สำนักงานคณะกรรมการดิจิทัล
เพื่อเศรษฐกิจและสังคมแห่งชาติ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

ประกาศสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
พ.ศ. ๒๕๖๔
ที่ ดศ๐๐๑ / ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ พ.ศ. ๒๕๖๔"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันออกประกาศ เป็นต้นไป

ข้อ ๓ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติเป็นลายลักษณ์อักษรตามเอกสารแนบท้ายประกาศ ประกอบด้วยเนื้อหาดังต่อไปนี้

๑. วัตถุประสงค์และขอบเขต

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม (สดช.) จัดทำนโยบายนี้เพื่อเป็นส่วนหนึ่งของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ในการป้องกันภัยคุกคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้สารสนเทศมีความปลอดภัย สามารถรักษาความลับและความถูกต้องของข้อมูล และมีความพร้อมในการให้บริการอยู่ในระดับที่ยอมรับได้ สดช. จึงได้กำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศเพื่อเป็นแนวทางเสริมสร้างความมั่นคงปลอดภัยด้านสารสนเทศให้กับ สดช. หรือหน่วยงานที่มีความเกี่ยวข้องในการปฏิบัติราชการกับ สดช. โดยนโยบายนี้มีจุดประสงค์เพื่อการสนับสนุนการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. ดังนี้

- เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศของ สดช. ทำให้การปฏิบัติราชการมีประสิทธิภาพและประสิทธิผล
- เพื่อการใช้งานเป็นไปตามภารกิจของ สดช. ในการควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยให้มีการควบคุมการเข้าถึงสารสนเทศ และปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย
- เพื่อเผยแพร่ให้ **"เจ้าหน้าที่ (Officer)"** ทุกระดับใน สดช. ได้รับทราบ และทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- เพื่อให้มีการดำเนินการที่เหมาะสมและสัมฤทธิผล มีการตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง
- เพื่อสร้างความตื่นตัวให้**"เจ้าหน้าที่ (Officer)"**และ **"หน่วยงานภายนอก"** ที่ปฏิบัติงานให้กับ สดช. ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ
- เพื่อดำเนินการหรือประสานงานกับหน่วยงานอื่นๆ ทั้งภายในประเทศและต่างประเทศในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงปลอดภัย ที่เป็นประโยชน์ต่อการทำงานหรือการพัฒนาบุคลากรที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

๒. องค์ประกอบของนโยบาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. ใช้แนวทางและกระบวนการโดยอ้างอิงจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติมถึง (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี ๒๕๕๐ รายละเอียดบางส่วนจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรฐาน ISO/IEC 27001 ซึ่งประกอบด้วย ๑๑ หมวด ที่ครอบคลุมประเด็นสำคัญ ดังนี้

หมวด ๑ นโยบายความมั่นคงปลอดภัย
หมวด ๒ โครงสร้างทางด้านความมั่นปลอดภัยสำหรับองค์กร
หมวด ๓ ความมั่นคงปลอดภัยทางด้านทรัพยากรบุคคล
หมวด ๔ การบริหารจัดการสินทรัพย์
หมวด ๕ การควบคุมการเข้าถึง
หมวด ๖ การเข้ารหัสข้อมูล
หมวด ๗ ความมั่นคงปลอดภัยทางด้านกายภาพและสภาพ
หมวด ๘ ความมั่นคงปลอดภัยในการปฏิบัติงาน
หมวด ๙ ความมั่นคงปลอดภัยในการสื่อสารข้อมูล
หมวด ๑๐ การจัดหาพัฒนา และบำรุงรักษาระบบ
หมวด ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก
หมวด ๑๒ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย
หมวด ๑๓ ความมั่นคงปลอดภัยด้านการบริหารความต่อเนื่องในการดำเนินงาน
หมวด ๑๔ การปฏิบัติตามข้อกำหนด

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศแต่ละหมวดที่กล่าวมาข้างต้น จะประกอบด้วย วัตถุประสงค์ในการดำเนินการที่เกี่ยวข้องกับหมวดนั้น และมีรายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และวิธีปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของ สดช. เพื่อลดความเสียหายต่อการปฏิบัติงาน ทำให้ สดช. เป็นหน่วยงานที่ได้รับการยอมรับจากองค์กรต่างๆ ในการปฏิบัติราชการได้อย่างมั่นคงปลอดภัยสอดคล้องตามที่ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. นี้ จัดเป็นมาตรฐานด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของ สดช. ซึ่งข้าราชการ เจ้าหน้าที่ ลูกจ้างของ สดช. และบุคคลภายนอกหรือหน่วยงานภายนอก จะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑๕ มกราคม พ.ศ. ๒๕๖๔

(นางวรรณพร เทพหัสดิน ณ อยุธยา)
เลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

เอกสารแนบท้าย

ประกาศสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ พ.ศ. ๒๕๖๔

เอกสารแนบท้าย

ประกาศสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
พ.ศ. ๒๕๖๔

สารบัญ

นิยาม

"สดช."	หมายถึง	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
"ศูนย์ข้อมูลเศรษฐกิจและสังคมดิจิทัล (ขศ.)"	หมายถึง	หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายสารสนเทศภายใน สดช.
"ผู้บังคับบัญชา"	หมายถึง	ผู้มีอำนาจสั่งการตามโครงสร้างของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief of Information Officer ; CIO)"	หมายถึง	ผู้มีอำนาจสูงสุดในด้านระบบสารสนเทศของ สดช. มีบทบาทหน้าที่ในการกำหนดนโยบายและมาตรฐานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ การวางแผนแม่บทและการติดตามการพัฒนาระบบสารสนเทศ การกำกับดูแลการปฏิบัติงานสารสนเทศ การประเมินและตรวจสอบคุณภาพของงานสารสนเทศ และการรายงานผลการปฏิบัติงานสารสนเทศแก่ผู้บริหารระดับสูง
"ผู้อำนวยการศูนย์ข้อมูลเศรษฐกิจและสังคมดิจิทัล"	หมายถึง	ผู้มีอำนาจในด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สดช. ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
"การรักษาความมั่นคงปลอดภัย (IT Security)"	หมายถึง	การรักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
"มาตรฐาน (Standard)"	หมายถึง	บรรทัดฐานที่บังคับใช้ในการปฏิบัติจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย ~~ได้แก่~~ การกำหนดรหัสผ่านต้องมีความยาวไม่ต่ำกว่า ๘ ตัวอักษร เป็นต้น
"วิธีการปฏิบัติ (Procedure)"	หมายถึง	รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
"แนวทางปฏิบัติ (Guideline)"	หมายถึง	แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
"ผู้ใช้งาน (User)"	หมายถึง	บุคคลที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้งาน บริหารจัดการข้อมูลส่วนบุคคล ได้แก่ รหัสผ่าน (Password) หรือ ไฟล์งานที่ถูกสร้างขึ้น โดยมีสิทธิและหน้าที่ที่ขึ้นกับบทบาท (Role) ซึ่ง สดช.กำหนดไว้
"ผู้ดูแลระบบ (System Administrator)"	หมายถึง	เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบ และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
"เจ้าหน้าที่ (Officer)"	หมายถึง	ข้าราชการ พนักงานราชการ จ้างเหมาเอกชน เจ้าหน้าที่ประจำ

		โครงการ และที่ปรึกษาผู้เชี่ยวชาญ ของ สดช.
"หน่วยงานภายนอก (Third party)"	หมายถึง	องค์กรซึ่ง สดช. อนุญาตให้มีสิทธิในการเข้าถึงและใช้ข้อมูลหรือสินทรัพย์ต่างๆ ของ สดช. โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล
"บุคคลภายนอก (Third Person)"	หมายถึง	บุคคลที่ไม่ใช่ข้าราชการและเจ้าหน้าที่ของ สดช.
"ผู้บริหารระดับสูงสุด"	หมายถึง	เลขาธิการ สดช.
"ผู้บริหารระดับสูง (Top Management Level)"	หมายถึง	ผู้บริหารระดับสูง ได้แก่ รองเลขาธิการ สดช.ผู้ตรวจราชการ สดช. เป็นต้น
ผู้บริหารระดับสูงด้านสารสนเทศ (CIO)	หมายถึง	ผู้บริหารระดับสูงด้านสารสนเทศที่มีอำนาจหน้าที่ในการตัดสินใจด้านสารสนเทศ
"ผู้บริหารระดับกลาง (Middle Management Level)"	หมายถึง	ผู้อำนวยการกอง/ศูนย์
"ผู้บริหารระดับต้น (Management Level) "	หมายถึง	ผู้อำนวยการกลุ่มงาน
"สิทธิของผู้ใช้งาน"	หมายถึง	สิทธิที่เกี่ยวข้องกับระบบสารสนเทศของ สดช. รวมถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ
"เจ้าของข้อมูลและสารสนเทศ (Data and Information Owner) "	หมายถึง	ผู้ที่เป็นผู้สร้างข้อมูลและสารสนเทศซึ่งมีหน้าที่ ● กำหนดการจัดระดับชั้นความลับ และจัดทำ label ให้แก่ข้อมูลนั้นๆ ● อนุญาตให้ผู้ใช้งานเข้าใช้ข้อมูลนั้นๆ ● ทำการควบคุมตามที่กำหนดไว้ในแนวทางการจัดระดับชั้นความลับ
"เจ้าของระบบสารสนเทศ (System Owner)"	หมายถึง	ผู้ที่มีหน้าที่ดูแลและบริหารจัดการระบบสารสนเทศ ของตนเอง
"ผู้ส่งข้อมูลและสารสนเทศ (Data and Information Sender)"	หมายถึง	เจ้าของข้อมูลและสารสนเทศ และ/หรือ ผู้ที่ได้รับอนุญาตจากเจ้าของข้อมูลและสารสนเทศให้ใช้ข้อมูลได้ ที่ต้องการส่งข้อมูลและสารสนเทศไปยังบุคคลภายใน / บุคคลภายนอก สดช.
"ความมั่นคงปลอดภัยด้านสารสนเทศ (Information security)"	หมายถึง	การธำรงไว้ ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)
"ข้อมูลคอมพิวเตอร์	หมายถึง	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ใน

(Computer Data)"		ระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตาม พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และฉบับแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑
"สารสนเทศ (Information)"	หมายถึง	ข้อเท็จจริงที่ได้จากข้อมูลคอมพิวเตอร์นำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ"	หมายถึง	การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตหน่วยงานภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
"ระบบคอมพิวเตอร์ (Computer System)"	หมายถึง	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มี การกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
"ระบบเครือข่าย (Network System)"	หมายถึง	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของ สดช. ได้แก่ ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น
"ระบบ LAN (Local Area Network) และ "ระบบอินทราเน็ต (Intranet)"	หมายถึง	หมายถึงระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานของ สดช. เข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศ ภายในหน่วยงาน
"ระบบอินเทอร์เน็ต (Internet)"	หมายถึง	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของ สดช. เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
"ระบบเทคโนโลยีสารสนเทศ (Information Technology System)"	หมายถึง	ระบบงานของ สดช. ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่ สดช. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหารการสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) โปรแกรม (Software) ข้อมูล (Data) สารสนเทศ (Information) เป็นต้น
"พื้นที่ใช้งานระบบ	หมายถึง	พื้นที่ที่ สดช. อนุญาตให้มีการใช้งานระบบเทคโนโลยี

เทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspaces)"		สารสนเทศและการสื่อสาร โดยแบ่งเป็น ● พื้นที่ทำงานทั่วไป ● พื้นที่ทำงานของผู้ดูแลระบบ ● พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย ● พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์
"เจ้าของข้อมูล (Data Owner)"	หมายถึง	ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหายหรือเสียหาย
"เจ้าของระบบงาน (System Owner)"	หมายถึง	ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลและพัฒนาระบบ ของ สดช.
"สินทรัพย์ (Asset)"	หมายถึง	สินทรัพย์ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สดช. ได้แก่ อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
"จดหมายอิเล็กทรอนิกส์ (e-mail)"	หมายถึง	ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง
"ที่อยู่จดหมายอิเล็กทรอนิกส์" (E-mail address)	หมายถึง	ชุดอักขระที่ระบุเฉพาะเจาะจงถึงตำแหน่งที่อยู่ของตู้ไปรษณีย์ของผู้ที่ใช้จดหมายอิเล็กทรอนิกส์ ซึ่งจะประกอบด้วยชื่อของบุคคล ได้แก่ info และตามด้วยสัญลักษณ์ @ และชื่อของโดเมน (Domain name) ได้แก่ info@onde.go.th
"รหัสผ่าน (Password)"	หมายถึง	เครื่องมือรักษาความปลอดภัยที่ประกอบด้วยชุดของตัวอักษร ซึ่งใช้ตรวจสอบสิทธิในการเข้าถึงระบบแก่ผู้ใช้แต่ละคน เพื่อแสดงรับรองความถูกต้องแท้จริง (Authentication) ของผู้ใช้
"ชุดคำสั่งไม่พึงประสงค์ (Malicious Code)"	หมายถึง	ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
"ช่องโหว่ (Vulnerability)"	หมายถึง	ช่องทางของระบบซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้
"ความเสี่ยง (Risk)"	หมายถึง	โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ ที่ไม่พึงประสงค์ที่ทำให้ระบบสารสนเทศไม่สามารถทำงานได้ตามวัตถุประสงค์
"มัลแวร์ (Malware)"	หมายถึง	โปรแกรมคอมพิวเตอร์สร้างขึ้นมาเพื่อให้เกิดความเสียหายหรือรบกวนการทำงานของระบบ ทำให้ข้อมูลรั่วไหล เปิดช่องให้มีผู้บุกรุกเข้ามาหรือสร้างความเดือดร้อนรำคาญ ได้แก่ ไวรัส

