารสนเทศ และอุปกรณ์บริหารจัดการเครือข่าย

๕.๔ กลุ่มประเภทของเครือข่ายคอมพิวเตอร์ ได้แก่ ระบบเครือข่ายภายใน (Intranet) ระบบเครือข่ายภายนอก (Internet) และระบบเครือข่ายโซนพิเศษ (Demilitarized Zone : DMZ)

๖. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้ดำเนินการ ดังนี้

๖.๑ ศูนย์เทคโนโลยีสารสนเทศต้องติดตั้งระบบป้องกันการบุกรุกโจมตีทางเครือข่าย (Friwall) เพื่อใช้เป็นจุดควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๖.๒ ผู้ดูแลระบบ (Administrator) ต้องไม่เปิดเผยข้อมูลการเชื่อมต่อทางเครือข่าย ก่อนได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

๖.๓ ผู้ดูแลระบบ (Administrator) มีหน้าที่ในการควบคุมการเชื่อมต่อสัญญาณหรือยกเลิก การเชื่อมต่อสัญญาณ ตามที่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ ทั้งนี้ หากพบข้อผิดพลาดหรือเห็นว่า หมดความจำเป็นในการเชื่อมต่อสัญญาณให้รายงานศูนย์เทคโนโลยีสารสนเทศทันที

๖.๔ การเชื่อมต่อเครือข่ายสารสนเทศระหว่าง สคร. กับหน่วยงานภายนอก ต้องได้รับอนุญาต จากผู้อำนวยการ สคร. และเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ของผู้ให้บริการที่มีความน่าเชื่อถือ

๗. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ให้ดำเนินการ ดังนี้

๗.๑ ผู้ดูแลระบบ (Administrator) ต้องควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ และการรับ - ส่งหรือการไหลเวียนของข้อมูลหรือสารสนเทศเป็นไปอย่างรวดเร็ว

๗.๒ ผู้ดูแลระบบ (Administrator) ต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ใช้งาน (User) เป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

/หมวด ๕...

หมวด ๕

การควบคุมการเข้าถึงระบบปฏิบัติการ

(Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) โดยต้องมีการควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวตนที่ปลอดภัย

๒. กำหนดแนวปฏิบัติในการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยต้องกำหนดให้ผู้ใช้งาน (User) มีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน (User) ได้ และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการยืนยันว่าเป็นผู้ใช้งาน (User) ที่ได้รับอนุญาต

๓. กำหนดแนวปฏิบัติในการบริหารจัดการรหัสผ่าน (Password Management System) โดยต้องจัดทำระบบบริหารจัดการรหัสผ่าน (Password) ที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่าน (Password) ที่มีคุณภาพ

๔. กำหนดแนวปฏิบัติในการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้

๕. กำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน (Session Time - Out)

๖. กำหนดระยะเวลาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time)

แนวปฏิบัติ

๑. ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองสำหรับเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง เพื่อตรวจสอบความถูกต้องในการพิสูจน์ยืนยันตัวตน (Authentication) ก่อนเข้าถึงระบบปฏิบัติการ (Operating System)

/๓. ศูนย์เทคโน...

๓. ศูนย์เทคโนโลยีสารสนเทศต้องจัดให้มีระบบการบริหารจัดการรหัสผ่าน (Password Management System) ที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการเปลี่ยนรหัสผ่าน (Password) ที่มีคุณภาพ โดยผู้ใช้งาน (User) สามารถเปลี่ยนรหัสผ่าน (Password) ใหม่ หรือขอรหัสผ่าน (Password) ใหม่ได้ด้วยตนเองผ่านระบบบริหารจัดการรหัสผ่าน (Password Management System) กำหนด ดังนี้

๓.๑ กรณีปกติ

การใช้รหัสผ่าน (Password) เดิม เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตน (Authentication) และตั้งรหัสผ่าน (Password) ใหม่ ไปในคราวเดียวกัน

๓.๒ กรณีลืมรหัสผ่าน (Password)

๓.๒.๑ การเลือกใช้วิธีการตอบคำถาม หรือ

๓.๒.๒ การเลือกรับ Link/URL สำหรับการตั้งรหัสผ่าน (Password) ใหม่ผ่านระบบจดหมายอิเล็กทรอนิกส์ (E - Mail) สำรองของผู้ใช้งาน (User)

๔. การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) กำหนด ดังนี้

๔.๑ ผู้ใช้งาน (User) ต้องไม่ดัดแปลงหรือติดตั้งโปรแกรมอรรถประโยชน์ใดๆ บนระบบปฏิบัติการทั้งนี้ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์ต่อศูนย์เทคโนโลยีสารสนเทศ

๔.๒ การใช้งานโปรแกรมอรรถประโยชน์อื่นๆ นอกเหนือจากที่ติดตั้งมากับระบบปฏิบัติการ ได้แก่ โปรแกรมประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรม Formatter กำหนดให้ผู้ดูแลระบบ (Administrator) เท่านั้นที่มีสิทธิใช้งาน

๕. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ เมื่อเว้นว่างจากการใช้งาน (Session Time - Out) เมื่อครบ ๑๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time) โดยให้ใช้งานได้เป็นเวลา ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง และในกรณีที่เชื่อมต่อจากภายนอก กำหนดให้ใช้งานได้ภายในวันและเวลาราชการ เว้นแต่รณีที่มีเหตุผลความจำเป็นให้ขออนุญาตผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

/หมวด ๖...

หมวด ๖
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
(Application and Information Access Control)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ของผู้ใช้งาน (User) และฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น (Application and Information Access Control) ตามสิทธิที่กำหนดไว้

๒. กำหนดแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อ สคร. โดยต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking)

๓. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องระบบคอมพิวเตอร์และระบบสารสนเทศและข้อมูลสารสนเทศจากความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๔. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) โดยต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกสำนักงาน

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการ ดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User) การกำหนดสิทธิตามตำแหน่งและหน้าที่ที่ได้รับมอบหมาย และการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง ซึ่งรวมถึงบุคคลภายนอกหรือผู้รับจ้าง (Outsource) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศด้วย

๑.๒ ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งาน (User) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายภายนอก ให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) โดยมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL)

๑.๓ การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) รายละเอียดปรากฏตามภาคผนวก

/๒. ระบบ...

๒. ระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อ สคร. ให้ดำเนินการ ดังนี้

๒.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ดังนี้

๒.๑.๑ ระบบการบริหารจัดการความมั่นคงปลอดภัยและเครือข่าย ได้แก่ ระบบ Antivirus, ระบบ Active Directory, ระบบ Backup Systems, ระบบ Domain Name Server, ระบบ Dynamic Host Configuration Protocol, ระบบ Network Management, ระบบ Network Monitoring และระบบจัดเก็บข้อมูลกลาง

๒.๑.๒ ระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ - รัฐวิสาหกิจ (GFMIS - SOE)

๒.๒ ระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อ สคร. ต้องได้รับการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกออกจากระบบอื่นๆ

๒.๓ ผู้ดูแลระบบ (Administrator) ต้องแบ่งพื้นที่สำหรับการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายตามระดับความสำคัญและความปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อ สคร. เพื่อควบคุมสภาพแวดล้อมโดยเฉพาะ

๒.๔ การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking) เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องเข้าถึงในสถานที่ที่มีความปลอดภัยและต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

๓. การควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ให้ดำเนินการ ดังนี้

๓.๑ ผู้ดูแลระบบ (Administrator) ต้องตรวจสอบเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ของผู้ใช้งาน (User) หรือบุคคลภายนอก ก่อนนำมาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศ

๓.๑.๑ เครื่องคอมพิวเตอร์ ต้องตรวจสอบ ดังนี้

(๑) ระบบปฏิบัติการต้องได้รับการติดตั้ง Service Pack เวอร์ชั่นล่าสุด

(๒) โปรแกรมตรวจสอบและป้องกันไวรัสคอมพิวเตอร์ต้องได้รับการอัพเดทฐานข้อมูลไวรัสคอมพิวเตอร์ที่เป็นปัจจุบัน

(๓) ไม่ติดตั้งโปรแกรมประเภทดักจับข้อมูล (Network Sniffer) และโปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer)

๓.๑.๒ อุปกรณ์สื่อสารเคลื่อนที่ ได้แก่ Smart Phone และ Taplet ต้องได้รับการยืนยันตัวตนโดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของผู้ใช้งาน (User) สำหรับเข้าใช้งาน

/๔. การปฏิบัติงาน...

๔. การปฏิบัติงานจากภายนอก สคร. (Teleworking) กำหนด ดังนี้

๔.๑ ผู้ใช้งาน (User) ต้องปฏิบัติตามหมวด ๔ แนวปฏิบัติ ข้อ ๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections)

๔.๒ บุคคลภายนอกต้องปฏิบัติตามหมวด ๒ แนวปฏิบัติ ข้อ ๑.๒ การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (๒) กรณีบุคคลภายนอก และหากต้องปฏิบัติงานด้านเทคนิคจากภายนอก สคร. (Teleworking) ให้ดำเนินการตามที่ศูนย์เทคโนโลยีสารสนเทศกำหนดเป็นการเฉพาะคราว

๔.๓ เมื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศแล้ว ผู้ใช้งาน (User) ต้องระมัดระวังไม่ให้ผู้ไม่มีส่วนเกี่ยวข้องเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศจากเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ได้ และต้องออกจากระบบ (Log Out) ทันทีเมื่อปฏิบัติเลิกใช้งาน

/หมวด ๗...

หมวด ๗

การจัดทำระบบสำรองของระบบสารสนเทศ

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศ และการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินและการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่องแม้ในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม และสามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง

นโยบาย

๑. พิจารณาคัดเลือกระบบสารสนเทศที่เหมาะสมในการจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน

๒. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. เพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๓. กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบตามแผนบริหารความต่อเนื่องของ สคร. ด้านสารสนเทศ

๔. ทดสอบสภาพพร้อมใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ และระบบสำรองตามแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. อย่างน้อยปีละ ๑ ครั้ง

๕. กำหนดความถี่ของการปฏิบัติในแต่ละข้อ โดยต้องมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของหน่วยงาน

แนวปฏิบัติ

๑. ศูนย์เทคโนโลยีสารสนเทศต้องจัดทำระบบสารสนเทศและระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน โดยมีขั้นตอน ดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) จัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูลและการกู้คืนข้อมูลสารสนเทศ

๑.๒ ผู้ดูแลระบบ (Administrator) กำหนดรูปแบบการสำรองข้อมูลของระบบการสำรองข้อมูล (Backup System) ดังนี้

๑.๒.๑ รายชื่อระบบคอมพิวเตอร์และระบบสารสนเทศที่ได้รับการพิจารณาคัดเลือก ดังนี้

(๑) ระบบคอมพิวเตอร์เครื่องลูกข่ายเสมือน (Virtual Desktop Infrastructure : VDI)

(๒) ระบบติดตามการดำเนินการของโครงการ (Tracking System)

/(๓) ระบบจดหมาย...

(๓) ระบบจดหมายอิเล็กทรอนิกส์ (E - Mail)

(๔) ระบบสำนักงานอัตโนมัติ (E - Office)

(๕) ระบบสารบรรณอิเล็กทรอนิกส์ (E - Sarabun)

(๖) ระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ - รัฐวิสาหกิจ (GFMIS - SOE)

๑.๒.๒ กำหนดรูปแบบการสำรองข้อมูลเฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) หรือเฉพาะส่วนที่มีการเปลี่ยนแปลง (Differential Backup) ทุกวัน

๑.๒.๓ กำหนดรูปแบบการสำรองข้อมูลแบบสมบูรณ์ (Full Backup) ทุกสัปดาห์และทุกเดือน ทั้งนี้ เนื่องจากศูนย์เทคโนโลยีสารสนเทศได้ดำเนินการสำรองข้อมูลระบบคอมพิวเตอร์และระบบสารสนเทศแบบสมบูรณ์ (Full Backup) ทุกระบบงานจึงได้รับการสำรองข้อมูลด้วย

๑.๓ ผู้ดูแลระบบ (Administrator) ต้องพิมพ์รายละเอียดไว้บนตลับเทปแม่เหล็ก (Magnetic Tape Drive) ที่ใช้สำหรับการสำรองข้อมูล ได้แก่ รูปแบบการสำรองข้อมูลแบบรายวันหรือรายสัปดาห์หรือรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล

๑.๔ ผู้ดูแลระบบ (Administrator) ต้องกำหนดรูปแบบการกู้คืนข้อมูลของระบบการสำรองข้อมูล (Backup System) โดยมีความถี่และรูปแบบ ดังนี้

๑.๔.๑ การกู้คืนข้อมูลรายวันจากตลับเทปแม่เหล็ก (Magnetic Tape Drive) ที่สำรองข้อมูลเฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) หรือที่สำรองข้อมูลเฉพาะส่วนที่มีการเปลี่ยนแปลง (Differential Backup)

๑.๔.๒ การกู้คืนข้อมูลรายสัปดาห์หรือรายเดือนจากตลับเทปแม่เหล็ก (Magnetic Tape Drive) ที่สำรองข้อมูลแบบสมบูรณ์ (Full Backup)

๒. ศูนย์เทคโนโลยีสารสนเทศดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ดังนี้

๒.๑ กำหนดผู้มีหน้าที่รับผิดชอบระบบสารสนเทศ

๒.๒ กำหนดผู้มีหน้าที่รับผิดชอบระบบสำรองข้อมูลสารสนเทศ

๒.๓ กำหนดผู้มีหน้าที่รับผิดชอบการจัดทำแผนดังกล่าว

๒.๔ กำหนดให้ปรับปรุงแผนดังกล่าวทุก ๒ ปี

๓. ศูนย์เทคโนโลยีสารสนเทศต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้อย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์และแผนการสำรองข้อมูล สคร. รวมถึงการทดสอบสภาพความพร้อมใช้งาน ได้นำข้อมูลไปรวมไว้ในแผนบริหารความต่อเนื่องในสภาวะวิกฤต ด้านสารสนเทศของ สคร. รายละเอียดปรากฏตามเอกสารภาคผนวก

/หมวด ๘...

หมวด ๘
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ทำให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่กำหนด มีความมั่นคงปลอดภัยและหน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

นโยบาย

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒. การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

แนวปฏิบัติ

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒. กำหนดให้มีผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๒.๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศประจำปีงบประมาณ ให้ดำเนินการโดยกลุ่มตรวจสอบภายใน (Internal Auditor)

๒.๒ หากมีความประสงค์ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศเชิงเทคนิค ให้ดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๓. กำหนดแนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๓.๑ ผู้ตรวจสอบต้องจัดทำรายงานพร้อมข้อเสนอแนะในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๒ ศูนย์เทคโนโลยีสารสนเทศต้องอำนวยความสะดวกแก่ผู้ตรวจสอบในการตรวจสอบข้อมูลที่สำคัญ

๓.๓ ในกรณีที่ผู้ตรวจสอบจำเป็นต้องเข้าถึงข้อมูลสำคัญให้ศูนย์เทคโนโลยีสารสนเทศสร้างสำเนาสำหรับข้อมูลนั้น โดยให้ผู้ตรวจสอบใช้งานและทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือหากประสงค์จัดเก็บข้อมูลนั้นเป็นหลักฐานให้แจ้งศูนย์เทคโนโลยีสารสนเทศทราบ

๓.๔ ศูนย์เทคโนโลยีสารสนเทศต้องจัดสรรอุปกรณ์ที่จำเป็นต้องใช้ในการตรวจสอบเชิงเทคนิค

/๓.๕ ในกรณี...

๓.๕ ในกรณีมีการติดตั้งเครื่องมือที่ใช้ในการตรวจประเมินความเสี่ยงระบบคอมพิวเตอร์และระบบสารสนเทศสารสนเทศ ให้แยกการติดตั้งเครื่องมือออกจากระบบที่ให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว (Read Only)

๓.๖ ผู้ตรวจสอบต้องแจ้งความเสี่ยงและระบุความรุนแรงของเครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยง

๓.๗ ผู้ดูแลระบบ (Administrator) ต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ตรวจสอบเป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

ภาคผนวก

แผนการฝึกอบรมผู้ใช้งาน (User)

๑. การฝึกอบรมการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศของ สคร. อย่างถูกต้อง และปลอดภัย

การฝึกอบรมการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศของ สคร. ให้แก่บุคลากร สคร. โดยเฉพาะบุคลากรใหม่ เพื่อให้ผู้ใช้งาน (User) มีความรู้ความเข้าใจและสามารถใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศได้อย่างถูกต้อง สามารถสนับสนุนการปฏิบัติงานได้เป็นอย่างดี ตลอดจนตระหนักถึงภัยจากการใช้งานเครือข่ายทั้งภายใน (Intranet) และภายนอก (Internet) ได้อย่างปลอดภัย ดังนี้

๑.๑ ระบบสารบรรณอิเล็กทรอนิกส์ (E - Sarabun)

<u>เนื้อหาหลักสูตร</u>

เนื่องจากเป็นระบบสารสนเทศที่ได้รับการปรับปรุงใหม่เพื่อทดแทนระบบเดิมที่ใช้งานมานาน จึงต้องมีการฝึกอบรม ซึ่งระบบดังกล่าว สามารถสร้าง รับ ส่ง หนังสือราชการ ติดตามงาน และการออกสรุปรายงานตามเงื่อนไขที่กำหนด เพื่อนำไปใช้ในการวางแผนการปฏิบัติงานของบุคลากรได้อย่างมีประสิทธิภาพ

<u>กลุ่มเป้าหมาย</u>

บุคลากร สคร. ทุกคน โดยเฉพาะเจ้าหน้าที่ธุรการ หรือผู้ที่ปฏิบัติงานด้านธุรการ

๑.๒ ระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์-รัฐวิสาหกิจ (GFMIS - SOE)

<u>เนื้อหาหลักสูตร</u>

เนื่องจากเป็นระบบสารสนเทศที่ได้รับการปรับปรุงใหม่ที่รองรับต่อภารกิจหลักของ สคร. ดังนี้

๑.๒.๑ ด้านรัฐวิสาหกิจในส่วนของรูปแบบและวิธีการนำส่งข้อมูลเข้าระบบ GFMIS - SOE ทั้งในส่วนของงบการเงิน งบลงทุนข้อมูลทั่วไป ข้อมูลผู้บริหารและพนักงาน และข้อมูลกรรมการรัฐวิสาหกิจ ทั้งนี้ เพื่อให้การเปิดเผยข้อมูลงบการเงินและงบลงทุนแก่สาธารณะในรูปแบบอิเล็กทรอนิกส์ (Open Data) ในรูปแบบ .XLS, .CSV และ .JSON อย่างปลอดภัย

๑.๒.๒ ด้านหลักทรัพย์ของรัฐ สำหรับช่วยให้ สคร. และกระทรวงการคลัง สามารถบริหารหลักทรัพย์ที่ถือครอง หน่วยลงทุน ทั้งในกองทุนรวมวายุภักษ์หนึ่งและกองทุนรวมเพื่อร่วมทุนในวิสาหกิจขนาดกลางและขนาดย่อมได้อย่างมีประสิทธิภาพ รวมถึงสามารถจำหน่ายหลักทรัพย์ที่ไม่มีความจำเป็นต้องถือครอง

๑.๒.๓ ด้านโครงการร่วมลงทุนในกิจการของรัฐ มีฐานข้อมูลที่ถูกต้อง และเป็นปัจจุบัน เพื่อให้กระทรวงการคลัง และ สคร. สามารถกำหนดยุทธศาสตร์การให้เอกชนร่วมลงทุนในกิจการของรัฐไปในทิศทางที่ถูกต้อง

/<u>กลุ่มเป้าหมาย...</u>

กลุ่มเป้าหมาย

- ด้านรัฐวิสาหกิจ : บุคลากรกองพัฒนารัฐวิสาหกิจ ๑ - ๓ บุคลากรสำนักนโยบายและแผน และบุคลากรของหน่วยงานรัฐวิสาหกิจที่เกี่ยวข้อง
- ด้านหลักทรัพย์ของรัฐ : บุคลากรสำนักบริหารหลักทรัพย์
- ด้านโครงการร่วมลงทุนในกิจการของรัฐ : บุคลากรกองส่งเสริมการให้เอกชนร่วมลงทุนในกิจการของรัฐ

๑.๓ ระบบ Web Portal

เนื้อหาหลักสูตร

เนื่องจากเป็นระบบสารสนเทศที่ได้รับการปรับปรุงใหม่เพื่อทดแทนระบบเดิม เพื่อให้ผู้ใช้งาน (User) สามารถทำงานได้อย่างมีประสิทธิภาพด้วยความสะดวกและรวดเร็ว โดยสามารถลดขั้นตอนและระยะเวลาในการปฏิบัติงานจากการเชื่อมโยงระหว่างระบบสารสนเทศและข้อมูลต่างๆ เข้าไว้ด้วยกัน

กลุ่มเป้าหมาย

บุคลากร สคร. ทุกคน

๑.๔ ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงความมั่นคงปลอดภัย

เนื้อหาหลักสูตร

อบรมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงความมั่นคงปลอดภัย เพื่อให้สามารถเข้าถึงระบบคอมพิวเตอร์แบบคลาวด์คอมพิวติ้ง (Cloud Computing) ผ่านเครื่องคอมพิวเตอร์ลูกข่ายเสมือน (Virtual Desktop Infrastructure : VDI) หรือเข้าถึงด้วยอุปกรณ์สื่อสารเคลื่อนที่ทั้งจากภายในและภายนอกองค์กร รวมทั้งเข้าถึงระบบสารสนเทศ เช่น ระบบ Web Portal ระบบสำนักงานอัตโนมัติ (ระบบจองรถ/ระบบจองห้องประชุม/ระบบลาราชการ/ระบบพัสดุ) ระบบติดตามการดำเนินการของโครงการ (Tracking System) ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) รวมถึงความมั่นคงปลอดภัย เช่น ไวรัสคอมพิวเตอร์ การใช้สื่อสังคมออนไลน์ (Social Network) ที่อาจเป็นภัยต่อผู้ใช้งาน (User) หรือต่อ สคร.