		คอมพิวเตอร์ (Computer Virus) หนอนคอมพิวเตอร์ (Computer Worm) ม้าโทรจัน (Trojan Horse) โปรแกรมเข้ารหัสไฟล์คอมพิวเตอร์เพื่อเรียกค่าไถ่ (Ransomware) เป็นต้น
"แชร์แวร์ (Shareware)"	หมายถึง	โปรแกรมที่ผู้ผลิตหรือผู้ที่ได้ลิขสิทธิ์โปรแกรมนั้นๆ ยินยอมให้สามารถทดลองใช้โปรแกรม ซึ่งอาจจะใช้งานได้ครบตามความสามารถทั้งหมดของโปรแกรมหรือเพียงบางส่วน แต่มีกำหนดระยะเวลาหรือจำนวนการใช้งาน เมื่อครบตามที่ได้ตกลงกันไว้ ก็ไม่สามารถใช้โปรแกรมได้ ต้องสั่งซื้อโปรแกรมจากผู้ผลิตเพื่อใช้งานต่อไป
"ฟรีแวร์ (Freeware)"	หมายถึง	โปรแกรมที่ผู้ผลิตหรือผู้ที่ได้ลิขสิทธิ์โปรแกรมนั้นๆ ยินยอมให้มีการคัดลอก และนำไปใช้ได้โดยไม่คิดค่าใช้จ่าย
"ชุดคำสั่งต้นฉบับ (Source Code)"	หมายถึง	เป็นชุดคำสั่งที่ใช้สั่งงานคอมพิวเตอร์หรือภาษาในโปรแกรมคอมพิวเตอร์โดยปกติจะเป็นข้อความ (Text) ที่มนุษย์สามารถอ่านเข้าใจได้ เมื่อคอมพิวเตอร์ได้รับคำสั่งจาก Source Code คอมพิวเตอร์ก็จะทำการแปลงเป็นภาษาที่คอมพิวเตอร์เข้าใจโดยใช้ Interpreter หรือ Compiler ในการแปลง
"โอเพนซอร์ส (Open Source)"	หมายถึง	ซอฟต์แวร์ที่สามารถนำไปใช้งาน ศึกษา แก้ไข และเผยแพร่ได้อย่างเสรี ปราศจากเงื่อนไขเพิ่มเติม การพัฒนาที่เปิดเผย Source Code ให้สาธารณะนำไปพัฒนาต่อยอดได้ ทำให้เกิดการร่วมมือกันทำงานอย่างไร้พรมแดนผ่านเครือข่ายอินเทอร์เน็ต
"หน่วยงานดูแลรับผิดชอบด้านตรวจสอบภายใน"	หมายถึง	หน่วยงานของ สดช. ที่มีหน้าที่รับผิดชอบในการสอบทานให้ดำเนินไปภายใต้มาตรฐานและแนวทางการปฏิบัติที่ได้กำหนดไว้ในนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. โดยหน่วยงานที่รับผิดชอบคือ กลุ่มงานตรวจสอบภายใน ของ สดช.
"หน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง"	หมายถึง	หน่วยงานของ สดช. ที่มีหน้าที่รับผิดชอบในการวิเคราะห์และประเมินความเสี่ยงระบบสารสนเทศของ สดช. ที่เกี่ยวกับการบริหารงานราชการ เพื่อให้ สดช. มีคุณภาพ ประสิทธิภาพในการปฏิบัติราชการมากยิ่งขึ้น และลดโอกาสความเสียหายที่อาจจะเกิดขึ้นได้ โดยหน่วยงานที่รับผิดชอบคือ ศูนย์ข้อมูลเศรษฐกิจและสังคมดิจิทัล (ขศ.) ของ สดช.
"หน่วยงานดูแลรับผิดชอบด้านกฎหมาย"	หมายถึง	หน่วยงานของ สดช. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการดำเนินการยกร่างกฎหมาย พิจารณา และให้คำปรึกษาตอบข้อหารือที่เกี่ยวกับกฎหมาย ระเบียบ คำสั่ง บันทึกสั่งการดำเนินการเกี่ยวกับนิติกรรมของ สดช. ดำเนินการบอกกล่าวทวงถาม รวบรวมพยานหลักฐานเพื่อดำเนินคดี ดำเนินการสอบสวนข้อเท็จจริงและหาผู้รับผิดทางแพ่ง ให้คำปรึกษาทางกฎหมายแก่"เจ้าหน้าที่"ของ สดช. ตลอดจนประสานงานกับ

		หน่วยงานต่างๆ ในเรื่องที่เกี่ยวข้อง) โดยหน่วยงานที่รับผิดชอบคือ กองกฎหมาย (กม.) ของ สดช.
"หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ"	หมายถึง	หน่วยงานของ สดช. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการกำหนดนโยบายและแนวทางปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ติดต่อประสานงานความร่วมมือทางด้านความมั่นคงปลอดภัยระหว่างองค์กร วางแผนควบคุมระบบความมั่นคงปลอดภัยด้านสารสนเทศและการเตือนภัย รวมถึงวิเคราะห์หาวิธีการแก้ไขช่องโหว่ของระบบสารสนเทศ และรายงานเกี่ยวกับการฝ่าฝืนนโยบายดังกล่าวไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) โดยหน่วยงานที่รับผิดชอบคือ ศูนย์ข้อมูลเศรษฐกิจและสังคมดิจิทัล (ขศ.) ของ สดช.
"หน่วยงานดูแลรับผิดชอบการบริหารงานบุคคลและสวัสดิการ"	หมายถึง	หน่วยงานของ สดช. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการสรรหาเจ้าหน้าที่ใหม่ การตรวจสอบคุณสมบัติของผู้สมัคร การกำหนดเงื่อนไขการจ้างงาน การลงนามมิให้เปิดเผยความลับของ สดช. รวมทั้งการรายงานเกี่ยวกับการจ้างงาน การเปลี่ยนแปลงสภาพการจ้างงาน การลาออกจากงาน การถึงแก่กรรม การโยกย้าย และการพักงานหรือการลงโทษทางวินัย ให้แก่หน่วยงานที่รับผิดชอบระบบสารสนเทศทราบ โดยหน่วยงานที่รับผิดชอบคือ สำนักงานเลขาธิการ (สลธ.) ของ สดช.
"หน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร"	หมายถึง	หน่วยงานของ สดช. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการจัดการประชุม สัมมนา หรืออบรมให้ความรู้แก่บุคลากรใหม่และผู้ใช้งาน เกี่ยวกับวิธีปฏิบัติงาน เพื่อสร้างความมั่นคงปลอดภัยให้กับสารสนเทศของ สดช. โดยหน่วยงานที่รับผิดชอบคือ สำนักงานเลขาธิการ (สลธ.) ของ สดช.
"หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่"	หมายถึง	หน่วยงานของ สดช. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ควบคุมการเข้า-ออกอาคารและสำนักงาน จัดเตรียมการป้องกันต่อภัยคุกคามต่างๆ ทั้งจากมนุษย์และธรรมชาติ ได้แก่ ไฟไหม้ น้ำท่วม เป็นต้น โดยหน่วยงานที่รับผิดชอบคือ สำนักงานเลขาธิการ (สลธ.) ของ สดช.
"หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและสินทรัพย์ที่เป็นซอฟต์แวร์"	หมายถึง	หน่วยงานของ สดช. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการจัดการข้อมูลและสินทรัพย์ที่เป็นซอฟต์แวร์ โดยหน่วยงานที่รับผิดชอบคือ ศูนย์ข้อมูลเศรษฐกิจและสังคมดิจิทัล (ขศ.) ของ สดช.
"หน่วยงานที่รับผิดชอบอุปกรณ์สำคัญของระบบสารสนเทศ"	หมายถึง	หน่วยงานของ สดช. ที่มีอุปกรณ์สำคัญของระบบสารสนเทศและมีห้อง Server/Data Center ในความดูแล หน้าที่รับผิดชอบดูแลอุปกรณ์สำคัญของระบบสารสนเทศที่ครอบครองอยู่
"การบริหารจัดการเปลี่ยนแปลง (Change	หมายถึง	การเปลี่ยนแปลงระบบสารสนเทศ หรือระบบงานทางราชการซึ่งการเปลี่ยนแปลงดังกล่าวจะมีผลกระทบต่อฮาร์ดแวร์

Management)"		ซอฟต์แวร์ระบบ (System Software) โปรแกรมประยุกต์ (Application Software) ระบบเครือข่าย เป็นต้น
"เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event)"	หมายถึง	สภาพของการให้บริการหรือ การแจ้งเตือนของระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident)"	หมายถึง	สถานการณ์ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
"ข้อมูลและสารสนเทศที่กำหนดชั้นความลับ (Confidential Data and Information)"	หมายถึง	ข้อมูลและสารสนเทศที่มีความสำคัญ และเป็นความลับทางราชการ ซึ่งถ้าหากถูกเปิดเผยออกไปแล้ว จะเกิดความเสียหายหรือเกิดผลเสียอื่นๆ ต่อหน่วยงานภาครัฐ ซึ่ง สดช. ได้กำหนดชั้นความลับตามความสำคัญของเนื้อหา การจำกัดการเข้าถึงและจำกัดให้ทราบเท่าที่จำเป็น สอดคล้องกับ "ระเบียบ ว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔" โดยได้กำหนดชั้นความลับของข้อมูลและสารสนเทศไว้ ๓ ระดับ คือ ชั้นลับที่สุด ชั้นลับมาก และชั้นลับ
"ชั้นลับที่สุด" (Top Secret)	หมายถึง	ข้อมูลและสารสนเทศซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐและ สดช. อย่างร้ายแรงที่สุด "ผู้บริหาร" และ "เจ้าของข้อมูลและสารสนเทศ" เท่านั้นที่จะสามารถเข้าใช้งานข้อมูลและสารสนเทศประเภทนี้ได้ "ผู้ใช้" ที่ต้องการใช้ข้อมูลและสารสนเทศดังกล่าวจะต้องได้รับอนุญาตจาก "ผู้บริหารระดับกลาง" ของเจ้าของข้อมูลและสารสนเทศขึ้นไปเท่านั้น ตัวอย่างข้อมูลและสารสนเทศชั้นลับที่สุด ได้แก่ • รายงานเสนอการแต่งตั้ง ถอดถอนหรือโยกย้ายเจ้าหน้าที่ในตำแหน่งที่สำคัญมาก • การเจรจาข้อตกลงที่สำคัญกับหน่วยงานที่เกี่ยวข้อง • สัญญาที่ทำขึ้นระหว่างองค์กร • เทคนิคที่ต้องอาศัยความชำนาญพิเศษ • อื่นๆ ตามที่เจ้าของข้อมูลและสารสนเทศกำหนด
"ชั้นลับมาก" (Secret)	หมายถึง	ข้อมูลบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐและ สดช. อย่างร้ายแรง หากถูกเปิดเผยออกไปหรือสูญหายจะก่อให้เกิดผลกระทบต่อประสิทธิภาพในการปฏิบัติงานของหน่วยงานราชการ อาจจะก่อให้เกิดความสูญเสียความเชื่อมั่น

		โดย "ผู้บริหาร"และ "เจ้าของข้อมูลและสารสนเทศ" เท่านั้นที่จะสามารถเข้าใช้งานข้อมูลและสารสนเทศประเภทนี้ได้ "ผู้ใช้" ที่ต้องการใช้ข้อมูลและสารสนเทศดังกล่าว จะต้องได้รับอนุญาตจาก "ผู้บริหารระดับต้น" ของเจ้าของข้อมูลและสารสนเทศขึ้นไปเท่านั้น ตัวอย่างข้อมูลและสารสนเทศชั้นลับมาก ได้แก่ ● การดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงตำแหน่งที่สำคัญใน สดช. ● ระเบียบวาระและรายงานการประชุมลับ ● ประกาศหรือคำสั่งที่สำคัญที่อยู่ระหว่างการดำเนินการ ● อื่นๆ ตามที่เจ้าของข้อมูลและสารสนเทศกำหนด
"ชั้นลับ" (Confidential)	หมายถึง	ข้อมูลและสารสนเทศลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ของ สดช. ซึ่งไม่พึงเปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบ ในกรณี "ผู้ใช้" ที่ต้องการใช้ข้อมูลและสารสนเทศดังกล่าวจะต้องได้รับอนุญาตจาก "เจ้าของข้อมูลและสารสนเทศ" เป็นอย่างน้อย ตัวอย่างข้อมูลและสารสนเทศชั้นลับ ได้แก่ ● ขั้นตอนปฏิบัติงานภายใน สดช. ● อื่นๆ ตามที่เจ้าของข้อมูลและสารสนเทศกำหนด
ชั้นความลับของระบบสารสนเทศ	หมายถึง	ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศ ที่ต้องเก็บเป็นความลับ ได้แก่ รายชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ที่ใช้สำหรับเข้าสู่ระบบงานคอมพิวเตอร์ต่าง ๆ การตั้งค่าระบบ (Configuration) สิทธิ์ในการใช้งานระบบสารสนเทศ (Access Control list) เป็นต้น
สื่อสังคมออนไลน์ (Social Media)	หมายถึง	ช่องทางหรือสื่อใดๆ ที่ใช้เผยแพร่ข้อมูลและแสดงความคิดเห็นบนโลกออนไลน์ ที่เปิดโอกาสให้ผู้ใช้สามารถสร้างสรรค์เนื้อหาได้ด้วยตนเอง ได้แก่ บล็อกเสรี (Blog) วิกิพีเดีย (Wikipedia) พันทิป (Pantip) เว็บเครือข่ายสังคม (Social Network) ต่างๆ ได้แก่ FaceBook Twitter LinkedIn Line Instargram Flickr MySpace Multiply และ YouTube เป็นต้น
ผู้มีส่วนได้ส่วนเสีย	หมายถึง	บุคลากรภายนอก ได้แก่ ผู้รับบริการ ประชาชน ผู้ประกอบการ บุคคลทั่วไป หน่วยงานราชการ รัฐวิสาหกิจ ภาคเอกชน สดช.ระหว่างประเทศที่เกี่ยวข้อง สถานศึกษา นิสิต นักศึกษา
โพสต์ (Post)	หมายถึง	การส่งข้อความตัวอักษร ภาพ หรือคลิปวีดิโอ คลิบเสียง การถ่ายทอดสดผ่านสื่อสังคมออนไลน์ เข้าสู่สื่อออนไลน์ ได้แก่ เว็บไซต์ เพื่อแสดงความคิดเห็นหรือเผยแพร่ข้อมูลข่าวสาร

ข้อมูลส่วนบุคคล	หมายถึง	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
ไซเบอร์	หมายถึง	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป
การรักษาความมั่นคงปลอดภัยไซเบอร์	หมายถึง	มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ
ภัยคุกคามทางไซเบอร์	หมายถึง	การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ	หมายถึง	คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

หมวด ๑
นโยบายความมั่นคงปลอดภัย
(Security Policy)