กลุ่มเป้าหมาย

บุคลากรใหม่ของ สคร. และบุคลากร สคร. ที่สนใจ

/๒. การฝึก...

๒. การฝึกอบรมที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

๒.๑ หลักการและเหตุผล

กระทรวงการคลังมีนโยบายที่จะพัฒนาบุคลากรของกระทรวงการคลังทุกระดับให้มีความรู้ความสามารถด้านเทคโนโลยีสารสนเทศและการสื่อสาร สามารถใช้ปฏิบัติงานได้อย่างคล่องแคล่ว รวดเร็ว และสามารถพัฒนาทักษะด้านเทคโนโลยีสารสนเทศ พร้อมที่จะปฏิบัติงานกับโปรแกรมการทำงานและเครื่องคอมพิวเตอร์ได้ในอนาคต เท่าทันกับการเปลี่ยนแปลงไปสู่กระทรวงการคลังดิจิทัลได้อย่างมีประสิทธิภาพ ดังนั้น เพื่อเป็นการเพิ่มพูนและพัฒนาความรู้ความสามารถของบุคลากร ให้มีความรู้ทางด้านเทคโนโลยีสารสนเทศ และการสื่อสาร กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ ให้สามารถนำวิทยาการและเทคโนโลยีที่ทันสมัย เพื่อใช้ในการปฏิบัติงานและการบริหารงานของหน่วยงานต่างๆ และไม่ละเมิดกฎหมายที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยด้านสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงการคลังในฐานะเป็นศูนย์พัฒนาบุคลากร จึงได้จัดให้มีโครงการอบรมด้านการพัฒนาเทคโนโลยีสมัยใหม่ หลักสูตร “รู้เท่าทัน การรักษาความมั่นคงปลอดภัยสารสนเทศ” ให้แก่บุคลากรกระทรวงการคลังในครั้งนี้

๒.๒ วัตถุประสงค์

๒.๒.๑ เพื่อพัฒนาความรู้ความสามารถบุคลากรกระทรวงการคลังได้เรียนรู้กฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๒.๒ เพื่อให้บุคลากรได้ตระหนักถึงความสำคัญและบทลงโทษของการรักษาความมั่นคงปลอดภัยสารสนเทศ ของหน่วยงาน

๒.๒.๓ เพื่อให้บุคลากรได้เข้าใจ เข้าถึงการจัดการ ควบคุม และการสำรองข้อมูลสารสนเทศเพื่อให้อยู่ในสภาพพร้อมใช้งาน

๒.๒.๔ เพื่อเตรียมบุคลากรซึ่งปฏิบัติงานด้านอื่น ๆ ให้มีความรู้ทางด้านเทคโนโลยีสารสนเทศและการสื่อสาร และพร้อมที่จะปฏิบัติงานกับโปรแกรมการทำงาน และเครื่องคอมพิวเตอร์ได้ในอนาคตได้อย่างถูกระเบียบ

๒.๒.๕ เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

/๒.๓ รายละเอียด...

๒.๓ รายละเอียดโครงการ

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ให้หน่วยงานจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ เพื่อให้การดำเนินการต่างๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงาน เพื่อเป็นเครื่องมือให้กับบุคลากรของกระทรวงการคลัง ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคนใช้เป็นแนวทางการปฏิบัติงานและการบริหารราชการมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล อีกทั้งเป็นการพัฒนาทักษะด้านเทคโนโลยีดิจิทัลให้มีความพร้อมที่จะปฏิบัติงานโดยนำเทคโนโลยีดิจิทัลมาใช้ให้เกิดประโยชน์สูงสุดให้เท่าทันกับการเปลี่ยนแปลงไปสู่รัฐบาลดิจิทัล โดยมีเนื้อหาดังนี้

๒.๓.๑ ความรู้เกี่ยวกับกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๒.๓.๒ กรณีศึกษาการละเมิดการรักษาความมั่นคงปลอดภัยสารสนเทศ

๒.๓.๓ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๓.๔ ข้อปฏิบัติเบื้องต้นในการใช้สารสนเทศและระบบเครือข่าย

๒.๓.๕ มาตรการการรักษาความมั่นคงปลอดภัย

๒.๓.๖ เทคนิคการติดตั้งค่าอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เชื่อมต่อกับเครือข่าย

๒.๓.๗ เทคนิคการป้องกันการละเมิดหรือบุกรุกข้อมูลโดยรู้เท่าไม่ถึงการณ์

๒.๓.๘ การเตรียมความพร้อมกรณีฉุกเฉิน

๒.๔ คุณสมบัติผู้เข้ารับการฝึกอบรม

ข้าราชการในสังกัดกระทรวงการคลัง

๒.๕ จำนวนผู้เข้ารับการฝึกอบรมสัมมนา

จำนวน ๑๐๐ คน

๒.๖ ค่าใช้จ่าย

ใช้เงินกองทุนพัฒนาบุคลากรของกระทรวงการคลัง ประจำปีงบประมาณ ๒๕๖๒

๒.๗ ระยะเวลาดำเนินการ

สิงหาคม ๒๕๖๒ เวลา ๘.๓๐ - ๑๖.๐๐ น.

/๒.๘ กำหนดการ...

๒.๘ กำหนดการ

๘.๓๐ – ๘.๕๐ น.	ลงทะเบียน
๘.๕๐ – ๙.๐๐ น.	พิธีเปิด
๙.๐๐ – ๑๐.๓๐ น.	“รู้ทันภัยคุกคาม เพื่อกำจัดความเสี่ยง” ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ กฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ตัวอย่างการละเมิดและโทษที่ได้รับ และเทคนิคการอุดช่องโหว่/ป้องกันภัยจากผู้ไม่ประสงค์ดี
๑๐.๓๐ – ๑๐.๔๕ น.	พักรับประทานอาหารว่าง
๑๐.๔๕ – ๑๒.๐๐ น.	“รู้ทัน ภัยคุกคาม เพื่อกำจัดความเสี่ยง” (ต่อ)
๑๒.๐๐ – ๑๓.๐๐ น.	พักรับประทานอาหารกลางวัน
๑๓.๐๐ – ๑๔.๓๐ น.	“ควบคุม ป้องกัน กำจัดภัยคุกคาม” ได้แก่ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เทคนิคการติดตั้งค่าอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่เชื่อมต่อกับเครือข่าย เทคนิคการป้องกันการละเมิดหรือบุกรุกข้อมูลโดยรู้เท่าไม่ถึงการณ์ และการเตรียมความพร้อมกรณีฉุกเฉิน หมายเหตุ โปรดนำอุปกรณ์สื่อสารไร้สาย เช่น โทรศัพท์สมาร์ทโฟน ไอแพด โน๊ตบุ๊ค มาด้วย
๑๔.๓๐ – ๑๔.๔๕ น.	พักรับประทานอาหารว่าง
๑๔.๔๕ – ๑๖.๐๐ น.	“ควบคุม ป้องกัน กำจัดภัยคุกคาม” (ต่อ) ถาม - ตอบปัญหา

๒.๙ สถานที่จัดฝึกอบรมสัมมนา

ห้องประชุมวายุภักษ์ ๔ ชั้น ๔ กระทรวงการคลัง

๒.๑๐ ประโยชน์ที่ได้รับ

๒.๑๐.๑ บุคลากรของกระทรวงการคลัง มีแนวทางการป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลสารสนเทศของหน่วยงาน และมาตรการการลงโทษ

๒.๑๐.๒ บุคลากรของกระทรวงการคลัง สามารถจัดการควบคุม และสำรองข้อมูลสารสนเทศได้อย่างมีประสิทธิภาพ

๒.๑๐.๓ บุคลากรของกระทรวงการคลัง ได้พึงระวังการเข้าถึงข้อมูลสารสนเทศได้อย่างระมัดระวัง และรอบคอบมากยิ่งขึ้น

๒.๑๐.๔ บุคลากรมีความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

/ตารางสรุป...

ตารางสรุปแผนการฝึกอบรมผู้ใช้งาน (User)

หลักสูตร	จำนวน/ชั่วโมง	จำนวน/วัน	ช่วงเวลา											
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
๑. ระบบสารบรรณอิเล็กทรอนิกส์ (E - Sarabun)	๓	๔												
๒. ระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ - รัฐวิสาหกิจ (GFMIS - SOE)	๓	๑๔												
๓. ระบบ Web Portal	๓	๒												
๔. ระบบคอมพิวเตอร์และระบบสารสนเทศรวมถึงการรักษาความมั่นคงปลอดภัย	๓	๒												
๕. การฝึกอบรมที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ	ตามที่กระทรวงการคลังหรือหน่วยงานภายนอกจัดขึ้น													

การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้รับจ้าง (Outsource)

เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศ ห้องศูนย์ข้อมูล (Data Center) และพื้นที่ปฏิบัติงานทั่วไป ซึ่งเป็นทรัพย์สินที่มีค่าของ สคร. มีความปลอดภัยต่อการถูกบุกรุกโจมตี และลดความเสี่ยงต่อการลักลอบเปิดเผยข้อมูลสารสนเทศ จึงกำหนดแนวปฏิบัติการควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้รับจ้าง (Outsource) ดังนี้

๑. ก่อนปฏิบัติงาน

๑.๑ ผู้รับจ้าง (Outsource) ต้องขออนุญาตผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับผู้รับจ้าง (Outsource) พร้อมแนบสำเนาสัญญาจ้างหรือเหตุผลในการปฏิบัติงาน

๑.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายพิจารณาเหตุผลการขออนุญาตดังกล่าว และต้องอนุมัติเป็นลายลักษณ์อักษร

๑.๓ ผู้ดูแลระบบ (Administrator) ดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านชั่วคราว (Temporary Password) สำหรับเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๔ เจ้าของระบบ (System Owner) อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้ผู้รับจ้าง (Outsource)

๑.๕ ผู้ดูแลระบบ (Administrator) กำหนดสิทธิให้ผู้ใช้งาน (User) ตามที่เจ้าของระบบ (System Owner) อนุมัติ พร้อมทั้งแจ้งให้ผู้รับจ้าง (Outsource) ได้รับทราบ

๒. ระหว่างปฏิบัติงาน

๒.๑ ผู้รับจ้าง (Outsource) ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน

๒.๒ เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศต้องกำกับดูแลการปฏิบัติงานของผู้รับจ้าง (Outsource) โดยเฉพาะการติดตั้ง ซ่อมแซม หรือการเปลี่ยนอุปกรณ์ประมวลผลข้อมูล (Process Device) ภายในห้องศูนย์ข้อมูล (Data Center) ต้องกำกับดูแลโดยเคร่งครัด

๒.๓ ผู้รับจ้าง (Outsource) ต้องปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมายเท่านั้น และต้องคำนึงถึงการรักษาความลับข้อมูลของทางราชการเป็นสำคัญ หากเกิดปัญหาระหว่างการปฏิบัติงานให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศที่กำกับดูแลการปฏิบัติงานทันที

/๓. หลังปฏิบัติ...

๓. หลังปฏิบัติงาน

๓.๑ ให้ผู้รับจ้าง (Outsource) แจ้งความประสงค์ต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศทันทีเมื่อปฏิบัติงานแล้วเสร็จ

๓.๒ ผู้ดูแลระบบ (Administrator) จะยกเลิกสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศและลบข้อมูลสารสนเทศของผู้รับจ้าง (Outsource) เป็นการถาวรเมื่อพ้นกำหนด ๙๐ วัน

๔. การรักษาความลับ

ผู้รับจ้าง (Outsource) ต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงดังกล่าว ต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

แผนบริหารความต่อเนื่องในสภาวะวิกฤต ด้านสารสนเทศ
ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ
พ.ศ. ๒๕๖๒

สารบัญ

๑. บทนำ

ด้วยสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ได้นำระบบคอมพิวเตอร์และระบบสารสนเทศที่ทันสมัยเข้ามาให้บริการเพื่อสนับสนุนการปฏิบัติงานแก่บุคลากร สคร. ทั้งในภารกิจหลักประกอบด้วย ภารกิจด้านรัฐวิสาหกิจ ด้านหลักทรัพย์ของรัฐ และด้านการให้เอกชนร่วมลงทุนในกิจการของรัฐ และภารกิจสนับสนุนสำหรับการบริหารจัดการภายใน สคร. รวมทั้งการประชาสัมพันธ์ข้อมูลข่าวสารให้กับบุคคลภายนอกที่สนใจ อย่างไรก็ตาม ในการให้บริการดังกล่าวอาจมีความเสี่ยงที่เกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศอันเนื่องมาจากเหตุการณ์ที่ไม่พึงประสงค์ต่างๆ เช่น ไฟฟ้าดับ อัคคีภัย และเหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เป็นต้น ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศไม่สามารถให้บริการได้อย่างต่อเนื่อง ประกอบกับประกาศ สคร. เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒ กำหนดให้ศูนย์เทคโนโลยีสารสนเทศ (ศทส.) จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ สามารถให้บริการแก่ผู้ใช้งาน (User) ได้อย่างต่อเนื่องและมีประสิทธิภาพ ตลอดจนสามารถปฏิบัติงานตามภารกิจของ สคร. ได้ตามเป้าหมายที่กำหนดไว้

ดังนั้น ศทส. จึงได้วิเคราะห์และประเมินความเสี่ยงด้านสารสนเทศ โดยพิจารณาจากเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) และภัยพิบัติหรือสถานการณ์อื่นๆ รวมถึงได้กำหนดแนวทางการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต และการสำรองและกู้คืนข้อมูลสารสนเทศ เพื่อจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. พ.ศ. ๒๕๖๒ สำหรับใช้เป็นแนวทางในการปฏิบัติงานต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อให้ สคร. มีแนวทางในการระบุและประเมินความเสี่ยงด้านสารสนเทศ รวมถึงการกำหนดแนวทางบริหารความเสี่ยงด้านสารสนเทศ โดยการป้องกัน จัดการ และลดความเสี่ยงดังกล่าวให้อยู่ในระดับที่ยอมรับได้ และทำให้ สคร. สามารถดำเนินงานได้อย่างต่อเนื่อง

๒.๒ เพื่อให้ สคร. มีแนวทางในการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศและสามารถเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤตที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงมีแนวปฏิบัติในการบริหารจัดการ กำกับ ตรวจสอบ และดูแลรักษาระบบคอมพิวเตอร์และระบบสารสนเทศ ให้มีความมั่นคง ปลอดภัย มีเสถียรภาพ และพร้อมใช้งานตลอดเวลา

๒.๓ เพื่อให้ สคร. มีแนวทางในการสำรองระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ โดยสามารถกู้คืนระบบและข้อมูลดังกล่าวได้ทันที เพื่อให้ผู้ใช้งาน (User) สามารถปฏิบัติงานได้อย่างต่อเนื่อง

/๓. ขอบเขต...

๓. ขอบเขต

แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของ สคร. พ.ศ. ๒๕๖๒ ฉบับนี้ เพื่อรองรับสถานการณ์ฉุกเฉินในสภาวะวิกฤตในพื้นที่ สคร. ดังนี้

๓.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร.

๓.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี

๓.๓ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device)

๓.๔ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค

๓.๕ เหตุการณ์ไฟฟ้าดับ

๓.๖ เหตุการณ์อัคคีภัย

๓.๗ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง

๔. การวิเคราะห์ความเสี่ยงด้านสารสนเทศ

เนื่องจาก สคร. มีภารกิจในการบริหารและพัฒนารัฐวิสาหกิจและหลักทรัพย์ของรัฐ โดยการเสนอแนะนโยบายและมาตรการการกำกับดูแล การประเมินผลและการพัฒนารัฐวิสาหกิจ เพื่อเพิ่มประสิทธิภาพรัฐวิสาหกิจและสร้างมูลค่าเพิ่มให้แก่ทรัพย์สินของรัฐ พร้อมทั้งส่งเสริมและสนับสนุนการให้เอกชนร่วมลงทุนในกิจการของรัฐ สคร. จึงได้นำระบบคอมพิวเตอร์และระบบสารสนเทศเข้ามาสนับสนุนและอำนวยความสะดวกในการปฏิบัติงาน ซึ่งระบบดังกล่าวจำเป็นต้องมีการวิเคราะห์และประเมินความเสี่ยงด้านสารสนเทศ รวมถึงมีแผนการบริหารความต่อเนื่อง เพื่อรองรับสถานการณ์ฉุกเฉินในสภาวะวิกฤต ลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้น อันจะส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ มีความมั่นคงปลอดภัย และเกิดประโยชน์สูงสุดแก่การปฏิบัติราชการ

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศ พบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบคอมพิวเตอร์และสารสนเทศ รวมถึงข้อมูลสารสนเทศ มีดังนี้

๔.๑ ความเสี่ยงที่เกิดจากบุคคล ดังนี้

๔.๑.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร. หมายถึง บุคลากรของ สคร. ขาดความรู้ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศ เช่น ด้านฮาร์ดแวร์ ด้านซอร์ฟแวร์ และด้านเครือข่าย รวมถึงการใช้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศที่ไม่เหมาะสม

๔.๑.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี หมายถึง ผู้ที่หวังก่อกวน เจาะทำลายระบบเพื่อสร้างความเสียหายแก่ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ หากไม่ได้รับการป้องกันด้วยเครื่องมือหรืออุปกรณ์ที่มีมาตรฐานและอัพเดทให้ทันสมัย เช่น Firewall ระบบ IPS และระบบป้องกันไวรัส

/๓) เหตุการณ์...

๔.๑.๓ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) หมายถึง ผู้ที่ลักลอบเข้าไปโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) หากศูนย์ข้อมูลดังกล่าวไม่ได้รับการป้องกันที่ดี เช่น มาตรการในการเข้าถึงห้องศูนย์ข้อมูล (Data Center) เครื่องอ่านบัตรแถบแม่เหล็ก กล้องวงจรปิด และเจ้าหน้าที่รักษาความปลอดภัย เป็นต้น

๔.๒ ความเสี่ยงที่เกิดจากด้านเทคนิค หมายถึง เหตุการณ์หรือภัยที่เกิดจากอุปกรณ์ในห้องศูนย์ข้อมูล (Data Center) ทำงานไม่เต็มประสิทธิภาพหรือไม่สามารถให้บริการได้ เช่น อุปกรณ์ประมวลผลข้อมูล (Process Device) ชำรุด เสียหาย เนื่องจากอุปกรณ์บางรายการเสื่อมสภาพตามอายุการใช้งาน ระบบปรับอากาศชำรุดส่งผลให้อุณภูมิห้องศูนย์ข้อมูล (Data Center) สูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ที่ให้บริการหยุดการทำงาน ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถใช้งานได้ หรืออาจได้รับความเสียหาย

๔.๓ ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ

๔.๓.๑ เหตุการณ์ไฟฟ้าดับ หมายถึง เหตุการณ์หรือภัยที่เกิดจากไฟฟ้าดับ ซึ่งส่งผลให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) ไม่มีแหล่งพลังงานที่ใช้ในการเปิดระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับให้บริการ เช่น สายไฟฟ้าขาด ไฟฟ้าช็อต หม้อแปลงไฟฟ้าที่ติดตั้งบริเวณกระทรวงการคลังระเบิดเสียหาย เนื่องจาก สคร. ใช้ไฟฟ้าจากแหล่งจ่ายไฟฟ้าดังกล่าว

๔.๓.๒ เหตุการณ์อัคคีภัย หมายถึง เหตุการณ์หรือภัยที่เกิดจากไฟไหม้ ซึ่งเป็นเหตุการณ์ที่สร้างความเสียหายร้ายแรงที่สุด ทำให้ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) ถูกไฟไหม้จนทำให้ไม่สามารถปฏิบัติงานได้ ซึ่งเกิดได้หลายสาเหตุ เช่น ไฟฟ้าลัดวงจร หรือไฟไหม้บริเวณอื่นแล้วไหม้ลุกลามมาที่ห้องศูนย์ข้อมูล (Data Center)

๔.๓.๓ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง หมายถึง อันเกิดจากภัยตามธรรมชาติหรือสถานการณ์ที่เกิดจากกลุ่มบุคคล ซึ่งอาจไม่เกิดผลกระทบโดยตรงต่อการให้บริการของระบบคอมพิวเตอร์และระบบสารสนเทศ แต่จะเกิดผลกระทบต่อการเข้าไปปฏิบัติงานภายในพื้นที่ สคร.

/๕. การประเมิน...