๑. คำแถลงนโยบาย

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม (สดช.) จัดทำนโยบายนี้เพื่อเป็นส่วนหนึ่งของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ในการป้องกันภัยคุกคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้สารสนเทศมีความปลอดภัย สามารถรักษาความลับและความถูกต้องของข้อมูล และมีความพร้อมในการให้บริการอยู่ในระดับที่ยอมรับได้ สดช. จึงได้กำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นแนวทางเสริมสร้างความมั่นคงปลอดภัยด้านสารสนเทศให้กับ สดช. หรือหน่วยงานที่มีความเกี่ยวข้องในการปฏิบัติราชการกับ สดช. โดยนโยบายนี้มีจุดประสงค์เพื่อการสนับสนุนการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. ดังนี้

- เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศของ สดช. ทำให้การปฏิบัติราชการมีประสิทธิภาพและประสิทธิผล
- เพื่อการใช้งานเป็นไปตามภารกิจของ สดช. ในการควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยให้มีการควบคุมการเข้าถึงสารสนเทศ และปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย
- เพื่อเผยแพร่ให้ **"เจ้าหน้าที่ (Officer)"** ทุกระดับใน สดช. ได้รับทราบ และทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- เพื่อให้มีการดำเนินการที่เหมาะสมและสัมฤทธิผล มีการตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง
- เพื่อสร้างความตื่นตัวให้**"เจ้าหน้าที่ (Officer)"**และ **"หน่วยงานภายนอก"** ที่ปฏิบัติงานให้กับ สดช. ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ
- เพื่อดำเนินการหรือประสานงานกับหน่วยงานอื่นๆ ทั้งภายในประเทศและต่างประเทศในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงปลอดภัย ที่เป็นประโยชน์ต่อการทำงานหรือการพัฒนาบุคลากรที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

๒. องค์ประกอบของนโยบาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. ใช้แนวทางและกระบวนการโดยอ้างอิงจากพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ประจำปี ๒๕๕๐ รายละเอียดบางส่วนจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรฐาน ISO/IEC 27001 ซึ่งประกอบด้วย ๑๑ หมวด ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังต่อไปนี้

หมวด ๑ นโยบายความมั่นคงปลอดภัย (Security Policy) มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับการใช้งานระบบสารสนเทศของ สดช. เพื่อให้สอดคล้องกับข้อกำหนดทางราชการ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งจัดทำเป็นลายลักษณ์อักษร โดยที่ฝ่ายบริหารเห็นชอบและอนุมัติ และเผยแพร่ให้ **"เจ้าหน้าที่"** ทุกระดับได้รับรู้ มีการทบทวนนโยบายฯ ตามระยะเวลาที่กำหนดพร้อมทั้งปรับเปลี่ยนนโยบายตามความเหมาะสม

หมวด ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information security) มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สดช. ที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก โดยจัดให้มีคณะทำงานและบุคลากรเฉพาะด้านความมั่นคงปลอดภัย มีการประสานงานความรับผิดชอบ ประเมินความเสี่ยง และตรวจสอบการทำงานด้านความมั่นคงปลอดภัย รวมทั้งประสานงานกับหน่วยงานภายนอกและผู้ใช้งานสารสนเทศจากภายนอก โดยมีการระบุและจัดทำข้อกำหนดที่ชัดเจนในการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สดช.

หมวด ๓ การบริหารจัดการสินทรัพย์ (Asset Management) มีจุดประสงค์เพื่อป้องกันสินทรัพย์ของ สดช. จากความเสียหายที่อาจเกิดขึ้นได้ และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสม โดยมีการจัดทำบัญชีสินทรัพย์ ระบุผู้เป็นเจ้าของสินทรัพย์ และกำหนดหลักเกณฑ์การใช้งานสินทรัพย์ที่เหมาะสม มีการจัดหมวดหมู่สินทรัพย์ตามระดับชั้นความลับ และจัดทำป้ายชื่อ เพื่อการบริหารจัดการสินทรัพย์ตามที่ได้จัดหมวดหมู่ไว้

หมวด ๔ ความมั่นคงปลอดภัยทางด้านทรัพยากรบุคคล (Human Resource Security) มีจุดประสงค์เพื่อให้ **"เจ้าหน้าที่ (Officer)"** ผู้ที่ สดช. ทำสัญญาจ้างและหน่วยงานภายนอก เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตน ทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และการสิ้นสุดหรือการเปลี่ยนการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

หมวด ๕ ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) มีจุดประสงค์เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ป้องกันสินทรัพย์ไม่ให้เกิดการสูญหาย ถูกขโมย เกิดความเสียหาย เกิดการก่อกวนหรือแทรกแซง ป้องกันการถูกเปิดเผยโดยไม่ได้รับอนุญาต และป้องกันไม่ให้กิจกรรมการดำเนินงานต่างๆ ของ สดช. เกิดการติดขัดหรือหยุดชะงัก ได้แก่ การมีระบบกระแสไฟฟ้าสำรอง ระบบสื่อสารสำรอง เป็นต้น

หมวด ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงาน (Communications and Operations Management) มีจุดประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย รักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลง ลดความเสี่ยงจากความล้มเหลวของระบบ ป้องกันซอฟท์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟท์แวร์ที่ไม่ประสงค์ดี ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลง แก้ไข การลบหรือการทำลายสินทรัพย์โดยไม่ได้รับอนุญาต รักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกัน สร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ และตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

หมวด ๗ การควบคุมการเข้าถึง (Access Control) มีจุดประสงค์เพื่อควบคุมการเข้าถึงหรือควบคุมการใช้งานสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

หมวด ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition, Development and Maintenance) มีจุดประสงค์เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ ป้องกันความผิดพลาด การสูญหายและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาตหรือการใช้งานสารสนเทศผิดวัตถุประสงค์ รักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยวิธีการเข้ารหัสข้อมูล สร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์ สารสนเทศและไฟล์ต่างๆ ของระบบที่ให้บริการ ลดความความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

หมวด ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information Security Incident Management) มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ สดช. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศของ สดช. รวมถึงการรับมือภัยคุกคามทางไซเบอร์

หมวด ๑๐ การบริหารความต่อเนื่องในการดำเนินงาน (Continuity Management) มีจุดประสงค์เพื่อป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมต่างๆ ป้องกันกระบวนการทำงานที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

หมวด ๑๑ การปฏิบัติตามข้อกำหนด (Compliance) มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อการปฏิบัติราชการน้อยที่สุด

หมวด ๒
โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร
(Organization of Information Security)

จุดประสงค์ เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สดช. ที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก โดยจัดให้มีคณะทำงานและบุคลากรเฉพาะด้านความมั่นคงปลอดภัย มีการประสานงานความรับผิดชอบ ประเมินความเสี่ยง และตรวจสอบการทำงานด้านความมั่นคงปลอดภัย รวมทั้งประสานงานกับหน่วยงานภายนอกและผู้ใช้งานสารสนเทศจากภายนอก โดยมีการระบุและจัดทำข้อกำหนดที่ชัดเจนในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สดช. โดยประกอบด้วย

- นโยบายสิทธิ หน้าที่และความรับผิดชอบ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ
- นโยบายการควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศต่อหน่วยงานภายนอก
- นโยบายสำหรับผู้ปฏิบัติงานชั่วคราว

นโยบายสิทธิ หน้าที่และความรับผิดชอบ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

นโยบายนี้ระบุถึงสิทธิของผู้ใช้งาน หน้าที่ และความรับผิดชอบของบุคคล หน่วยงานที่มีส่วนเกี่ยวข้องในการใช้งาน การดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ สดช. เพื่อเป็นการปกป้องสินทรัพย์ของ สดช. ให้มีความมั่นคงปลอดภัย นโยบายนี้มีผลกับผู้ใช้งานที่มีส่วนเกี่ยวข้องกับ สดช. ทั้งหมด

๒. สิทธิ หน้าที่และความรับผิดชอบ

๒.๑. "ผู้บริหารระดับสูงสุด" "ผู้บริหารระดับสูง" และ "CIO"

หน้าที่ และความรับผิดชอบ

๒.๑.๑. ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่ สดช. หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศของ สดช. ต้องเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น โดยมีอำนาจจัดตั้งคณะกรรมการเพื่อสอบสวนข้อเท็จจริงที่เกิดขึ้น

สิทธิ

๒.๑.๒. สามารถกำหนดชั้นความลับทุกชั้นความลับ สำหรับข้อมูลและสารสนเทศที่กำหนดชั้นความลับของ สดช. ที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๑.๓. สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๑.๔. สามารถสั่งการอนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๑.๕. สามารถมอบอำนาจอย่างเป็นลายลักษณ์อักษรให้ผู้ใต้บังคับบัญชามีสิทธิในการสั่งการอนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๑.๖. สามารถแต่งตั้งให้ "เจ้าหน้าที่" ของ สดช. ทำหน้าที่เป็นผู้ดูแลระบบสำหรับงานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๑.๗. สามารถอนุญาตให้หน่วยงานภายนอกเข้ามาปฏิบัติงานกับระบบสารสนเทศของ สดช.

๒.๑.๘. สามารถกำหนดและจำแนกพื้นที่ใช้งานระบบสารสนเทศของ สดช. ที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๑.๙. สามารถกำหนดสิทธิของผู้ใช้งานในการผ่านเข้าออกพื้นที่ใช้งานระบบสารสนเทศของ สดช. ที่อยู่ภายใต้สายงานการบังคับบัญชา และต้องกำกับดูแลให้ผู้ที่มีสิทธิผ่านเข้าออกดังกล่าวปฏิบัติตามนโยบาย กฎระเบียบ ข้อบังคับ อันเกี่ยวข้องกับระบบสารสนเทศของ สดช. อย่างเคร่งครัด

๒.๒. *"ผู้บริหารระดับกลาง"*

หน้าที่ และความรับผิดชอบ

๒.๒.๑. ควบคุมดูแลให้ผู้ใต้บังคับบัญชาปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

๒.๒.๒. มีหน้าที่แจ้งต่อหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เพื่อให้รับทราบและรวบรวมข้อมูลอันเกี่ยวกับ

- การกำหนดหรือเปลี่ยนแปลงสิทธิของผู้ใช้งานที่อยู่ภายใต้สายงานการบังคับบัญชา
- การกำหนดหรือเปลี่ยนแปลงพื้นที่ใช้งานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา
- การกำหนดหรือเปลี่ยนแปลงชั้นความลับของข้อมูล ที่อยู่ภายใต้สายงานการบังคับบัญชา

สิทธิ

๒.๒.๓. สามารถกำหนดชั้นความลับทุกชั้นความลับ สำหรับข้อมูลและสารสนเทศที่กำหนดชั้นความลับของ สดช. ที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๒.๔. สามารถเสนอต่อผู้บริหารระดับสูง เพื่อพิจารณาสั่งการให้ข้อมูลหรือสารสนเทศอันเป็นผลลัพธ์ซึ่งเกิดจากการประมวลผลข้อมูลหรือสารสนเทศที่มาจากสายงานการบังคับบัญชา (ได้แก่ ผลลัพธ์จากการประมวลผลข้อมูลหรือสารสนเทศที่มาจากหลายหน่วยงาน หรือมีการกำหนดชั้นความลับไว้ต่างกัน) ได้รับการกำหนดชั้นความลับตามความเหมาะสม

๒.๒.๕. สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๒.๖. สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับอื่นๆ ของ สดช. เท่าที่ได้รับอนุญาตจากผู้บริหารระดับสูง

๒.๒.๗. สามารถสั่งการ อนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๒.๘. สามารถเสนอเพื่อแต่งตั้งให้ "เจ้าหน้าที่ (Officer)" ของ สดช. ทำหน้าที่เป็นผู้ดูแลระบบ สำหรับงานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา ทั้งนี้ขึ้นอยู่กับหน้าที่ความผิดชอบของหน่วยงานนั้นๆ

๒.๒.๙. สามารถเสนอต่อผู้บริหารระดับสูงเพื่อขออนุญาตให้หน่วยงานภายนอกเข้าปฏิบัติงานกับระบบสารสนเทศของ สดช. ที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๒.๑๐. สามารถกำหนดและจำแนกพื้นที่ใช้งานระบบสารสนเทศของ สดช. ที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๒.๑๑. สามารถกำหนดสิทธิของผู้ใช้งานในการผ่านเข้าออกพื้นที่ใช้งานระบบสารสนเทศของ สดช. ที่อยู่ภายใต้สายงานการบังคับบัญชา และมีหน้าที่ต้องกำกับดูแลให้ผู้ที่มีสิทธิผ่านเข้าออกดังกล่าว ปฏิบัติตามนโยบาย กฎระเบียบ ข้อบังคับ อันเกี่ยวข้องกับระบบสารสนเทศของ สดช. อย่างเคร่งครัด

๒.๓. *"ผู้บริหารระดับต้น"*

หน้าที่ และความรับผิดชอบ

๒.๓.๑. ควบคุมดูแลให้ผู้ใต้บังคับบัญชาปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

๒.๓.๒. ควบคุม ดูแล รับผิดชอบอุปกรณ์ด้านเทคโนโลยีสารสนเทศ ของหน่วยงาน

สิทธิ

๒.๓.๓. สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับเฉพาะ "ชั้นลับ" ที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๓.๔. สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับเฉพาะ "ชั้นลับมาก" เท่าที่ได้รับอนุญาตจาก "ผู้บริหารระดับสูง" โดยต้องผ่านความเห็นชอบของ "ผู้บริหารระดับกลาง" ที่เป็นเจ้าของงานระบบสารสนเทศ

๒.๓.๕. สามารถอนุญาตให้บุคคลหรือผู้ใช้งานยืมอุปกรณ์ด้านเทคโนโลยีสารสนเทศในความรับผิดชอบ ได้แก่ Projector, PC เป็นต้น

๒.๔. *"ผู้ดูแลระบบ (System Administrator)"*

หน้าที่ และความรับผิดชอบ

๒.๔.๑. ไม่มีสิทธิเปิดอ่านจดหมายอิเล็กทรอนิกส์หรือการสื่อสารระหว่างกันที่เป็นส่วนตัว (ได้แก่ ICQ, MSN, Talk) ของ "ผู้ใช้งาน" ยกเว้นในกรณีที่ใช้ในการสืบสวนเกี่ยวกับการใช้งานระบบอย่างไม่ถูกต้อง หรือละเมิดสิทธิผู้อื่น หรือมีการร้องขอจากหน่วยงานภายนอกตามคำสั่งศาลหรือตามกฎหมาย