๕. การประเมินความเสี่ยงด้านสารสนเทศ

ศทส. ได้ประเมินความเสี่ยงด้านสารสนเทศจากความเสี่ยงที่เกิดจากบุคคล จากด้านเทคนิค และจากภัยพิบัติหรือสถานการณ์อื่นๆ ในข้อ ๓ และ ๔ มาเป็นแนวทางในการดำเนินงาน โดย ศทส. ได้ประเมินสถานการณ์ความเสี่ยงด้านสารสนเทศของ สคร. แล้วปรากฏ ดังนี้

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๑. เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร.	- ระบบคอมพิวเตอร์ติดไวรัส หรือหนอนอินเทอร์เน็ตจากอินเตอร์เน็ต หรือไฟล์ที่คัดลอกจากอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศประมวลผลข้อมูลได้ช้าลงหรืออาจทำงานผิดพลาดได้	๕	๑	๕	ค่อนข้างต่ำ	- ผู้ดูแลระบบ (Administrator) ตัดการเชื่อมต่อเครื่องที่ติดไวรัสดังกล่าว ออกจากระบบเครือข่ายภายใน และดำเนินการสแกนไวรัสเพื่อกำจัดไวรัสเครื่องดังกล่าว - หากไวรัสดังกล่าวไม่หายไป ให้ดำเนินการสแกนไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server)
๒. เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี	- ระบบคอมพิวเตอร์และระบบสารสนเทศอาจถูกบุกรุกโจมตี หรือถูกขโมยข้อมูลสารสนเทศ หรือปรับแต่งแก้ไขระบบ หน้าเว็บไซต์ ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศล่มได้	๓	๔	๑๒	ค่อนข้างสูง	- ตรวจพอร์ตทั้งหมดที่ใช้เชื่อมต่อแล้วให้ปิดพอร์ตที่ไม่ได้ใช้งานโดยทันที

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๓. เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device)	- อุปกรณ์ประมวลผลข้อมูล (Process Device) สูญหาย และอาจเสี่ยงต่อการถูกโจรกรรมข้อมูลบนอุปกรณ์ประมวลผลข้อมูล (Process Device) ซึ่งส่งผลกระทบต่อ สคร. โดยเฉพาะข้อมูลที่เป็นความลับ - ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถให้บริการได้เต็มประสิทธิภาพหรือไม่สามารถให้บริการได้	๑	๕	๕	ค่อนข้างต่ำ	- ผู้พบเหตุรายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป - ผู้ดูแลระบบ (Administrator) ตรวจสอบความครบถ้วนและความเสียหายของอุปกรณ์ประมวลผลข้อมูล (Process Device) และผลกระทบต่อระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ
๔. เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค	- อุปกรณ์ประมวลผลข้อมูล (Process Device) บางรายการหยุดทำงานชั่วขณะหรือใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศได้ไม่เต็มประสิทธิภาพ - ระบบปรับอากาศชำรุดส่งผลให้อุณหภูมิในห้องศูนย์ข้อมูล (Data Center) สูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ได้รับความเสียหาย - การปฏิบัติงานเกิดความล่าช้า เนื่องจากต้องรอการซ่อมแซมแก้ไข	๓	๒	๖	ค่อนข้างต่ำ	- ผู้พบเหตุรายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป - ผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหาย ผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) หรือระบบปรับอากาศที่ได้รับความเสียหาย หากเสียหายเล็กน้อยให้ดำเนินการแก้ไข และเปิดใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศต่อไป

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๕. เหตุการณ์ไฟฟ้าดับ	- อุปกรณ์ประมวลผลข้อมูล (Process Device) หยุดทำงาน - การปฏิบัติงานด้านระบบคอมพิวเตอร์และระบบสารสนเทศเกิดความล่าช้าเนื่องจากต้องรอการซ่อมแซมแก้ไข	๕	๒	๑๐	ค่อนข้างสูง	- ผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหาย ผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) และระบบปรับอากาศ พร้อมทั้งรายงานให้ผู้อำนวยการ ศทส. ทราบเพื่อสั่งการต่อไป - ศทส. ประชาสัมพันธ์ให้กับบุคลากร สคร. ได้รับทราบถึงการหยุดให้บริการชั่วคราวเนื่องจากไฟฟ้าดับ - ศทส. ประสานงานกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงการคลัง เพื่อสอบถามปัญหา และระยะเวลาการแก้ไขที่จะสามารถกลับมาให้บริการได้ - ผู้ดูแลระบบ (Administrator) เปิดการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ รวมทั้งรายงานให้ผู้อำนวยการ ศทส. ทราบ

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
						- ศทส. ประชาสัมพันธ์ให้กับบุคลากร สคร. ได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศสามารถกลับมาใช้งานได้แล้ว
๖. เหตุการณ์อัคคีภัย	- สินทรัพย์ (Asset) ที่ย้ายไม่ทันอาจถูกไฟไหม้ - อุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) ไม่สามารถให้บริการได้	๑	๕	๕	ค่อนข้างต่ำ	<u>กรณีที่ ๑ ไฟเริ่มไหม้หรือสามารถดับไฟได้</u> - ให้ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณที่เป็นต้นเพลิงของไฟไหม้จนไฟดับและให้แจ้ง ศทส. ทราบโดยเร็ว - ผู้ดูแลระบบ (Administrator) ประเมินสถานการณ์ในเบื้องต้นว่าควรหยุดให้บริการระบบคอมพิวเตอร์และระบบสารสนเทศหรือไม่ - ถ้าหยุดให้บริการ ศทส. ประชาสัมพันธ์ ให้กับบุคลากร สคร. ได้รับทราบถึงการหยุดให้บริการชั่วคราวเนื่องจากเหตุไฟไหม้

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
						- ผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายในห้องศูนย์ข้อมูล (Data Center) พร้อมทั้งรายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป - หากเสียหายเล็กน้อยให้ผู้ดูแลระบบ (Administrator) ดำเนินการแก้ไขและเปิดการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ - ศทส. ประชาสัมพันธ์ให้กับบุคลากร สคร. ได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศสามารถกลับมาใช้งานได้แล้ว

/ตาราง (ต่อ)..

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
						- หากเสียหายมาก ให้ผู้ดูแลระบบ (Administrator) รายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป <u>กรณีที่ ๒ ไฟไหม้เริ่มลุกลามถึงขั้นรุนแรง</u> - ให้ผู้พบเหตุโทรแจ้งหน่วยดับเพลิงเป็นลำดับแรก และแจ้งให้ ศทส. ทราบโดยเร็ว - ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณไฟที่เริ่มลุกลามและบริเวณโดยรอบ หากไม่สามารถระงับเหตุได้ให้ออกจากพื้นที่โดยเร็ว - ศทส. ประชาสัมพันธ์ให้กับบุคลากร สคร. ได้รับทราบถึงการหยุดให้บริการเนื่องจากเหตุไฟไหม้

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
						- หากสามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายในห้องศูนย์ข้อมูล (Data Center) พร้อมทั้งรายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป - หากไม่สามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (Administrator) รายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป

/ตาราง (ต่อ)...

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสที่เกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๗. เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง	- เช่น กรณีการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง อาจถูกปิดกั้นการเข้าออกและอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำบริเวณกระทรวงการคลัง ซึ่งส่งผลกระทบต่อห้องศูนย์ข้อมูล (Data Center) หรือสถานที่ปฏิบัติงานบริเวณอาคารธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย	๓	๔	๑๒	ค่อนข้างสูง	- ถ้าเกิดเหตุการณ์ไฟฟ้าดับ ให้ดำเนินการตามแนวทางแก้ไขข้อ ๕ - กำหนดให้ผู้ใช้งาน (User) ปฏิบัติงานจากสถานที่ปฏิบัติงานสำรองหรือที่พักอาศัย ตามที่ สคร. กำหนด

หมายเหตุ เกณฑ์การประเมินการให้คะแนนโอกาสที่จะเกิดและผลกระทบ

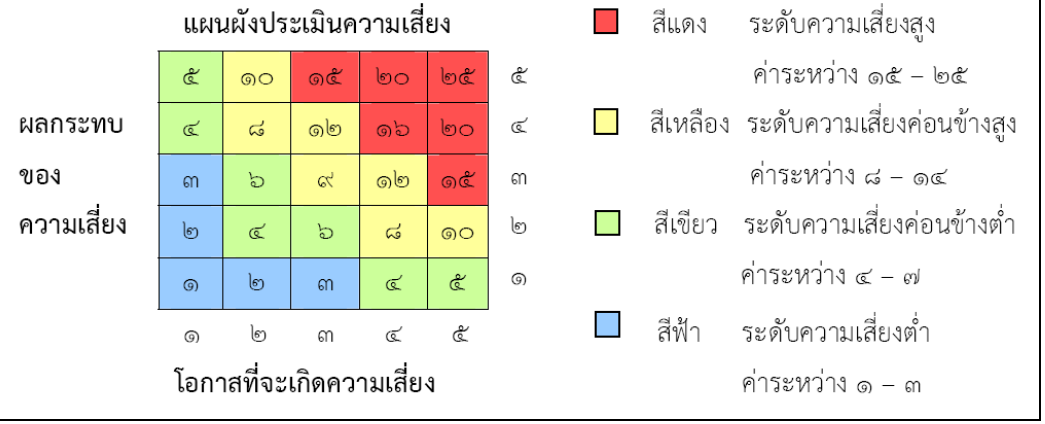
ระดับ ๑ = รุนแรงน้อยที่สุด / โอกาสเกิดน้อยที่สุด

ระดับ ๒ = รุนแรงน้อย / โอกาสเกิดน้อย

ระดับ ๓ = รุนแรงปานกลาง / โอกาสเกิดปานกลาง

ระดับ ๔ = รุนแรงมาก / โอกาสเกิดมาก

ระดับ ๕ = รุนแรงมากที่สุด / โอกาสเกิดมากที่สุด



/๖. การเตรียม...

๖. การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต

เนื่องจากเหตุการณ์ที่เป็นความเสี่ยงด้านสารสนเทศข้างต้น ศทส. จึงได้ดำเนินการจัดทำแนวทางการเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต เพื่อป้องกันภัยจากเหตุการณ์หรือภัยที่จะเกิดขึ้น ดังนี้

๖.๑ เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร. มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๑.๑ กำหนดให้ปฏิบัติตามประกาศ สคร. เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๖.๑.๒ การสร้างความรู้ความเข้าใจในการใช้ระบบคอมพิวเตอร์และระบบสารสนเทศเบื้องต้น โดยการจัดอบรมให้กับบุคลากร สคร. หรือส่งไปอบรมร่วมกับหน่วยงานภายนอกที่จัดขึ้น เพื่อลดความเสี่ยงด้านสารสนเทศ

๖.๑.๓ มีการประชาสัมพันธ์ให้ความรู้แก่บุคลากรผ่านช่องทางสื่อสารต่างๆ ตามความเหมาะสม เช่น ผ่านระบบ Web Portal ติดบอร์ดประชาสัมพันธ์ Line, G - Chat, Facebook ของ สคร. เป็นต้น

๖.๒ เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๒.๑ ติดตั้งและใช้งาน Firewall เพื่อป้องกันการบุกรุกจากผู้ไม่ประสงค์ดีต่อระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device)

๖.๒.๒ ติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๖.๓ เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๓.๑ มีมาตรการควบคุมการเข้า - ออกห้องศูนย์ข้อมูล (Data Center) ดังนี้

(๑) ปฏิบัติตามหลักเกณฑ์สำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center) ตามที่ ศทส. กำหนด

(๒) การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจาก ศทส. ก่อนเริ่มดำเนินการทุกครั้ง

(๓) ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับอนุญาตจาก ศทส.

(๔) ผู้ใช้งาน (User) หรือบุคคลภายนอก ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน โดยมีผู้ดูแลระบบ (Administrator) ควบคุมการปฏิบัติงานของผู้ใช้งาน (User) หรือบุคคลภายนอกตลอดเวลา และต้องไม่นำอาหาร หรือเครื่องดื่มเข้าไปในห้องศูนย์ข้อมูล (Data Center) และห้ามสูบบุหรี่ในห้องศูนย์ข้อมูล (Data Center)

(๕) มีเจ้าหน้าที่รักษาความปลอดภัยตลอด ๒๔ ชั่วโมง

(๖) มีการติดตั้งระบบควบคุมการเข้าถึง (Access Control) ห้องศูนย์ข้อมูล (Data Center) ด้วยระบบอิเล็กทรอนิกส์

(๗) มีการติดตั้งกล้องวงจรปิดบันทึกเหตุการณ์บริเวณทางเข้าและภายในห้องศูนย์ข้อมูล (Data Center) เพื่อเฝ้าระวังเหตุการณ์หรือภัยที่จะเกิดขึ้น

/๖.๔ เหตุการณ์...

๖.๔ เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๔.๑ มีการตรวจความพร้อมอุปกรณ์ประมวลผลข้อมูล (Process Device) ทั้งทางกายภาพและด้านเทคนิคให้พร้อมใช้งานอยู่เสมออย่างน้อยเดือนละ ๑ ครั้ง หากพบอุปกรณ์ประมวลผลข้อมูล (Process Device) หรืออุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ชำรุดเสียหาย หรือใกล้เสื่อมสภาพการใช้งาน ให้รายงานให้ผู้อำนวยการ ศทส. ทราบ เพื่อรายงานตามลำดับชั้นและสั่งการแก้ไขด้วยการซ่อมแซมหรือจัดซื้อทดแทนต่อไป

๖.๔.๒ มีการตรวจสอบปริมาณการเข้าถึงเครือข่ายภายนอก (Internet) เพื่อสังเกตปริมาณการใช้งาน อัตราความเร็วของข้อมูล เพื่อเฉลี่ยแบนด์วิดท์ (Bandwidth) ให้ทั่วถึงทั้งองค์กร และป้องกันไม่ให้ผู้ใช้งาน (User) มีการใช้แบนด์วิดท์ (Bandwidth) มากเกินไป

๖.๕ เหตุการณ์ไฟฟ้าดับ มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

มีการติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) จำนวน ๒ เครื่อง ขนาด ๓๐ KVA และ ๒๐ KVA เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ประมวลผลข้อมูล (Process Device) โดยทั้ง ๒ เครื่อง สามารถสำรองไฟฟ้าได้เป็นเวลาประมาณ ๓๐ นาที ซึ่งเพียงพอต่อการจัดเก็บและสำรองข้อมูลสารสนเทศในกรณีที่เกิดไฟฟ้าดับ

๖.๖ เหตุการณ์อัคคีภัย มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๖.๑ มีการติดตั้งอุปกรณ์ตรวจจับควัน กรณีเกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องศูนย์ข้อมูล (Data Center) อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือน เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุทราบและเข้ามาระงับเหตุฉุกเฉินก่อนเกิดอัคคีภัยได้อย่างทันท่วงที เพราะเป็นภัยที่มีผลกระทบรุนแรงที่สุด

๖.๖.๒ มีการติดตั้งถังดับเพลิงชนิดที่ใช้สารเคมีไม่ทำอันตรายต่ออุปกรณ์ประมวลผลข้อมูล (Process Device) ไว้ในห้องศูนย์ข้อมูล (Data Center) จำนวน ๑ ถัง และหน้าห้องศูนย์ข้อมูล (Data Center) จำนวน ๒ ถัง เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุใช้ระงับเหตุก่อนไฟเริ่มลุกลามถึงขั้นรุนแรง

๖.๗ เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๖.๗.๑ ให้ผู้ใช้งาน (User) สำรองข้อมูลสารเทศส่วนตัวลงในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk

๖.๗.๒ มีเจ้าหน้าที่รักษาความปลอดภัยตลอด ๒๔ ชั่วโมง เพื่อป้องกันไม่ให้บุคคลภายนอกเข้าไปภายในห้องศูนย์ข้อมูล (Data Center) โดยไม่ได้รับอนุญาต

๖.๗.๓ ตรวจสอบการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ เพื่อให้ผู้ใช้งาน (User) ปฏิบัติงานจากภายนอก สคร. (Teleworking) โดยผ่านเครือข่ายภายนอก (Internet) ได้

/๔) ตรวจสอบ...

๖.๗.๔ ตรวจสอบความพร้อมของข้อมูลสารสนเทศที่ได้สำรองระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศที่ได้บันทึกลงในตลับเทปแม่เหล็ก (Magnetic Tape Drive) สำหรับเตรียมนำไปกู้คืน ณ ไซต์สำรอง (Disaster Recovery Site : DR Site) ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง หรือตามที่ผู้บริหารเห็นชอบ หากเกิดเหตุการณ์ฉุกเฉินในสภาวะวิกฤตจนส่งผลให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต้องปิดระบบการให้บริการถูกปิดลง

๖.๗.๕ เมื่อ ศทส. ได้รับแจ้งว่าจะเกิดเหตุชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมืองบริเวณกระทรวงการคลัง ซึ่งอาจถูกปิดกั้นการเข้าออก และอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำ ให้ผู้ดูแลระบบ (Administator) นำตลับเทปแม่เหล็ก (Magnetic Tape Drive) ที่สำรองข้อมูลไว้ไปเก็บในสถานที่ปลอดภัย

๗. กลยุทธ์ความต่อเนื่องในสภาวะวิกฤต

หากเหตุการณ์หรือภัยได้เกิดขึ้นแล้ว ต้องมีการดำเนินกลยุทธ์ความต่อเนื่องในสภาวะวิกฤต เพื่อให้การปฏิบัติงานของบุคลากร สคร. ดำเนินการไปได้อย่างต่อเนื่องหรือได้รับผลกระทบน้อยที่สุด ดังนี้

ทรัพยากร	กลยุทธ์ความต่อเนื่อง
๑. สถานที่ปฏิบัติงาน อาคารธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย	๑. กำหนดพื้นที่ปฏิบัติงานสำรอง ได้แก่ ห้องคอมพิวเตอร์หรือพื้นที่อื่นๆ ของกรมบัญชีกลาง โดยประสานงานและสำรวจความเหมาะสมของสถานที่ร่วมกับกรมบัญชีกลาง ๒. ประสานขอใช้พื้นที่กับส่วนราชการหรือรัฐวิสาหกิจเป็นสถานที่ปฏิบัติงานสำรองเพิ่มเติม ๓. หากพื้นที่ปฏิบัติงานสำรองมีพื้นที่จำกัด หรืออาจเกิดอันตรายระหว่างเดินทางไปปฏิบัติงาน ให้บุคลากร สคร. ปฏิบัติงานจากที่พักอาศัย
๒. วัสดุอุปกรณ์	๑. จัดหาเครื่องคอมพิวเตอร์สำรองพร้อมอุปกรณ์ในการเข้าถึงระบบเครือข่าย เพื่อให้ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศได้ ๒. จัดเตรียมอุปกรณ์สารสนเทศสำหรับนำมาใช้ในการปฏิบัติงาน เช่น เครื่องพิมพ์ (Printer) เครื่องสแกนเนอร์ (Scaner) และสายเชื่อมต่อระบบเครือข่ายเฉพาะที่ (Lan) ๓. ผู้ใช้งาน (User) สามารถใช้คอมพิวเตอร์แบบพกพาส่วนตัวในการปฏิบัติงานได้

/ตาราง (ต่อ)...

ทรัพยากร	กลยุทธ์ความต่อเนื่อง
๓. ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ	๑. ระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศได้ติดตั้งและจัดเก็บไว้ใน ณ ห้องศูนย์ข้อมูล (Data Center) อาคารกรมบัญชีกลาง ๓ ชั้น ๖ ซึ่งรองรับการเข้าถึงจากภายนอก โดยการรับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) และมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL) ๒. ประสานศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เพื่อจัดเตรียมไซต์สำรอง (Disaster Recovery Site : DR Site) เมื่อเกิดเหตุฉุกเฉินหรือสภาวะวิกฤต ๓. ศทส. พิจารณาและนำตลับเทปแม่เหล็ก (Magnetic Tape Drive) ที่สำรองระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ ณ ห้องศูนย์ข้อมูล (Data Center) ไปไว้ในสถานที่ปลอดภัย ๔. สำหรับระบบ GFMIS - SOE ซึ่งเป็นระบบสารสนเทศตามภารกิจหลักเพื่อบริการแก่บุคลากร สคร. หน่วยงานรัฐวิสาหกิจ และส่วนราชการที่เกี่ยวข้อง ได้ติดตั้ง ณ ศูนย์คอมพิวเตอร์พิบูลสงคราม และศูนย์คอมพิวเตอร์สำรองบางบัวทอง ๕. ให้ผู้ใช้งาน (User) สำรองข้อมูลสารสนเทศที่จำเป็นและสำคัญไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk
๔. บุคลากร สคร.	๑. หากผู้ดูแลระบบ (Administrator) มีจำนวนไม่เพียงพอต่อการปฏิบัติหน้าที่ให้ผู้รับจ้างที่ดูแลระบบคอมพิวเตอร์และระบบสารสนเทศให้การสนับสนุนด้านเทคนิค ๒. อนุญาตให้ผู้ใช้งาน (User) ปฏิบัติงานจากภายนอก สคร. (Teleworking) โดยเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านระบบคอมพิวเตอร์ลูกข่ายแบบเสมือน (Virtualization System)
๕. ผู้รับบริการและผู้ที่เกี่ยวข้อง	๑. แจ้งสถานที่การติดต่อราชการสำรองผ่านทางหน้าเว็บไซต์ของ สคร. ๒. บุคลากร สคร. ที่มีหน้าที่ปฏิบัติงานร่วมกับรัฐวิสาหกิจ ให้ประสานงานทางโทรศัพท์เคลื่อนที่หรือจดหมายอิเล็กทรอนิกส์ (E - Mail) หรือหากระบบคอมพิวเตอร์และระบบสารสนเทศอยู่ระหว่างดำเนินการกู้คืน ให้พิจารณาใช้จดหมายอิเล็กทรอนิกส์ (E - Mail) จากภายนอกที่มีความน่าเชื่อถือ

/๘. ระยะ...