๒.๔.๒. ไม่มีสิทธิเปิดอ่าน หรือใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับ ยกเว้นในกรณีที่ได้รับอนุญาตสิทธิเป็นลายลักษณ์อักษรจากผู้บริหาร สดช. ที่สามารถอนุญาตสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับนั้น

๒.๔.๓. แจ้งให้ผู้ใช้งานทราบล่วงหน้าถึงวันเวลาที่ต้องปิดระบบเพื่อบำรุงรักษาปรับปรุง หรือเปลี่ยนแปลงระบบ ซึ่งส่งผลให้ต้องหยุดบริการในช่วงเวลาหนึ่ง ยกเว้นในกรณีฉุกเฉินผู้ดูแลระบบมีสิทธิปิดระบบทันที และจะต้องพยายามให้ผู้ใช้งานสามารถเก็บบันทึกข้อมูลได้อย่างสมบูรณ์ก่อนที่จะดำเนินการปิดระบบ และทำรายงานให้ผู้อำนวยการกองทราบ

๒.๔.๔. ต้องดูแลรักษา ตรวจสอบแก้ไข และเสนอ สดช. ให้ปรับปรุงระบบสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อให้ระบบสามารถใช้งานได้ดี มีเสถียรภาพ มีความมั่นคงปลอดภัย และมีประสิทธิภาพอยู่เสมอ

๒.๔.๕. ติดตาม กำชับผู้ใช้งาน และปรับปรุงฐานข้อมูลของผู้ใช้งาน ให้มีความถูกต้องเป็นปัจจุบันอยู่เสมอ รวมทั้งต้องลบบัญชีผู้ใช้งานของผู้ที่หมดสิทธิในการใช้งานระบบออกจากฐานข้อมูล

๒.๔.๖. ต้องติดตามข่าวสาร ภาวะภัยคุกคาม ช่องโหว่ของระบบสารสนเทศ และต้องปรับปรุงดูแลระบบเพื่อลดความเสี่ยงของการถูกบุกรุกอย่างสม่ำเสมอ

๒.๔.๗. ต้องขออนุญาตผู้อำนวยการกองในกรณีที่มีการร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ในการประเมิน ตรวจสอบ ทดสอบ หาจุดอ่อน ช่องโหว่ อันเกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศ และทำการแก้ไขอย่างรวดเร็ว

๒.๔.๘. ต้องแจ้งต่อหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ทันทีและทำรายงานแจ้งผู้บังคับบัญชาตามลำดับชั้น ในกรณีที่ตรวจพบหรือได้รับรายงานจากผู้ใช้งานหรือสงสัยว่าระบบสารสนเทศที่รับผิดชอบโดยตรงหรือระบบที่เกี่ยวข้องอื่นใดของ สดช. ถูกละเมิดทางด้านความมั่นคงปลอดภัย

สิทธิ

๒.๔.๙. สามารถยุติการทำงานของระบบสารสนเทศ ซึ่งพบว่าเป็นภัยต่อความมั่นคงปลอดภัย หรือสร้างภาระให้ระบบสารสนเทศของ สดช. โดยไม่จำเป็นต้องมีการแจ้งล่วงหน้าในกรณีฉุกเฉินเท่านั้น และติดตามสอบสวนหาสาเหตุที่มาของภัยหรือภาระนั้น และทำรายงานให้ผู้อำนวยการกองที่รับผิดชอบระบบทราบ

๒.๔.๑๐. สามารถยุติการทำงานของระบบสารสนเทศที่เปิดใช้โดยไม่ได้รับอนุญาตจาก สดช. โดยไม่ต้องมีการแจ้งล่วงหน้า และติดตามสอบสวนหาสาเหตุที่มาของระบบงานนั้นและทำรายงานให้ผู้อำนวยการกองทราบ

๒.๔.๑๑. สามารถจำกัดหรือระงับสิทธิของผู้ใช้งานระบบอย่างไม่เหมาะสม และแจ้งให้ผู้บริหาร สดช. ตั้งคณะกรรมการพิจารณาสอบสวนหรือลงโทษตามความเหมาะสม

๒.๕. *"เจ้าของข้อมูล (Information Owner)"* มีหน้าที่และความรับผิดชอบ ดังต่อไปนี้

หน้าที่ และความรับผิดชอบ

๒.๕.๑. ตรวจทานระดับชั้นความปลอดภัยของข้อมูลเพื่อให้มั่นใจว่ายังเป็นไปตามความต้องการของการปฏิบัติงานและมีความเหมาะสมและสอดคล้องกับระดับความปลอดภัยนั้นๆ

๒.๕.๒. ตรวจสอบให้แน่ใจว่าข้อมูลที่ได้มีการระบุหรือแสดงระดับความปลอดภัยตามที่ได้จัดระดับไว้อย่างถูกต้องและเหมาะสม ไม่ว่าจะอยู่ในรูปแบบหรือสื่อประเภทใดก็ตาม

๒.๕.๓. จัดทำข้อกำหนดในการสำรองข้อมูล และดำเนินการให้มีการจัดการในเรื่องของการละเมิดความปลอดภัยอย่างเหมาะสม

สิทธิ

๒.๕.๔. อนุมัติและตรวจทานเพื่อให้แน่ใจว่าสิทธิของผู้ใช้งานถูกต้องเหมาะสม

๒.๕.๕. กำหนดระดับชั้นความปลอดภัยให้กับข้อมูล

๒.๕.๖. กำหนดพื้นฐานการรักษาความปลอดภัยในการเข้าถึงข้อมูลของหน่วยงาน

๒.๖. "เจ้าของระบบงาน (Application Owner)" มีหน้าที่และความรับผิดชอบ ดังต่อไปนี้

หน้าที่ และความรับผิดชอบ

๒.๖.๑. ตรวจสอบให้แน่ใจว่าระบบงานสามารถทำงานได้ถูกต้องตามความต้องการได้อย่างสม่ำเสมอ

๒.๖.๒. ควบคุมดูแลความปลอดภัยในการเข้าใช้งานระบบงาน และความปลอดภัยของข้อมูล

๒.๖.๓. อนุมัติ ตรวจทาน และรับรองสิทธิการเข้าใช้ระบบที่เหมาะกับระดับความสำคัญของข้อมูล

๒.๖.๔. จัดทำข้อกำหนดในการสำรองข้อมูลและ Source Code ของระบบงาน

๒.๖.๕. ดำเนินการหรือมีการจัดการในเรื่องของการละเมิดความปลอดภัยอย่างเหมาะสม

สิทธิ

๒.๖.๖. สามารถมอบหมายหน้าที่และความรับผิดชอบดังกล่าวข้างต้นให้แก่บุคคลอื่นที่เหมาะสม แต่เจ้าของระบบงานยังคงมีหน้าที่และความรับผิดชอบต่อระบบงานดังกล่าวโดยสมบูรณ์

๒.๗. "ผู้ใช้ (Users)" มีสิทธิ หน้าที่และความรับผิดชอบ ดังต่อไปนี้

หน้าที่ และความรับผิดชอบ

๒.๗.๑. อุปกรณ์ระบบคอมพิวเตอร์และระบบเครือข่าย สดช. มีไว้เพื่อใช้ในกิจการของ สดช. เท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บริหาร สดช.

๒.๗.๒. ต้องช่วยกันรักษาอุปกรณ์ต่างๆ ไม่ให้เกิดความเสียหาย หากมีความเสียหายจากอุบัติเหตุหรือภัยต่างๆ ผู้ใช้งานต้องรายงานผู้ดูแลระบบ และผู้บังคับบัญชาให้รับทราบทันที

๒.๗.๓. การขอใช้งานอุปกรณ์และระบบต่างๆ ผู้ใช้งานต้องสามารถแสดงบัตรประจำตัวที่ถูกต้องได้หากผู้ดูแลระบบร้องขอ

๒.๗.๔. พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ ได้แก่ ไม่ Download ไฟล์ขนาดใหญ่โดยไม่จำเป็น ไม่ส่งหรือกระจายส่งต่อจดหมายอิเล็กทรอนิกส์ในลักษณะจดหมายลูกโซ่ ฯลฯ

๒.๗.๕. เพื่อให้การบริหารระบบเป็นไปอย่างถูกต้อง ผู้ใช้งานต้องให้ข้อมูลประจำตัวที่ถูกต้องสำหรับการเปิดบัญชีผู้ใช้งาน (User ID หรือ Login Account)

๒.๗.๖. ต้องรับผิดชอบในการกำหนดรหัสผ่าน (Password) ที่ปลอดภัยตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

๒.๗.๗. ต้องไม่อนุญาตให้ผู้อื่นใช้งานระบบคอมพิวเตอร์ผ่านบัญชีผู้ใช้งานของตนโดยเด็ดขาด มิฉะนั้น ผู้ใช้งานอาจมีความผิดทางวินัยและต้องรับผิดชอบต่อปัญหาที่เกิดขึ้น ได้แก่ การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย ฯลฯ

๒.๗.๘. ต้องรายงานต่อผู้ดูแลระบบและผู้บังคับบัญชาโดยทันที ในกรณีตรวจพบ หรือสงสัยว่ามีการนำบัญชีผู้ใช้งานของตนหรือของผู้อื่นไปใช้งานโดยไม่ได้รับอนุญาต หรือใช้งานในทางมิชอบและพบเห็นพฤติกรรมการล่วงละเมิดความมั่นคงปลอดภัยทุกอย่างในระบบ

๒.๗.๙. ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

๒.๗.๑๐. ไม่ล่วงล้ำเข้าในบริเวณพื้นที่ใช้งานระบบสารสนเทศที่ไม่ได้รับอนุญาต

๒.๗.๑๑. ต้องใช้ระบบในลักษณะที่ถูกต้องตามกฎหมาย ไม่ละเมิดสิทธิ์และไม่ก่อความเดือดร้อนหรือความเสียหายแก่บุคคลหรือองค์กรอื่น

๒.๗.๑๒. ไม่ติดตั้งหรือเปิดให้บริการระบบเครือข่ายบนเครื่องของ สดช. เพื่อทำภารกิจส่วนตัว

๒.๗.๑๓. ต้องคืนสินทรัพย์ สดช. อันเกี่ยวกับการปฏิบัติหน้าที่ในทันทีที่พ้นหน้าที่ ได้แก่ อุปกรณ์ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ

๒.๗.๑๔. ต้องทำรายงานแจ้งให้ผู้ดูแลระบบและผู้อำนวยการกองทราบทันที ในกรณีที่มีการเคลื่อนย้าย ถอดถอนอุปกรณ์ระบบสารสนเทศ

๒.๗.๑๕. ต้องปฏิบัติตามมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และวิธีการปฏิบัติ (Procedure) อันเกี่ยวเนื่องกับความมั่นคงปลอดภัยด้านสารสนเทศของ สดช.

๒.๗.๑๖. ห้ามผู้ใช้งานติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องของ สดช. ก่อนได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ เพื่อป้องกันปัญหาด้านลิขสิทธิ์และปัญหาอื่นๆ ที่จะเกิดขึ้นภายหลังการติดตั้ง ได้แก่ การติดตั้ง Access Point ด้วยตนเองแล้วเกิดการเจาะระบบเข้ามาในระบบเครือข่ายของ สดช. หรือทำให้เกิดการแพร่กระจายของไวรัสและภัยคุกคามอื่นๆ เป็นต้น

๒.๗.๑๗. หากพบว่าระบบรักษาความปลอดภัยมีข้อบกพร่อง หรือสงสัยว่ามีผู้ใดกระทำการที่น่าสงสัย ให้แจ้งต่อผู้ดูแลระบบโดยทันที

๒.๗.๑๘. ต้องให้ความร่วมมือกับเจ้าหน้าที่ที่ได้รับมอบหมายให้ทำการสืบสวนสอบสวนเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยของ สดช.

สิทธิ

๒.๗.๑๙. สามารถเข้าถึงข้อมูล ข่าวสาร ที่มิใช่ข้อมูลและสารสนเทศที่กำหนดชั้นความลับของ สดช. ยกเว้นในกรณีที่ได้รับอนุญาตสิทธิเป็นลายลักษณ์อักษรจากผู้บริหาร สดช. ที่สามารถอนุญาตสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับนั้น

๒.๘. "หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ" มีหน้าที่และความรับผิดชอบ ดังต่อไปนี้

หน้าที่ และความรับผิดชอบ

๒.๘.๑. พิจารณารายละเอียดการฝ่าฝืนหรือการละเมิดข้อบังคับและนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของ สดช. ถ้าเป็นการฝ่าฝืนระเบียบขั้นรุนแรงหรือกรณีที่ฝ่าฝืนแล้วก่อให้เกิดความเสียหายแก่ สดช. หรือต่อบุคคล ก็จะจัดทำบันทึกรายงานเกี่ยวกับการฝ่าฝืนนโยบายดังกล่าวไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

๒.๘.๒. ในกรณีการละเมิดหรือฝ่าฝืนมีเจตนาไม่ชัดเจน ผู้ละเมิดหรือฝ่าฝืนจะถูกตักเตือนและชี้แจงให้เข้าใจถึงข้อปฏิบัติที่ถูกต้อง หากมีการกระทำการฝ่าฝืนนั้นอีก ให้แต่งตั้งคณะกรรมการพิจารณา และต้องรายงานการกระทำดังกล่าวไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) และผู้บังคับบัญชาระดับผู้อำนวยการกองที่เกี่ยวข้องทันที โดยให้มีการสอบสวนและดำเนินการทางวินัยตามความรุนแรงของผลกระทบจากการละเมิดหรือฝ่าฝืนข้อบังคับนั้นๆ

๒.๘.๓. ป้องกันและแก้ไขปัญหาที่เกิดขึ้นทันที เพื่อให้แน่ใจว่าการละเมิดหรือฝ่าฝืนเหล่านั้นจะไม่ลุกลามเป็นปัญหาใหญ่

๒.๘.๔. จัดอบรมส่งเสริมให้ผู้ใช้งานตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๘.๕. ให้คำแนะนำด้านเทคนิคที่เกี่ยวกับการรักษาความปลอดภัยของระบบสารสนเทศ

๒.๘.๖. วางแผนควบคุมระบบความมั่นคงปลอดภัยด้านสารสนเทศและการเตือนภัย รวมถึงวิเคราะห์หาวิธีการแก้ไขจุดอ่อนของระบบสารสนเทศ

๒.๘.๗. สืบสวนเหตุการณ์ต่างๆ ที่ไม่เป็นไปตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๘.๘. ติดต่อและประสานงานเพื่อสร้างความร่วมมือทางด้านความมั่นคงปลอดภัยระหว่างองค์กร

๒.๘.๙. รวบรวมรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่นๆ ได้แก่ สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ ศูนย์ประสานงานความมั่นคงปลอดภัยด้านสารสนเทศคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

สิทธิ

๒.๘.๑๐. กำหนดกระบวนการในการอนุมัติการใช้งานระบบสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

๒.๘.๑๑. การดำเนินการทางกฎหมายใดๆ ต้องได้รับความช่วยเหลือจากหน่วยงานดูแลรับผิดชอบด้านกฎหมายและตัวแทนของ สดช. และในการดำเนินคดีใดๆ ที่เกี่ยวข้องกับ สดช. ต้องเป็นหน้าที่ของเจ้าหน้าที่ระดับผู้บริหารที่ได้รับมอบหมายเท่านั้น

๒.๙. "หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ" มีหน้าที่และความรับผิดชอบ ดังต่อไปนี้

๒.๙.๑. พัฒนา ติดตั้ง ตรวจสอบ ปรับปรุง ซ่อมแซมและบำรุงรักษาอุปกรณ์ บริหารจัดการระบบเกี่ยวกับอุปกรณ์ IT Infrastructure ให้แก่หน่วยงานของ สดช. ทั้งหมด

๒.๙.๒. บริหารจัดการระบบเครือข่ายเชื่อมโยงคอมพิวเตอร์ (Network Administration) ที่ใช้งานภายใน สดช. ทุกระบบ และควบคุมการเชื่อมต่อเครือข่ายอินเทอร์เน็ตโดยตรงผ่านช่องทางอื่น ได้แก่ Dial up Modem รวมทั้งควบคุมการเชื่อมต่อเครือข่ายจากภายนอก ได้แก่ การ Remote เครื่องคอมพิวเตอร์ การใช้งาน VPN เป็นต้น

๒.๙.๓. รับผิดชอบในการจัดหาและควบคุมการใช้งาน Corporate Antivirus จัดเตรียมคู่มือและข้อมูลต่างๆ ที่เกี่ยวกับ Corporate Antivirus จัดทำสถิติ กราฟ และผลการใช้งาน รวมไปถึงการอนุญาตหรือจำกัดการใช้งานของผู้ใช้งาน

๒.๙.๔. รับผิดชอบในการบำรุงรักษา ปิดช่องโหว่ในระบบ Corporate Antivirus ปรับปรุง Virus Signature ระบบ Corporate Antivirusให้ทันสมัย เสนองบประมาณผ่านหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ปรับเพิ่มลดจำนวนลิขสิทธิ์ของ Corporate Antivirus อนุญาตหรือจำกัดการใช้งานของผู้ใช้งาน และดำเนินการในส่วนที่เกี่ยวข้อง

๒.๙.๕. รับผิดชอบการจัดทำและปรับปรุงเนื้อหาของเว็บไซต์ของสดช. (www.onde.go.th)

๒.๙.๖. ควบคุมการติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องคอมพิวเตอร์ของ สดช.

๒.๙.๗. รับผิดชอบร่วมกับผู้ดูแลระบบในการตรวจสอบซอฟต์แวร์ เพื่อป้องกันการละเมิดข้อตกลง และหาทางป้องกันซอฟต์แวร์ที่ใช้ในการตรวจประเมินระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิดหรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้นๆ

๒.๙.๘. จัดทำข้อมูลสินทรัพย์ระบบสารสนเทศของ สดช. รวมถึงค่า Configuration ของอุปกรณ์เครือข่าย เพื่อประสิทธิภาพในบริหารจัดการระบบสารสนเทศของ สดช.

๒.๙.๙. ให้คำแนะนำและเป็นที่ปรึกษาร่วมในการพิจารณารายละเอียดการฝ่าฝืนหรือการละเมิดข้อบังคับและนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของ สดช. ร่วมกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ และร่วมกันแก้ไขปัญหาปัญหาที่เกิดขึ้นดังกล่าว

๒.๙.๑๐. ควบคุมระบบความมั่นคงปลอดภัยด้านสารสนเทศและการเตือนภัย รวมถึงวิเคราะห์หาวิธีการแก้ไขจุดอ่อนของระบบสารสนเทศร่วมกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ

๒.๙.๑๑. กำหนดและควบคุมการสำรองและกู้คืน (Backup & Recovery) ระบบสารสนเทศของ สดช.

๒.๙.๑๒. ควบคุมการพิสูจน์ตัวตน (Authentication) ก่อนเข้าถึงระบบสารสนเทศของ สดช.

๒.๑๐. *"หน่วยงานดูแลรับผิดชอบด้านตรวจสอบภายใน"* มีหน้าที่และความรับผิดชอบดังต่อไปนี้

๒.๑๐.๑. ตรวจสอบการปฏิบัติงานของผู้ใช้งานให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. ที่ดำเนินไปภายใต้มาตรฐานและแนวทางการปฏิบัติที่ได้กำหนดไว้ในนโยบาย และร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เพื่อป้องกันสินทรัพย์และข้อมูลต่างๆ ของ สดช.

๒.๑๐.๒. ให้ความช่วยเหลือแก่หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ในการชี้ถึงความเสี่ยงต่างๆ รวมถึงภัยคุกคามอันอาจก่อให้เกิดอันตรายต่อความมั่นคงปลอดภัยของ สดช.

๒.๑๑. "หน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง" มีหน้าที่และความรับผิดชอบในการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ เพื่อปรับปรุงให้องค์กรมีคุณภาพประสิทธิภาพ และลดโอกาสความเสียหายที่อาจจะเกิดขึ้นได้

๒.๑๒. "หน่วยงานดูแลรับผิดชอบด้านกฎหมาย" มีหน้าที่และความรับผิดชอบในการให้ความเห็นหรือให้คำปรึกษาเกี่ยวกับระเบียบ ข้อกำหนด กฎเกณฑ์ ข้อบังคับ กฎหมาย พระราชบัญญัติ พระราชกฤษฎีกา การฟ้องร้องดำเนินคดี รวมถึงข้อละเมิดสินทรัพย์ทางปัญญา ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของ สดช.

๒.๑๓. "หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการ" มีหน้าที่และความรับผิดชอบ ดังต่อไปนี้

๒.๑๓.๑. ตรวจสอบคุณสมบัติของผู้สมัคร เกี่ยวกับการละเมิดด้านความมั่นคงปลอดภัยระบบสารสนเทศ

๒.๑๓.๒. การให้"เจ้าหน้าที่"ลงนามมิให้เปิดเผยความลับของ สดช.

๒.๑๓.๓. รายงานข้อมูลการว่าจ้างงาน การเปลี่ยนแปลงสภาพการว่าจ้างงาน การลาออกจากงาน การถึงแก่กรรม การโยกย้าย และการพักงานหรือการลงโทษทางวินัย ให้แก่ หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เพื่อบริหารจัดการทรัพยากรระบบสารสนเทศ และ สิทธิ์ในการเข้าถึงระบบงานต่าง ๆ

๒.๑๔. "หน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร" มีหน้าที่และความรับผิดชอบในการจัดการประชุม สัมมนา หรืออบรมให้ความรู้แก่บุคลากรใหม่และผู้ใช้งาน เกี่ยวกับวิธีปฏิบัติงาน เพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของ สดช.

๒.๑๕. "หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่" มีหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ควบคุมการเข้า-ออกอาคารและสำนักงาน จัดเตรียมการป้องกันต่อภัยคุกคามต่างๆ ทั้งจากมนุษย์และธรรมชาติ ได้แก่ ไฟไหม้ น้ำท่วม แผนดินไหว ความไม่สงบของบ้านเมือง เป็นต้น

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก
(IT Security of Third Party Policy)

๑. วัตถุประสงค์

เพื่อควบคุมหน่วยงานภายนอกที่มีการใช้งานระบบสารสนเทศและทรัพยากรสารสนเทศอื่นๆ ของ สดช. ให้เป็นไปอย่างมั่นคงปลอดภัย นโยบายนี้ใช้กำกับการดำเนินงานซึ่งไม่สามารถทำขึ้นภายใน สดช. ได้แก่ การพัฒนาระบบสารสนเทศ การใช้บริการของที่ปรึกษา การใช้บริการด้านระบบสารสนเทศจากภายนอก

๒. การระบุสัญญาเพื่อควบคุมการเข้าใช้งานของหน่วยงานภายนอก

๒.๑. หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าถึงแหล่งข้อมูลของ สดช. จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการกองเจ้าของข้อมูล ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าว

๒.๒. ต้องทำการแจ้งเป็นลายลักษณ์อักษรให้หน่วยงานภายนอกทราบถึงความสำคัญที่มีต่อความมั่นคงปลอดภัยด้านสารสนเทศของข้อมูลสารสนเทศ ซึ่งหน่วยงานภายนอกจะต้องลงนามในเอกสารสัญญาเรื่องการไม่เปิดเผยข้อมูลของ สดช. โดยเอกสารดังกล่าวจะถูกจัดเก็บไว้เป็นหลักฐาน ในส่วนของผู้ร่วมสัญญาต้องทำการลงนามในสัญญาเรื่องการปกปิดเป็นความลับ และจัดเก็บเอกสารไว้ในแฟ้มสัญญา

๒.๓. เจ้าของโครงการหรือผู้จัดการโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้เฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๒.๔. คู่สัญญาหรือหน่วยงานภายนอก มีหน้าที่ที่ต้องแจ้งให้กับผู้เป็นเจ้าของหรือผู้รับผิดชอบโครงการทราบทันทีที่พบว่ามีการคุกคามที่มีผลต่อความมั่นคงปลอดภัยในลักษณะใดๆ ก็ตาม รวมถึงการเข้าถึงข้อมูลโดยผู้ไม่มีสิทธิ หรือการผ่อนปรน หรือละเว้นไม่ปฏิบัติตามวินัยความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. นอกจากนั้น “เจ้าหน้าที่ (Officer)” ของ สดช. ผู้ซึ่งรับทราบถึงเหตุการณ์คุกคามด้านความปลอดภัยซึ่งเกิดจากคู่สัญญาหรือบุคคลที่สาม ต้องแจ้งให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ทราบทันทีตามกระบวนการในนโยบายการรายงานเหตุการณ์ด้านความปลอดภัย

๒.๕. สัญญาการใช้งานระบบสารสนเทศทั้งหมดที่มีการจัดทำขึ้นต้องระบุถึง “สิทธิในการตรวจสอบ” เพื่อให้มั่นใจได้ว่า สดช. สามารถเข้าไปประเมินสภาพแวดล้อมของการควบคุมภายในทั้งทางกายภาพ (Physical) และทาง Logical ของคู่สัญญาหรือหน่วยงานภายนอกได้

๓. การให้ความสนับสนุนจาก สดช.

หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าถึงแหล่งข้อมูลของ สดช. จะต้องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการกองเจ้าของข้อมูล ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าว

๔. **มาตรฐานการเลือกหน่วยงานภายนอกโดยทั่วไป**

๔.๑. ผู้อำนวยการกองที่รับผิดชอบโครงการ ต้องขอข้อมูลเบื้องต้นของหน่วยงานภายนอกในรายที่ยังไม่ทราบรายละเอียด ซึ่งอาจจะรวมถึงข้อมูลด้านการเงินที่ใช้อ้างอิงได้

๔.๒. สดช. ต้องพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบที่เข้าไปปฏิบัติงานและข้อมูลที่ให้ไป

๔.๓. สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของ สดช. ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานในการประมวลผลข้อมูลนั้น

๕. **สัญญาในการไม่เปิดเผยข้อมูล**

๕.๑. **กรณีที่มีความจำเป็น** สดช. จะให้สิทธิหน่วยงานภายนอกในการเข้าถึงข้อมูลเดียวกับผู้ใช้งานภายใน โดยจะจำกัดเพียงการเข้าถึงข้อมูลเท่าที่จำเป็นเพื่อให้งานเสร็จสมบูรณ์
ข้อพิจารณา ให้อยู่ในดุลพินิจของผู้อำนวยการกองเจ้าของข้อมูลนั้นๆ หรือหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ

๕.๒. หน่วยงานภายนอก ที่ปรึกษา หรือคู่สัญญาที่ทำงานโดยตรงให้กับ สดช. ทุกคน ไม่ว่าจะทำงานอยู่ภายใน สดช. หรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของ สดช. โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเครือข่ายและข้อมูลต่างๆ ของ สดช.

๖. **มาตรฐานทั่วไปของหนังสือสัญญาว่าจ้าง ที่ต้องมีการใช้งานระบบสารสนเทศจากหน่วยงานภายนอก** ต้องประกอบไปด้วยข้อความดังต่อไปนี้

๖.๑. สัญญาในการยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยของ สดช.