๘. ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต

จากการวิเคราะห์ผลกระทบจากความเสี่ยงในข้อ ๕ เพื่อให้บุคลากรสามารถปฏิบัติงานด้วยความต่อเนื่อง จึงกำหนดระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต ดังนี้

กระบวนงาน	ระดับผลกระทบ	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต		
		ภายใน ๑ วัน	ภายใน ๗ วัน	มากกว่า ๗ วัน
๑. เหตุการณ์หรือภัยที่เกิดจากบุคลากร สคร.	ค่อนข้างต่ำ	✓		
๒. เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี	ค่อนข้างสูง		✓	
๓. เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device)	ค่อนข้างต่ำ		✓	
๔. เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค	ค่อนข้างต่ำ		✓	
๕. เหตุการณ์ไฟฟ้าดับ	ค่อนข้างสูง	✓		
๖. เหตุการณ์อัคคีภัย	ค่อนข้างต่ำ			✓
๗. เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ	ค่อนข้างสูง		✓	

๙. โครงสร้างและทีมบริหารความต่อเนื่อง (BCP Team)

เพื่อให้แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ จึงต้องมีการจัดตั้งทีมบริหารความต่อเนื่อง (BCP Team) ซึ่งประกอบด้วยผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) ผู้อำนวยการ ศทส. และบุคลากรของ ศทส. เนื่องจากมีความรู้ความสามารถด้านระบบคอมพิวเตอร์และระบบสารสนเทศ ประกอบกับปฏิบัติหน้าที่เป็นผู้ดูแลระบบ (Administrator) ของ สคร.

/๙.๑ หน้าที่...

๙.๑ หน้าที่ความรับผิดชอบทีมบริหารความต่อเนื่อง (BCP Team) ดังนี้

๙.๑.๑ หัวหน้าทีมและรองหัวหน้าทีม มีหน้าที่ในการพิจารณาแนวทางการแก้ไขปัญหา กำหนดขอบเขต และสั่งการให้ผู้ที่รับผิดชอบดำเนินการแก้ไข พร้อมทั้งรายงานให้คณะผู้บริหารระดับสูง สคร. ได้รับทราบ

๙.๑.๒ ผู้ประสานงาน มีหน้าที่ในการติดต่อประสานงานภายในและหน่วยงานภายนอก สคร. และจัดเตรียมเอกสารข้อมูลที่เกี่ยวข้อง รวมถึงจัดทำรายงานในแต่ละสถานการณ์

๙.๑.๓ ผู้ดูแลระบบ (Administrator) มีหน้าที่การพัฒนาและบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนการรักษาความมั่นคงปลอดภัย ดูแลสิทธิของผู้ใช้งาน (User) แก้ไขปัญหาการใช้งาน และดูแลห้องศูนย์ข้อมูล (Data Center)

๙.๒ รายชื่อทีมบริหารความต่อเนื่อง (BCP Team) และหน้าที่ความรับผิดชอบ

ชื่อ	บทบาท	โทรศัพท์
นางสาวรสา กาญจนสาย	หัวหน้าทีมบริหารความต่อเนื่อง (BCP Team)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๓๓๐๐ - ๐๘๑ ๘๕๔ ๙๓๓๑
นางสาวภัทรา นิยะถิระกุล	รองหัวหน้าทีมบริหารความต่อเนื่อง (BCP Team)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๗๕ - ๐๘๑ ๘๑๕ ๔๕๓๓
นายกรินทร์ ศิริพัฒน์พิบูลย์	ผู้ดูแลระบบ (Administrator) (บุคลากรหลัก)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๗๓ - ๐๘๑ ๙๓๐ ๕๓๖๐
นายโชคชัย อภัยโส		- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๘๔ - ๐๘๑ ๒๗๙ ๙๗๐๘
นายณัฐพล จรัสดำรงนิตย์	ผู้ดูแลระบบ (Administrator) (บุคลากรสำรอง)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๘๒ - ๐๘๓ ๘๕๑ ๓๓๖๐
นายวันชัย เพ็งจางค์		- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๘๐ - ๐๘๔ ๐๘๓ ๕๙๙๕
นายณัฐวุฒิ สมภารเพียง	ผู้ประสานงาน (บุคลากรหลัก)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๘๓ - ๐๙๑ ๑๗๑ ๙๕๙๕
นางสาวจตุพร นันทพรหม	ผู้ประสานงาน (บุคลากรสำรอง)	- ๐๒ ๒๙๘ ๕๘๘๐ ต่อ ๒๑๘๓ - ๐๘๖ ๓๘๖ ๓๒๒๑

/๑๐. กระบวนการ...

๑๐. กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree)

กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree) ตามแนวทางของแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ สคร. หมายถึง ขั้นตอนการแจ้งเหตุฉุกเฉินหรือการแจ้งปัญหาระบบคอมพิวเตอร์และระบบสารสนเทศ เพื่อรายงานให้ผู้บังคับบัญชาทราบตามลำดับชั้นและสั่งการให้ผู้ที่มีหน้าที่รับผิดชอบดำเนินการแก้ไขตามระดับความรุนแรงของเหตุนั้น เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศสามารถให้บริการสนับสนุนการปฏิบัติงานแก่บุคลากร สคร. ได้อย่างต่อเนื่อง ที่กำหนดรายละเอียดไว้ตามรายชื่อทีมบริหารความต่อเนื่อง (BCP Team) และหน้าที่ความรับผิดชอบ ทั้งนี้ ในกรณีที่บุคลากรหลักในแต่ละบทบาทไม่สามารถปฏิบัติหน้าที่ได้ให้บุคลากรสำรองรับผิดชอบปฏิบัติหน้าที่แทน

๑๑. การสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ

เนื่องจากระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศส่วนใหญ่ ถูกติดตั้งและจัดเก็บบนระบบประมวลผลกลาง ณ ห้องศูนย์ข้อมูล (Data Center) ซึ่งเข้าถึงด้วยเทคโนโลยีแบบคลาวด์คอมพิวติ้ง (Cloud Computing) ซึ่งเป็นการอำนวยความสะดวกแก่ผู้ใช้งาน (User) เป็นอย่างมาก แต่ก็มีความเสี่ยงสูงมากเช่นกันเพราะเป็นลักษณะแบบรวมศูนย์กลาง ศทส. ซึ่งเป็นผู้ดูแลรับผิดชอบหลักจึงจัดทำแนวปฏิบัติการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานสามารถให้บริการได้อย่างต่อเนื่อง และสามารถกู้คืนกลับมาใช้งานได้โดยเร็วหากเกิดปัญหา

๑๑.๑ ผู้รับผิดชอบ

รายละเอียดบุคลากรและหน้าที่ความรับผิดชอบ ตามข้อ ๙

๑๑.๒ แนวปฏิบัติในการดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนอุปกรณ์ประมวลผลข้อมูล (Process Device)

ศทส. มอบหมายให้ผู้ดูแลระบบ (Administrator) ดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนให้ตรวจสอบอุปกรณ์ประมวลผลข้อมูล (Process Device) ณ ห้องศูนย์ข้อมูล (Data Center) อย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง หากพบข้อผิดพลาดให้รายงาน ศทส. โดยทันที

๑๑.๓ แนวปฏิบัติในการสำรองข้อมูลสารสนเทศ กำหนดดังนี้

๑๑.๓.๑ ผู้ดูแลระบบ (Administrator) ต้องดำเนินการสำรองข้อมูลสารสนเทศไว้ในตลับเทปแม่เหล็ก (Magnetic Tape Drive) ตามขั้นตอนของโปรแกรม Symantec NetBackup

๑๑.๓.๒ ผู้ดูแลระบบ (Administrator) ต้องพิมพ์รายละเอียดไว้บนตลับเทปแม่เหล็ก (Magnetic Tape Drive) ที่ใช้สำหรับการสำรองข้อมูล ได้แก่ รูปแบบการสำรองข้อมูลแบบรายวันหรือรายสัปดาห์หรือรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล

/๑๑.๓.๓ รายละเอียด...

๑๑.๓.๓ รายละเอียดการสำรองข้อมูล กำหนดดังนี้

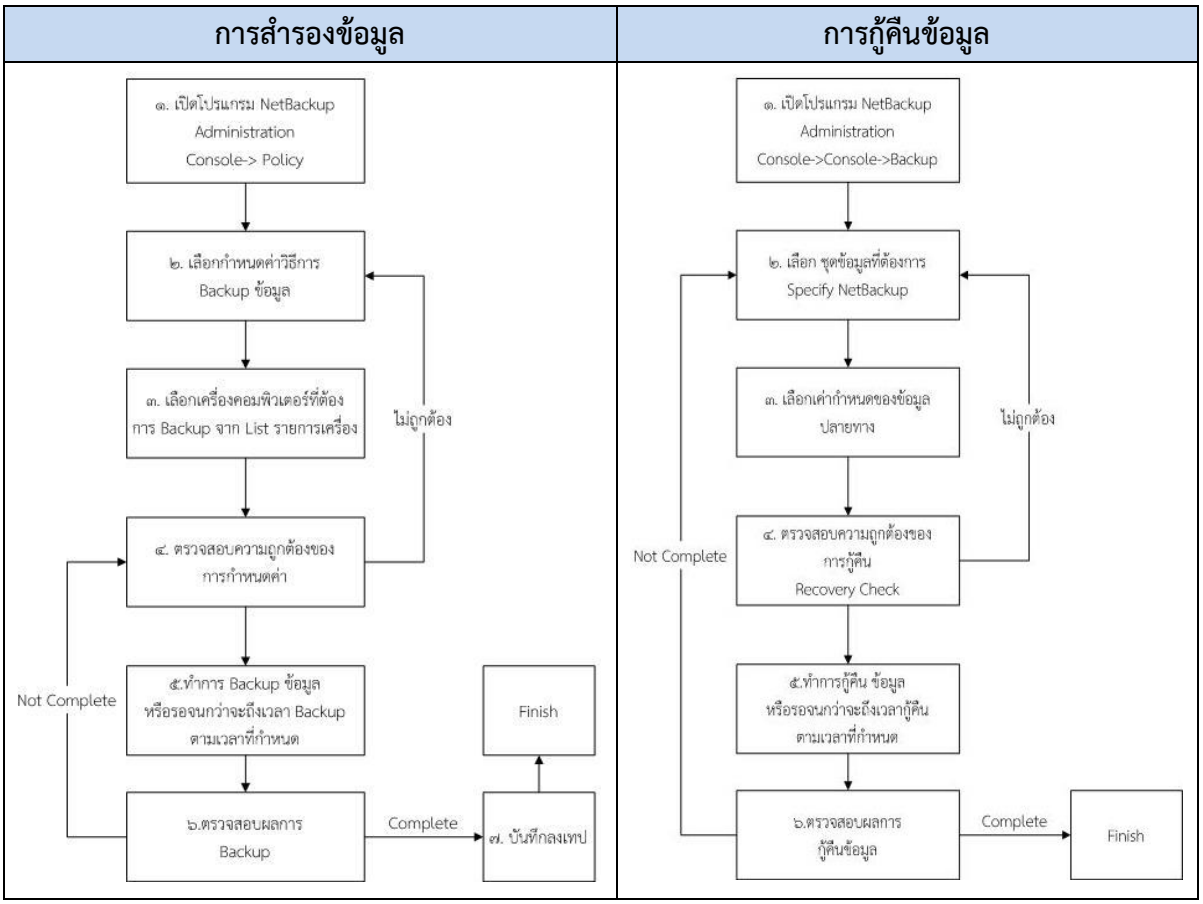
ลำดับ	รายการ	จำนวน (หน่วย)	ข้อมูลที่สำรอง
๑	เครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับประมวลผลระบบเครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน (VDI)	๔ เครื่อง	ค่า Configuration
๒	เครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน (VDI) สำหรับประมวลผลระบบสารสนเทศ	๓๖ เครื่อง	Full
๓	เครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับประมวลผลระบบเครื่องคอมพิวเตอร์ลูกข่ายแบบเสมือน (VDI)	๑๒ เครื่อง	ค่า Configuration
๔	เครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน สำหรับประมวลผลระบบคอมพิวเตอร์เครื่องลูกข่ายแบบเสมือน (VDI)	๖ เครื่อง	Full
๕	ระบบคอมพิวเตอร์เครื่องลูกข่ายแบบเสมือน (VDI)	๒๐๐ เครื่อง	Drive Z