๖.๒. สิทธิสำหรับ สดช. ที่จะตรวจสอบสภาพแวดล้อมการทำงานรวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก

๖.๓. เอกสารต่างๆ เกี่ยวกับมาตรการการควบคุมที่ใช้ทั้งด้าน Physical และด้าน Logical เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคงปลอดภัยได้ทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๖.๔. ข้อกำหนดทางด้านกฎหมาย ได้แก่ความลับส่วนบุคคล (Privacy) และการป้องกันข้อมูล

นโยบายสำหรับผู้ปฏิบัติงานชั่วคราว
(Temporary Worker Policy)

๑. วัตถุประสงค์

เพื่อให้ทุกหน่วยงาน กำกับ ดูแล ผู้ปฏิบัติงานชั่วคราว (Temporary Worker) ที่ไม่ใช่ "เจ้าหน้าที่ (Officer)"ของ สดช. และอยู่ในความรับผิดชอบ ให้ใช้ระบบสารสนเทศอย่างเหมาะสม เกิดประโยชน์สูงสุด และปลอดภัย จึงกำหนดข้อปฏิบัติเพื่อความปลอดภัยของระบบสารสนเทศ ดังนี้

๒. การขอรับสิทธิของผู้ใช้งาน

๒.๑. หน่วยงานที่มีความประสงค์ขออนุญาตให้ผู้ปฏิบัติงานชั่วคราวเข้าสู่ระบบสารสนเทศของ สดช. ให้ขออนุมัติจากผู้บังคับบัญชาระดับกองขึ้นไปที่มีอำนาจครอบคลุมระบบสารสนเทศที่ผู้ปฏิบัติงานชั่วคราวต้องการจะเข้าถึงทั้งหมด ทั้งนี้ให้ใช้แบบฟอร์ม เพื่อขออนุมัติตามที่ สดช. กำหนด

๒.๒. ผู้ดูแลระบบจะกำหนด Username และ Password ให้กับผู้ปฏิบัติงานชั่วคราวทุกท่านที่ได้รับอนุมัติจากผู้บริหารตามข้อ ๒.๑

๓. การดูแลระหว่างการปฏิบัติงานชั่วคราว

๓.๑. ผู้บังคับบัญชาตามข้อ ๒.๑ ต้องกำหนดให้มีหัวหน้าหน่วยงานที่เกี่ยวข้อง เป็นผู้ดูแลผู้ปฏิบัติงานชั่วคราวตลอดระยะเวลาการปฏิบัติงาน

๓.๒. หัวหน้าหน่วยงานที่ได้รับมอบหมายจากผู้บังคับบัญชาตามข้อ ๓.๑ ต้องชี้แจงให้ผู้ปฏิบัติงานชั่วคราวปฏิบัติตามข้อกำหนดว่าด้วยความมั่นคงปลอดภัยของระบบสารสนเทศและคำสั่งที่เกี่ยวข้องอย่างเคร่งครัด

๓.๓. หัวหน้าหน่วยงานที่ได้รับมอบหมายจากผู้บังคับบัญชาตามข้อ ๓.๑ มีหน้าที่กำกับ ดูแลพฤติกรรมการใช้ระบบสารสนเทศของ สดช. ให้เป็นไปตามความต้องการของหน่วยงาน

๓.๔. หัวหน้าหน่วยงานสามารถยกเลิกสิทธิการใช้ระบบของผู้ปฏิบัติงานชั่วคราวที่มีพฤติกรรมการใช้ระบบสารสนเทศของ สดช. ในทางที่ไม่เหมาะสม

๔. การดูแลเมื่อสิ้นสุดการปฏิบัติงานชั่วคราว

๔.๑. ผู้ปฏิบัติงานชั่วคราวที่ได้ทำการสร้างข้อมูลอิเล็คทรอนิกส์ที่ไม่ก่อให้เกิดประโยชน์กับ สดช. ไว้บนระบบสารสนเทศของ สดช. จะต้องทำการลบข้อมูลทิ้งทั้งหมด โดยผู้ดูแลผู้ปฏิบัติงานชั่วคราวต้องกำกับดูแลการลบข้อมูลอิเล็กทรอนิกส์ดังกล่าว

๔.๒. ผู้ดูแลระบบต้องลบ Username และ Password ของผู้ปฏิบัติงานชั่วคราวทันที หลังจากสิ้นสุดการปฏิบัติงาน

๔.๓. ผู้ดูแลผู้ปฏิบัติงานชั่วคราวต้องแจ้งผู้บังคับบัญชาทันทีที่ผู้ปฏิบัติงานชั่วคราวหมดความจำเป็น หรือเลิกการปฏิบัติงานก่อนกำหนด หรือครบกำหนดการปฏิบัติงานชั่วคราว

๕. การดูแลเรื่องข้อมูลด้านเทคโนโลยีสารสนเทศที่เป็นความลับ

๕.๑. ผู้ปฏิบัติงานชั่วคราวต้องไม่เปิดเผยข้อมูลในระบบสารสนเทศของ สดช. ต่อบุคคลอื่นที่ไม่เกี่ยวข้องกับการปฏิบัติงานนั้น ทั้งระหว่างการปฏิบัติงานและภายหลังการปฏิบัติงานเสร็จสิ้นไปแล้ว ยกเว้นกรณีที่จำเป็นตามคำสั่งศาลหรือตามกฎหมาย

๕.๒. สดช. สงวนสิทธิ์ที่จะเรียกร้องค่าเสียหาย หากพบว่าผู้ปฏิบัติงานชั่วคราวนำข้อมูลที่เป็นความลับในระบบสารสนเทศของ สดช. ไปใช้เพื่อประโยชน์ส่วนตน หรือเพื่อประโยชน์ของบุคคล/นิติบุคคลอื่นๆ

๖. สิทธิในการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว

การใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว หมายถึง การที่ผู้ปฏิบัติงานชั่วคราวเข้ามาปฏิบัติงานในระบบสารสนเทศของ สดช. โดยผ่าน Dial-up Modem, เครือข่าย Internet, เครือข่าย Wireless หรือเครือข่ายคอมพิวเตอร์อื่นๆ ที่อยู่นอกเหนือการควบคุมของ สดช.

สิทธิในการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราวเป็นสิทธิที่ สดช. จะอนุญาตให้เฉพาะกับตัวบุคคลในระหว่างที่บุคคลนั้นสังกัดอยู่กับบริษัท/องค์กรใดเท่านั้น โดยไม่สามารถถ่ายโอนกันได้ระหว่างบุคคล บริษัท หรือ องค์กร หากบุคคลผู้เคยได้รับสิทธิดังกล่าวไม่ได้สังกัดอยู่กับบริษัท/องค์กรที่เคยได้รับสิทธิแล้ว ให้ถือว่าบุคคลดังกล่าวหมดสิทธิไป

๖.๑. สดช. อาจจะให้สิทธิใช้งาน Remote Access ในการปฏิบัติงานชั่วคราวคือ ผู้ปฏิบัติงานชั่วคราวที่เป็นที่ปรึกษา (Consultant) หรือผู้ปฏิบัติงานตามสัญญาจ้าง (Contractor) เท่านั้น ผู้ปฏิบัติงานชั่วคราวที่เป็นนิสิตนักศึกษาฝึกงานอาจจะไม่ได้รับสิทธิดังกล่าว

๖.๒. ผู้ปฏิบัติงานชั่วคราวจะต้องขออนุญาตผู้อำนวยการกองหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศล่วงหน้าก่อนเข้ามาใช้งาน Remote Access สู่ระบบสารสนเทศของ ผู้ปฏิบัติงานชั่วคราวจะต้องระบุวัตถุประสงค์ วิธีการ Access และขอบข่ายของการ Access ที่แน่ชัด และ สดช. อาจจะอนุญาตให้เป็นรายครั้ง หรือเป็นช่วงระยะเวลาจำกัดแล้วแต่กรณีและความจำเป็น

๖.๓. สดช. สงวนลิขสิทธิ์ที่จะดำเนินคดีตามกฎหมายกับการโยกย้ายเปลี่ยนแปลงโปรแกรมหรือข้อมูลของ สดช. อื่นใดนอกเหนือไปจากที่ผู้ปฏิบัติงานชั่วคราวได้รับอนุญาต

๖.๔. สดช. สงวนสิทธิ์เรียกร้องค่าเสียหาย หากระบบคอมพิวเตอร์ของ สดช. ได้รับความเสียหาย ได้แก่ การติดไวรัสคอมพิวเตอร์ จากการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว

๗. ข้อกำหนดสำหรับผู้ปฏิบัติงานชั่วคราวที่เป็นนิสิตนักศึกษาฝึกงาน

ผู้ปฏิบัติงานชั่วคราวที่เป็นนิสิตนักศึกษาฝึกงานต้องส่งมอบ Source Code, Executable Files และ ลิขสิทธิ์ในผลงานที่ได้พัฒนาขึ้นทั้งหมดในระหว่างการฝึกงานให้กับ สดช. เพื่อประโยชน์ในการตรวจสอบด้านความมั่นคงปลอดภัย

แบบฟอร์มสำหรับผู้ปฏิบัติงานชั่วคราว

วันที่ .....

ชื่อ.....นามสกุล.....
เลขประจำตัวประชาชน.....ออกให้โดย.....
หน่วยงาน.....
วันที่เริ่มต้นปฏิบัติงาน..... วันสิ้นสุดการปฏิบัติงาน.....
ระบบที่ต้องการใช้.....
ชื่อผู้ดูแลระบบ.....กอง.....กอง.....
ชื่อผู้ดูแลผู้ปฏิบัติงาน.....ตำแหน่ง.....

ขอรับรองว่าข้อความดังกล่าวเป็นความจริงทุกประการ

ลงชื่อผู้ขอ.

.....

(.....)

เห็นชอบอนุมัติตามคำขอ

.....

ผู้อำนวยการกอง

.....

(โปรดแนบสำเนาบัตรประชาชนผู้ขอ)

International Temporary Worker Form

Date.....

Personal Information

First Name..... Last Name.....

Nationality..... Country .....

Permanent Address.....

Address in Thailand.....Telephone.....

Passport Information

Passport No. ..... Date of Issue .....

Date of Expiry ..... Place of Issue/Issued by .....

Visa Information

Visa No. ..... Date of Issue.....

Date of Expiry ..... Place of Issue/Issued by .....

Purpose of Visit

Objective ..... Project Name .....

Starting Operation Date ..... Ending Operation Date .....

System Detail .....

Administrator Name ..... Position .....

Section ..... Department .....

Contact Person Name ..... Position .....

History of Visit or use MICT's IT Resource.

"Is this the first time that you visit the MICT Limited or use MICT's IT Resource?"

☐ Yes

☐ No "List of your most recent visits to the MICT (up to three):
(Date and Project)

.....

.....

.....

I hereby certify, under the penalty of perjury, that all the information items given here are the most truthful and the most accurate to my present knowledge.

Signature ..... Authorized by .....

( ) ( )

หมวด ๓
การบริหารจัดการสินทรัพย์
(Asset Management)

มีจุดประสงค์ เพื่อป้องกันสินทรัพย์ของ สดช. จากความเสียหายที่อาจเกิดขึ้นได้ และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสม โดยมีการจัดทำบัญชีสินทรัพย์ ระบุผู้เป็นเจ้าของสินทรัพย์ และกำหนดหลักเกณฑ์การใช้งานสินทรัพย์ที่เหมาะสม มีการจัดหมวดหมู่สินทรัพย์ตามระดับชั้นความลับ และจัดทำป้ายชื่อ เพื่อการบริหารจัดการสินทรัพย์ตามที่ได้จัดหมวดหมู่ไว้ โดยมีนโยบายดังนี้

นโยบายการจัดหมวดหมู่และการควบคุมสินทรัพย์
(Asset Classification and Control Policy)

๑. วัตถุประสงค์

เพื่อเป็นการกำหนดมาตรฐานในการจัดหมวดหมู่และการควบคุมสินทรัพย์ของ สดช. เพื่อป้องกันสินทรัพย์จากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจเกิดขึ้นได้

๒. การจัดหมวดหมู่และการควบคุมสินทรัพย์

๒.๑. การจัดทำบัญชีสินทรัพย์ (Inventory of Assets)

ผู้อำนวยการกองแต่ละหน่วยงาน ต้องทำบัญชีสินทรัพย์ของหน่วยงานและแบ่งประเภทให้ชัดเจน ซึ่งรวมถึงบัญชีครุภัณฑ์คอมพิวเตอร์และบัญชีข้อมูลที่เก็บไว้ในสื่อต่างๆ ทั้งหมด เพื่อใช้ในการกำหนดมูลค่าสินทรัพย์ ระดับความสำคัญและวิธีการป้องกันที่เหมาะสม รวมทั้งต้องระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) ตามที่กำหนดไว้ในบัญชีสินทรัพย์ ซึ่งมีแนวทางปฏิบัติ ดังนี้

๒.๑.๑. สินทรัพย์ของ สดช. ที่เป็นครุภัณฑ์อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย และซอฟต์แวร์ที่มีค่าลิขสิทธิ์ ต้องมีการขึ้นบัญชีไว้ในสมุดทะเบียน หรือระบบของ สดช. ตามหลักเกณฑ์หรือสัญญาที่ได้มีการกำหนดไว้สำหรับระบบดังกล่าว

๒.๑.๒. สินทรัพย์ของ สดช. ที่เป็นซอฟต์แวร์ที่ใช้เพื่อการให้บริการของ สดช. ซึ่งไม่มีค่าลิขสิทธิ์ หากหน่วยงานใดมีการใช้งาน ให้หน่วยงานนั้นทำทะเบียนการใช้งานไว้ที่หน่วยงาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและสินทรัพย์ที่เป็นซอฟต์แวร์ของ สดช. เพื่อประโยชน์ในการค้นหาติดตามและสำรวจช่องโหว่ที่อาจมีผลกระทบต่อความมั่นคงปลอดภัยในระบบสารสนเทศ

๒.๑.๓. อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ซอฟต์แวร์ที่หน่วยงานจัดเช่า ต้องกำหนดให้มีเจ้าหน้าที่ของหน่วยงานเป็นผู้รับผิดชอบ และจะต้องจัดทำบัญชีรายการของอุปกรณ์ ซอฟต์แวร์ หรือระบบงานคอมพิวเตอร์ที่เช่ามาใช้งาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและสินทรัพย์ของ สดช.