๑๑.๔ แนวปฏิบัติการกู้คืนระบบ

หากระบบคอมพิวเตอร์และระบบสารสนเทศเกิดปัญหาไม่สามารถใช้งานได้ หรือข้อมูลสารสนเทศสูญหาย ให้ผู้ดูแลระบบ (Administrator) ดำเนินการกู้คืนข้อมูลสารสนเทศที่สำรองไว้ในตลับเทปแม่เหล็ก (Magnetic Tape Drive) เพื่อนำข้อมูลสารสนเทศกลับมาใช้งาน

/๑๑.๕ แผนผัง...

๑๑.๕ แผนผังการสำรองและกู้คืนระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศด้วยโปรแกรม Symantec NetBackup



๑๑.๖ ศทส. ต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง ดังนี้

๑๑.๖.๑ พิจารณาคัดเลือกระบบคอมพิวเตอร์และระบบสารสนเทศที่สำคัญเพื่อดำเนินการทดสอบพร้อมทั้งเตรียมความพร้อมก่อนการทดสอบ เพื่อมิให้เกิดความเสี่ยงและความเสียหายแก่ทางราชการ

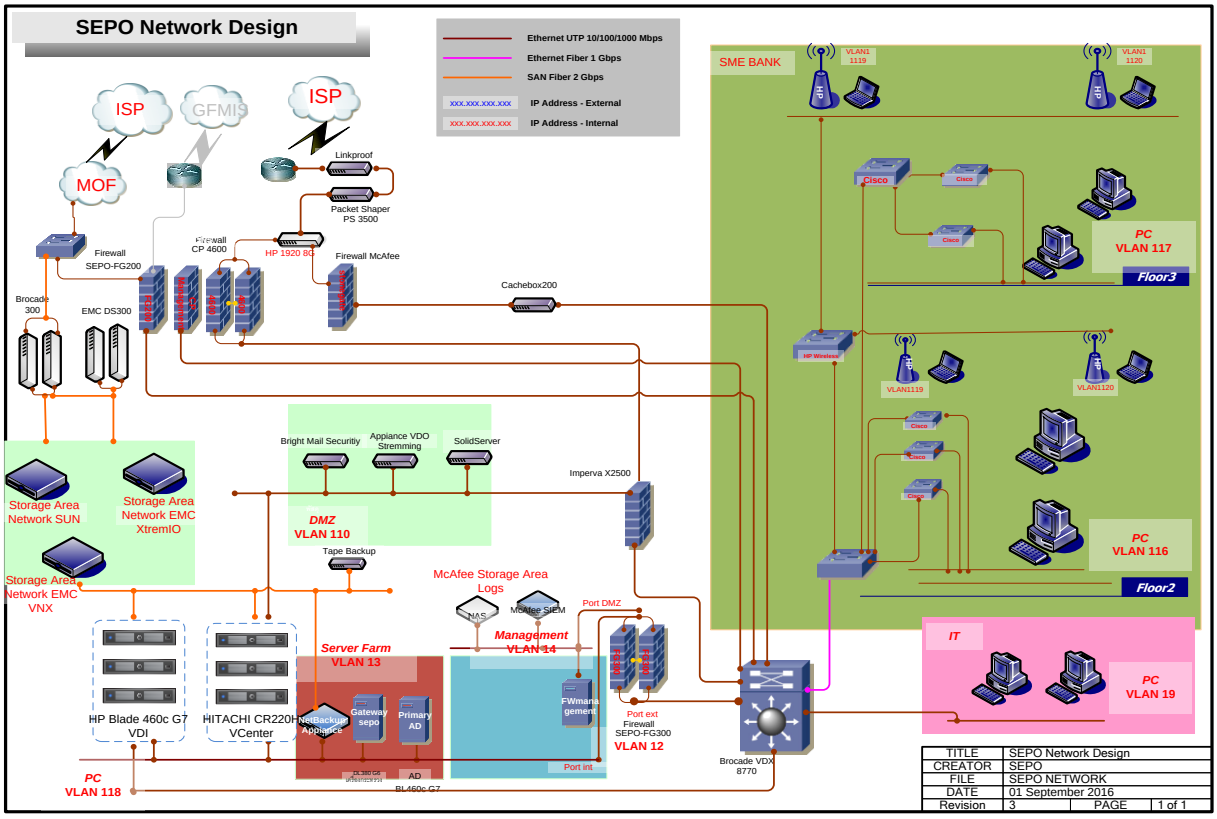
๑๑.๖.๒ จัดทำรายงานเสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ก่อนดำเนินการทดสอบ

๑๑.๖.๓ ดำเนินการทดสอบระบบคอมพิวเตอร์และระบบสารสนเทศตามที่กำหนดไว้

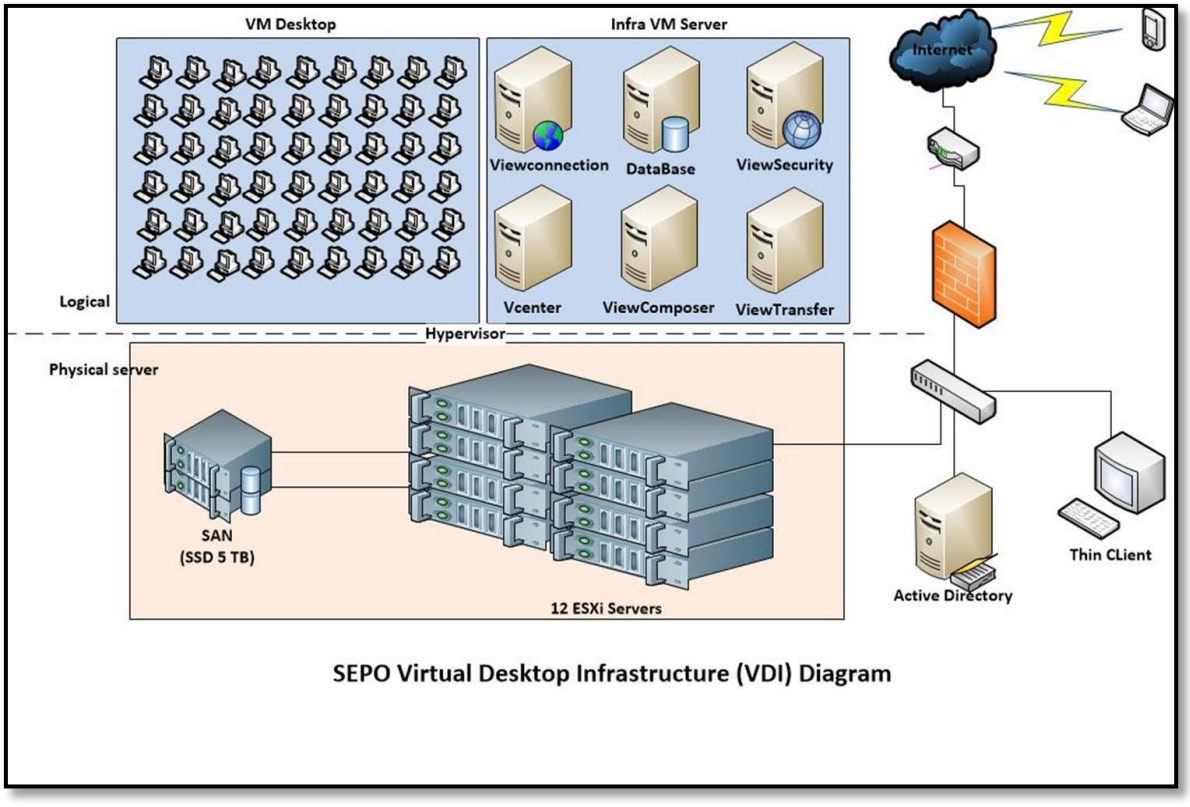
๑๑.๖.๔ รายงานผลการทดสอบเสนอผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

/ภาคผนวก...

๑. ผังแสดงสถาปัตยกรรมโครงข่ายคอมพิวเตอร์ (Network Infrastructure Diagram) ของ สคร.



๒. ผังแสดงสถาปัตยกรรมระบบเครื่องคอมพิวเตอร์ลูกข่ายเสมือน (Virtual Desktop Infrastructure : VDI)



/๓. ผู้ประสานงาน...

๓. ผู้ประสานงานภายนอก

ลำดับ	หน่วยงาน	หมายเลขโทรศัพท์
๑.	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง	๐๒ ๒๗๓ ๙๕๒๕-๖
๒.	บริษัท ทีโอที จำกัด	๐๒ ๕๗๔ ๘๘๔๘-๙ หรือสายด่วน ๑๑๐๐
๓.	บริษัท กสท โทรคมนาคม จำกัด (มหาชน)	๐๒ ๑๐๔ ๔๗๗๖ หรือสายด่วน ๑๓๒๒
๔.	สถานีดับเพลิง สำนักงานเขตพญาไท	๐๒ ๓๕๔ ๖๘๕๘ หรือสายด่วน ๑๙๙
๕.	สถานีตำรวจนครบาลเขตพญาไท	๐๒ ๓๕๔ ๖๙๕๘ หรือสายด่วน ๑๙๑