๒.๑.๔. สื่อบันทึกหรือบรรจุข้อมูล ทั้งกรณีที่เป็นสินทรัพย์ของ สดช. หากหน่วยงานใดมีการใช้สื่อเพื่อบันทึกข้อมูลที่มีการกำหนดชั้นความลับ “ชั้นลับที่สุด” หรือ “ชั้นลับมาก” หรือ “ชั้นลับ” หน่วยงานนั้นจะต้องมีการทำบัญชีควบคุมการใช้งานเพื่อระบุผู้รับผิดชอบและป้องกันไม่ให้รั่วไหล

๒.๒. ***การตรวจสอบบัญชีสินทรัพย์ (Inventory Check)***

ผู้อำนวยการกองแต่ละหน่วยงาน ต้องต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ตามระยะเวลาที่กำหนดไว้ ได้แก่ เดือนละครั้ง(สำหรับระบบสำคัญ) หรือปีละครั้ง(สำหรับระบบการใช้งานทั่วไป)

๒.๓. ***การจัดหมวดหมู่ข้อมูลและสารสนเทศ (Data and Information Classification)***

๒.๓.๑. ข้อมูลดิจิทัล (Digital Data) หรือสารสนเทศดิจิทัล (Digital Information) ให้หน่วยงานระบุชนิดลักษณะของข้อมูลให้ชัดเจนว่าเกี่ยวกับเรื่องใด (Topic) มีความสำคัญอย่างไร (Importance) และต้องมีการจัดลำดับชั้นความลับเป็นอย่างใดอย่างหนึ่งต่อไปนี้

๒.๓.๑.๑. ***"ชั้นลับที่สุด"***

๒.๓.๑.๒. ***"ชั้นลับมาก"***

๒.๓.๑.๓. ***"ชั้นลับ"***

โดยยึดถือจากคำนิยามในหมวดที่ ๑ ทั้งนี้หากไม่ได้มีการกำหนดชั้นความลับที่ชัดเจนไว้ ให้ถือว่าข้อมูลหรือสารสนเทศนั้นเป็น ***"ชั้นเปิดเผย"*** โดยปริยาย

๒.๓.๒. เอกสารหรือสิ่งตีพิมพ์ ที่พิมพ์หรือทำซ้ำขึ้นมาจากข้อมูลดิจิทัลหรือสารสนเทศดิจิทัลซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับข้อมูลดิจิทัลหรือสารสนเทศดิจิทัลนั้น ***ยกเว้นว่ามีการจัดลำดับชั้นความลับใหม่โดยหน่วยงานผู้ผลิตเอกสารหรือสิ่งพิมพ์นั้น***

๒.๓.๓. ผู้อำนวยการกองแต่ละหน่วยงาน ต้องทำการจัดหมวดหมู่ กำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันสารสนเทศของ สดช. ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดย สดช. จัดให้มีกระบวนการในการจัดหมวดหมู่ของข้อมูลและสินทรัพย์ ได้แก่ ชั้นลับที่สุด ชั้นลับมากและชั้นลับ การกำหนดแนวทางการแบ่งชั้นความลับของข้อมูล ต้องอยู่ในการควบคุมดูแลและรักษาความปลอดภัยที่เหมาะสมไม่ว่าจะอยู่ในรูปแบบใดก็ตาม

๒.๓.๔. ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การเก็บรักษา จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้ "เจ้าหน้าที่"ของ สดช. ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

๒.๔. ***การจัดทำป้ายชื่อ ข้อมูล และ สารสนเทศ (Data and Information Labeling and Handling)***

๒.๔.๑. ผู้อำนวยการกองแต่ละหน่วยงาน ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับข้อมูลและสารสนเทศ โดยแยกตามหมวดหมู่ที่กำหนดไว้ มีการส่งมอบและจัดเก็บตามขั้นตอนกระบวนการต่างๆ ซึ่งประกอบไปด้วย การถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสาร และการทำลาย มีแนวทางปฏิบัติดังนี้

๒.๔.๑.๑. ข้อมูลที่อยู่ "ชั้นลับที่สุด" ทั้งฉบับจริงและสำเนาต้องมีการระบุถึงระดับความปลอดภัยของข้อมูลในเอกสารตรงบริเวณส่วนหัวและ/หรือส่วนท้ายของเอกสารทุกหน้า

๒.๔.๑.๒. การนำส่งเอกสารข้อมูล “ชั้นลับที่สุด” ต้องใส่ซองเอกสารลับเฉพาะ ที่ไม่สามารถเห็นถึงเนื้อหาของเอกสารที่บรรจุภายในและปิดผนึก ลงชื่อของผู้รับอย่างชัดเจน

๒.๔.๑.๓. ข้อมูลที่อยู่ “ชั้นลับที่สุด” ต้องมีการจัดเก็บในลิ้นชักหรือตู้ที่มีการล็อคหรือ ห้องที่มีการออกแบบพิเศษสำหรับการเก็บรักษาเอกสารเหล่านี้โดยเฉพาะ และจำกัดเฉพาะผู้ที่มีสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลดังกล่าวได้

๒.๔.๑.๔. การทำสำเนาเอกสารข้อมูลที่อยู่ “ชั้นลับที่สุด” ต้องได้รับการอนุมัติจากผู้บริหารระดับสูงเท่านั้น

๒.๔.๑.๕. ข้อมูลที่อยู่ “ชั้นลับที่สุด” ต้องมีการควบคุมดูแลอย่างใกล้ชิดในขณะที่ใช้งานเครื่องพิมพ์และเครื่องถ่ายเอกสาร เพื่อพิมพ์หรือทำสำเนาของข้อมูล

๒.๔.๑.๖. ข้อมูลที่อยู่ “ชั้นลับที่สุด” ผู้ที่ควบคุมการใช้งานเท่านั้นที่ได้รับอนุญาตให้ตรวจสอบข้อมูลที่พิมพ์หรือสำเนา

๒.๔.๑.๗. ข้อมูลที่ถูกจัดอยู่ใน “ชั้นลับมาก” ต้องใช้ระบบการนำส่งแบบใส่ ๒ ซอง ซ้อนได้แก่เดียวกัน โดยซองด้านในระบุถึงชื่อและประเภทของข้อมูลอย่างชัดเจน ส่วนซองด้านนอกจะระบุถึงชื่อและที่อยู่ของผู้รับเท่านั้น

๒.๔.๑.๘. ข้อมูล “ชั้นลับมาก” ต้องส่งให้ถึงมือผู้รับที่ระบุเท่านั้นและต้องมีลายเซ็นของผู้รับระบุว่าได้รับเอกสารแล้ว

๒.๔.๑.๙. การทำสำเนาเอกสารข้อมูลที่อยู่ “ชั้นลับมาก” ต้องได้รับการอนุมัติจากผู้บริหารระดับกลางเท่านั้น

๒.๔.๑.๑๐. ข้อมูลที่อยู่ “ชั้นลับมาก” ต้องถูกจัดพิมพ์จากเครื่องพิมพ์ที่เชื่อมโยงกับระบบเครือข่ายที่สามารถควบคุมการใช้ได้เพื่อป้องกันการอ่าน เปลี่ยนแปลง หรือ ลบข้อมูลได้จากผู้ที่ไม่ได้รับอนุญาต

๒.๔.๑.๑๑. เอกสารข้อมูล “ชั้นลับที่สุด” “ชั้นลับมาก” และ “ชั้นลับ” ที่ไม่ได้นำมาใช้แล้วต้องถูกรวบรวม ขีดฆ่า และทำเครื่องหมาย **“ทำลายได้”** และนำเอกสารไปทำลายเพื่อไม่ให้สามารถอ่านหรือนำมาใช้ได้อีกโดยการฉีกหรือเผาทำลาย

หมวด ๔
ความมั่นคงปลอดภัยทางด้านทรัพยากรบุคคล
(Human Resource Security)

มีจุดประสงค์ เพื่อให้ "เจ้าหน้าที่ (Officer)" เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตน ทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และการสิ้นสุดหรือการเปลี่ยนการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่ โดยมีนโยบายดังนี้

นโยบายความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล
(Human Resource Security Policy)

๑. วัตถุประสงค์

เพื่อเป็นมาตรฐานในการควบคุมความปลอดภัยส่วนบุคคล โดยกำหนดเป็นมาตรฐานเกี่ยวกับผู้บริหาร "เจ้าหน้าที่ (Officer)"ของ สดช. เริ่มตั้งแต่กระบวนการสรรหา "เจ้าหน้าที่ (Officer)" ใหม่ เพื่อให้มั่นใจว่ามีการพิจารณาคุณสมบัติอย่างเพียงพอก่อนที่จะมีการว่าจ้าง ตลอดจนเมื่อเริ่มปฏิบัติงานต้องมีการกำหนดสิทธิในการเข้าสู่อาคารสถานที่และระบบงานที่สำคัญ เพื่อปฏิบัติงานตามหน้าที่และสิทธินั้นและจะต้องมีการยกเลิกเมื่อสิ้นสุดการว่าจ้างหรือมีการโยกย้ายการปฏิบัติงานของ "เจ้าหน้าที่"ดังกล่าว

๒. มาตรฐานการสร้างความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากร

๒.๑. การกำหนดหน้าที่ความรับผิดชอบพื้นฐานด้านความมั่นคงปลอดภัย (Including Basic Security in Job Responsibilities)

ผู้อำนวยการกองแต่ละหน่วยงาน ต้องกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในคุณสมบัติของบุคลากร IT ตามที่กำหนดเอาไว้ในนโยบาย หมวด ๖การบริหารจัดการด้านการสื่อสารและการดำเนินงาน (Communications and Operations Management)

๒.๒. การตรวจสอบคุณสมบัติของผู้สมัคร (Personnel Screening)

๒.๒.๑. หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการ ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็น "เจ้าหน้าที่ (Officer)" โดยจะต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบสารสนเทศของหน่วยงานใดมาก่อน

๒.๒.๒. หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการ จะต้องจัดเตรียมข้อมูลที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. เพื่อให้ "เจ้าหน้าที่ (Officer)" ที่เข้ามาใหม่ได้ศึกษาและรับทราบ

๒.๒.๓. "เจ้าหน้าที่ (Officer)" ใหม่ทุกคนจะต้องลงนามรับทราบและยอมรับสัญญาในนโยบายความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ความรับผิดชอบตามนโยบายเหล่านั้น

๒.๓. การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

๒.๓.๑. หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการต้องกำหนดเงื่อนไขการจ้างงานที่รวมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของ สดช.

๒.๓.๒. หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการ ต้องแจ้งรายละเอียดของ "เจ้าหน้าที่ (Office)" ที่บรรจุใหม่ สิ้นสุดการว่าจ้าง หรือมีการโยกย้ายการปฏิบัติงานให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ทราบทันที เพื่อให้การบริหารจัดการบัญชีผู้ใช้งาน (User ID) เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด

๒.๓.๓. ผู้อำนวยการกองของทุกหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ ต้องกำหนดเปลี่ยนแปลง หรือยกเลิกสิทธิของผู้ใช้งานที่เกี่ยวกับ Login หรือ User ID เพื่อให้สอดคล้องกับการเปลี่ยนแปลงสถานะของการว่าจ้างนั้นทันที โดยต้องเก็บข้อมูลให้สามารถตรวจสอบประวัติการเปลี่ยนแปลงสิทธิในระบบสารสนเทศที่เกิดขึ้นเหล่านั้นได้

๒.๓.๔. เมื่อสิ้นสุดการเป็นเจ้าหน้าที่หรือเปลี่ยนลักษณะการปฏิบัติราชการ ผู้ใช้งานจะต้องคืนสินทรัพย์อันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของ สดช. ได้แก่ อุปกรณ์ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ให้แก่ สดช. ในทันทีที่พ้นหน้าที่

๒.๔. การลงนามมิให้เปิดเผยความลับของ สดช. (Confidentiality Agreements)

หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการ ต้องจัดให้มีการลงนามในสัญญาระหว่าง "เจ้าหน้าที่ (Officer)" และ สดช. ว่าจะไม่เปิดเผยความลับของ สดช. โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้าง"เจ้าหน้าที่ (Officer)"นั้น ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า ๑ ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

๓. การอบรมเจ้าหน้าที่

หน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร ร่วมกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ดำเนินการอบรม "เจ้าหน้าที่ (Officer)" ได้รับทราบและตระหนักถึงภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้สามารถป้องกันภัยที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศได้อย่างมีประสิทธิภาพ

๓.๑. การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information Security Education and Training)

๓.๑.๑. หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ร่วมกับหน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร ต้องจัดการประชุม สัมมนา หรืออบรมให้ความรู้แก่ "เจ้าหน้าที่ (Officer)" เกี่ยวกับวิธีปฏิบัติงานเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศและเครือข่ายของ สดช. โดยหลักสูตรการอบรมขึ้นอยู่กับหน้าที่ความรับผิดชอบของ "เจ้าหน้าที่ (Officer)"

๓.๑.๒. หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ มีหน้าที่ในการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบสารสนเทศของ สดช. ด้วย

๓.๑.๓. "เจ้าหน้าที่ (Officer)" ใหม่ของ สดช. ต้องได้รับการอบรมเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้องกับ สดช. โดยต้องเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของ"เจ้าหน้าที่ (Officer)" ด้วย

๓.๒. กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary Process)

สดช. จัดให้มี "มาตรการดำเนินการกับผู้ฝ่าฝืนละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ สดช." โดยมีข้อปฏิบัติ ดังนี้

๓.๒.๑. การฝ่าฝืนระเบียบโดยเล็กน้อยจากความไม่ตั้งใจหรือบังเอิญ โดยก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ส่วนบุคคล ผู้ดูแลระบบจะแจ้งเตือนโดยวาจาหรือจดหมายอิเล็กทรอนิกส์ หรือเป็นลายลักษณ์อักษร แต่หากเป็นการกระทำผิดซ้ำซ้อน สดช. จะพิจารณาลงโทษตามข้อ ๓.๒.๖

๓.๒.๒. การฝ่าฝืนระเบียบขั้นรุนแรง โดยก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ระบบคอมพิวเตอร์ ข้อมูลบนระบบสารสนเทศ เป็นวงกว้าง ที่เกิดจากการละเมิดกฎโดยเจตนาซึ่งสร้างความเสียหายให้แก่ระบบ ยกเว้นการกระทำดังกล่าวได้รับสิทธิ์และได้รับอนุญาต ได้แก่ กรณีการสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) ซ้ำซ้อน สดช. จะพิจารณาลงโทษตามข้อ ๓.๒.๖

๓.๒.๓. การเข้าถึงระบบโดยมิชอบหรือโดยไม่มีอำนาจ (Unauthorized access) แบ่งเป็นการเข้าถึงทั้งในระดับกายภาพ การเข้าถึงระบบสารสนเทศหรือข้อมูล และการเข้าถึงโดยผ่านเครือข่ายสาธารณะ ได้แก่ การลักลอบดักฟังหรือดักเก็บข้อมูลที่มีชั้นความลับ ทั้งในส่วนของการติดตั้งซอฟท์แวร์และฮาร์ดแวร์ที่สามารถดักจับข้อมูล การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) การทดลอง Crack Password การทดลองถอดรหัส การตรวจสอบ Network Traffic โดยไม่ได้รับอนุญาตหรือมิเหตุอันสมควร เป็นต้น ซ้ำซ้อน สดช. จะพิจารณาลงโทษตามข้อ ๓.๒.๖

๓.๒.๔. การสร้างโฮมเพ็จส่วนตัว หรือการส่งต่อข้อมูลที่แสดงออกในลักษณะที่ขัดต่อกฎหมาย กฎระเบียบ และศีลธรรมซ้ำซ้อน สดช. จะพิจารณาลงโทษตามข้อ ๓.๒.๖

๓.๒.๕. การก่อความวุ่นวายที่ขัดต่อกฎระเบียบของ สดช. หรือสร้างความเดือดร้อนรบกวนการทำงานของผู้ใช้งานอื่นๆในระบบเครือข่าย ซ้ำซ้อน สดช. จะพิจารณาลงโทษตามข้อ ๓.๒.๖

๓.๒.๖. กรณีที่ฝ่าฝืนหรือละเมิดข้อกำหนดในระเบียบนี้ และก่อให้เกิดความเสียหายแก่ สดช. หรือบุคคลหนึ่งบุคคลใด สดช. จะพิจารณาดำเนินการทางวินัย

และกฎหมายแก่ผู้ใช้งานหรือหน่วยงานภายนอกนั้นตามความเหมาะสม ดังต่อไปนี้

- ผู้ดูแลระบบจะพิจารณาระงับการใช้งาน และจะแจ้งชื่อผู้ใช้งานที่ทำผิดระเบียบไปยังหน่วยงานต้นสังกัดให้รับทราบ หรือแจ้งผู้บริหาร สดช. รับทราบและพิจารณาตั้งกรรมการสอบสวนข้อเท็จจริง เพื่อพิจารณาจากความรุนแรงหรือความเสียหายที่เกิดขึ้นเป็นรายกรณีไป และ สดช. อาจพิจารณาดำเนินการทางวินัยหรือทางกฎหมายแก่ผู้นั้นตามความเหมาะสม
- ลงโทษทางวินัยต่อผู้ละเมิดตามความเหมาะสม เพื่อมิให้เกิดการละเมิดซ้ำ และในกรณีที่ผู้ละเมิดเป็นหน่วยงานภายนอก ให้ดำเนินการตามกฎหมายต่อไป
- หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อ สดช. อย่างร้ายแรง หรือเข้าข่ายความผิดตามกฎหมาย ให้ส่งตัวไปดำเนินการตามกฎหมายต่อไป
- หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อระบบสารสนเทศและต้องเสียค่าใช้จ่ายในการกู้คืน สดช. สามารถเรียกร้องค่าเสียหายในส่วนนี้ เพื่อเป็นค่าใช้จ่ายในการกู้คืน

ข้อยกเว้น : กิจกรรมที่เกี่ยวกับการทดสอบระบบสารสนเทศ เพื่อตรวจสอบหรือส่งเสริมความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่าย ได้แก่ การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) การทดลอง Crack Password การทดลองถอดรหัส การตรวจสอบ Network Traffic เป็นต้น หากปฏิบัติโดยหน่วยงานหรือบุคคลที่ได้รับอนุญาตหรือโดยหน่วยงานหรือบุคคลได้รับมอบหมายจาก สดช. แล้ว จะไม่ถือว่าเป็นการฝ่าฝืนระเบียบนี้

หมวด ๕
ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security)

มีจุดประสงค์ เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ป้องกันสินทรัพย์สารสนเทศของ สดช. ไม่ให้เกิดการสูญหาย ถูกขโมย เกิดความเสียหาย เกิดการก่อกวนหรือแทรกแซงป้องกันการถูกเปิดเผยโดยไม่ได้รับอนุญาตของสินทรัพย์ของ สดช. และป้องกันไม่ให้กิจกรรมการดำเนินงานต่างๆ ของ สดช. เกิดการติดขัดหรือหยุดชะงัก โดยมีนโยบายดังนี้

นโยบายความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security Policy)

๑. วัตถุประสงค์

เพื่อเป็นมาตรฐานในความมั่นคงปลอดภัยด้านสารสนเทศทางกายภาพที่เกี่ยวกับสถานที่ ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นสินทรัพย์ของ สดช. โดยนโยบายนี้มีผลบังคับใช้กับผู้ใช้งานและหน่วยงาน สดช. ซึ่งมีส่วนเกี่ยวข้องกับการใช้ระบบสารสนเทศของ สดช.

๒. มาตรฐานในการกำหนดบริเวณที่ต้องมีความมั่นคงปลอดภัยด้านสารสนเทศ (Secure Areas)

๒.๑. ทุกหน่วยงาน ตั้งแต่ระดับกองขึ้นไป จะต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวัง ควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้ และประกาศให้รับทราบทั่วกัน (ต้องระบุให้ชัดเจนว่ามีพื้นที่ใช้งานระบบสารสนเทศกี่ประเภทและประเภทใดบ้าง)

๒.๒. ทุกหน่วยงานต้องกำหนดการติดตั้งอุปกรณ์ในพื้นที่ใช้งานระบบสารสนเทศให้สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

๓. การควบคุมการเข้าออก (Physical Entry Controls)

กองต่าง ๆ ต้องดูแลสถานที่พื้นที่ใช้งานระบบสารสนเทศที่อยู่ในความรับผิดชอบ โดยต้องกำหนดมาตรการในการควบคุมการเข้าออกของเจ้าหน้าที่ (Officer) โดยจะได้รับสิทธิ์ในการเข้าออกสถานที่ทำงานได้เฉพาะบริเวณที่กำหนดเท่านั้น ส่วนบุคคลภายนอก การขอเข้าพื้นที่นั้นจะต้องได้รับอนุญาตจากเจ้าของพื้นที่เป็นกรณีไป ซึ่งมีแนวทางปฏิบัติเบื้องต้น ดังนี้

๓.๑. เจ้าหน้าที่ (Officer) จะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนดเท่านั้น

๓.๒. หากมีบุคคลภายนอก ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตหรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้จะต้องแสดงบัตรประจำตัวที่ สดช. ออกให้ หรือบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่)

๔. ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ (Securing Offices, Rooms and Facilities)

๔.๑. ผู้อำนวยการกองแต่ละหน่วยงาน ต้องจัดให้มีมาตรการความมั่นคงปลอดภัยด้านสารสนเทศให้กับสำนักงาน ห้องทำงานและเครื่องมือต่างๆ ได้แก่ เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก สำนักงานจะต้อง **ไม่มีป้าย** หรือ **สัญลักษณ์** ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณดังกล่าว ประตูหน้าต่างของสำนักงานต้องใส่กุญแจเมื่อไม่มีคนอยู่ เครื่องโทรสารหรือเครื่องถ่ายเอกสารต้องแยกออกมาจากบริเวณดังกล่าว เป็นต้น โดยมีแนวทางปฏิบัติ ได้แก่ กั้นพื้นที่อย่างรอบด้าน (ได้แก่ ติดตั้งผนัง ติดตั้งเหล็กดัด ล็อคประตูที่ใช้ดอกกุญแจ หรือมีระบบ Access Control) และปรับปรุงให้มีความเหมาะสมทางสภาวะแวดล้อม (ได้แก่ ติดตั้งระบบปรับอากาศ การควบคุมความชื้น เป็นต้น)

๔.๒. การปฏิบัติงานในพื้นที่ควบคุม (Working in Control Areas)

๔.๒.๑. ผู้อำนวยการกองแต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวิดีโอในบริเวณนั้น เป็นต้น

๔.๒.๒. ต้องมีป้ายประกาศข้อความ **"ห้ามเข้าก่อนได้รับอนุญาต" "ห้ามถ่ายภาพหรือวิดีโอ"** และ **"ห้ามสูบบุหรี่"** บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

๔.๓. การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery, and Loading Areas)

หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่ ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยหน่วยงานภายนอก เพื่อป้องกันการเข้าถึงสินทรัพย์ของ สดช. โดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ต้องจัดเป็นบริเวณแยกออกมาต่างหาก

๔.๔. ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

๔.๔.๑. ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

๔.๔.๒. ผู้อำนวยการกองที่เป็นเจ้าของระบบงาน ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ ได้แก่ จัดให้มีการซ่อมบำรุงปีละ ๑ ครั้ง หรือระบบที่สำคัญมากอาจจะกำหนดให้มีการบำรุงรักษาทุกสิ้นเดือน เป็นต้น

๔.๔.๓. ผู้อำนวยการกองแต่ละหน่วยงาน ต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของ สดช. ได้แก่ Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน โดยต้องปฏิบัติตามระเบียบในการใช้งานการยืม-คืน

๔.๔.๔. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

- กำหนดเลขไอพีแอดเดรสที่เจาะจง (Fix IP address) ให้อุปกรณ์ที่ขึ้นทะเบียนไว้และบันทึกเป็นบัญชีเก็บไว้
- ใช้ซอฟต์แวร์บริหารจัดการอุปกรณ์เครือข่าย (Monitoring) โดยระบุอุปกรณ์จากเลขไอพีแอดเดรสเพื่อดูพฤติกรรมการใช้งานรวมถึงควบคุมการเข้าถึงบริการ

๔.๔.๕. ผู้อำนวยการกองแต่ละหน่วยงาน ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ (Secure Disposal of Reuse of Equipment) ซึ่งมีข้อมูลสำคัญเก็บไว้ ได้แก่ ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น ทั้งนี้ เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว ซึ่งมีแนวทางปฏิบัติ ดังนี้

ระดับความปลอดภัย	สื่อที่อ่านเขียนด้วยแสง (Optical Media)	สื่ออิเล็กทรอนิคส์ (Electronic Media)
๑ (ลับ)	ทำลายสื่อโดยอุปกรณ์ทำลายสื่อเฉพาะ	ลบล้างข้อมูล และสามารถทิ้งได้
๒ (ลับมาก)	ทำลายสื่อโดยอุปกรณ์ทำลายสื่อเฉพาะ	ลบล้างข้อมูล หรือทำลายสื่อโดยอุปกรณ์ทำลายสื่อเฉพาะ
๓ (ลับที่สุด)	ทำลายสื่อโดยอุปกรณ์ทำลายสื่อเฉพาะ	ลบล้างข้อมูล และทำลายสื่อโดยอุปกรณ์ทำลายสื่อเฉพาะ
๔ (ข้อมูลส่วนบุคคล)	ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๓๓ และ ๓๗	ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๓๓ และ ๓๗

๔.๕. ระบบป้องกันภัย

ผู้อำนวยการกองแต่ละหน่วยงาน ต้องกำหนดให้มีระบบป้องกันภัย โดยมีแนวทางปฏิบัติ ดังนี้

๔.๕.๑. ต้องมีระบบเตือนภัย/ป้องกันภัย ได้แก่ ระบบดับเพลิง หรือระบบเตือนอัคคีภัย

๔.๕.๒. ต้องมีการวางแผน และซักซ้อมการปฏิบัติรับมือกับภัย

๔.๕.๓. ห้ามกระทำการใดๆ ให้เกิดมีประกายไฟหรือเปลวไฟ

๔.๕.๔. ระบบที่สำคัญของ สดช. จะต้องมีการปฏิบัติตามนโยบายแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ เพื่อป้องกันผลกระทบที่จะเกิดขึ้นกับการปฏิบัติราชการของ สดช.

๔.๖. การจัดการระบบไฟฟ้า (Power System) และระบบสายสัญญาณ (Data Cable)

ผู้อำนวยการกองแต่ละหน่วยงาน ต้องทราบถึงการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในพื้นที่ใช้งานระบบสารสนเทศที่อยู่ในความรับผิดชอบ และจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่หรือบุคคลที่มีสิทธิเท่านั้น

๔.๗. การควบคุมทั่วไป (General Controls)

๔.๗.๑. "เจ้าหน้าที่ (Officer)"ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศที่เป็น "ชั้นลับที่สุด" หรือ "ขั้นลับมาก" หรือ "ชั้นลับ" ไว้ในที่สามารถพบเห็นได้ง่าย (Clear Desk) โดยจัดเก็บไว้ในที่ที่ปลอดภัย นอกจากนี้ ตู้จ่ายเอกสารหรือจดหมายและเครื่องโทรสารจะต้องได้รับการดูแลให้ปลอดภัยด้วย

๔.๗.๒. การเคลื่อนย้ายสินทรัพย์ของ สดช. ผู้ดูแลระบบแต่ละหน่วยงาน ต้องทำเป็นบันทึกและขออนุญาตจากผู้อำนวยการกองอย่างถูกต้องในการเคลื่อนย้าย ซึ่งมีแนวทางปฏิบัติ ดังนี้

๔.๗.๒.๑. ผู้ที่รับผิดชอบในการย้ายสถานที่ทำงาน ต้องตรวจสอบความเรียบร้อยครั้งสุดท้ายทันทีหลังจากที่ทำการย้ายของเสร็จสิ้น รวมทั้งตรวจสอบพื้นที่และสินทรัพย์ด้วย การย้ายสถานที่ทำงาน เป็นช่วงเวลาที่ต้องระวังเรื่องการรักษาความปลอดภัยที่อาจมีการมองข้ามได้ โดยเฉพาะช่วงเวลาที่ต้องเร่งจัดการย้ายให้เสร็จสิ้น จึงต้องให้ความระมัดระวังเพราะอาจมีการผ่อนปรนมาตรการรักษาความปลอดภัยต่อข้อมูลที่มีความสำคัญหรือต่อระบบเครือข่ายของ สดช. ได้

๔.๗.๒.๒. ข้อมูลที่มีความสำคัญมาก รวมถึงข้อมูลในคอมพิวเตอร์แบบพกพา (Notebook) ต้องมีการเคลื่อนย้ายโดยผู้เป็นเจ้าของข้อมูลเท่านั้น ห้ามเคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล

๔.๗.๒.๓. ผู้ใช้งานจะต้องแน่ใจว่าข้อมูลสำคัญใดๆ ต้องมีการป้องกันการเข้าถึงข้อมูลจากผู้ที่ไม่ใช่เจ้าของข้อมูล ได้แก่ การเข้ารหัสไฟล์ เป็นต้น

๔.๗.๒.๔. ผู้ที่มีส่วนร่วมในการเคลื่อนย้ายสถานที่ทำงานจะต้องมีการตรวจตราสถานที่ย้ายสินทรัพย์ออก เพื่อให้มั่นใจได้ว่าไม่มีข้อมูลใดหลงเหลืออยู่ มีการกำหนดความรับผิดชอบในการดูแลให้ครอบคลุมส่วนที่เก็บเอกสาร (ได้แก่ ตู้เก็บแฟ้มเอกสาร, ห้องเก็บรักษาแฟ้มข้อมูล, ห้องนิรภัย เป็นต้น)

๔.๗.๒.๕. ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่างๆ เมื่อมีการเปลี่ยนแปลงหรือเคลื่อนย้าย เพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของ สดช.

หมวด ๖
การบริหารจัดการด้านการสื่อสารและการดำเนินงาน
(Communications and Operations Management)

จุดประสงค์ เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย ให้เป็นไปตามข้อตกลง ลดความเสี่ยงจากการล้มเหลวของระบบ ป้องกันซอฟท์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟท์แวร์ที่ไม่ประสงค์ดี ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายสินทรัพย์สารสนเทศโดยไม่ได้รับอนุญาต รักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกัน สร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ และตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่เหมาะสม และไม่ได้รับอนุญาต โดยประกอบด้วย

- นโยบายความมั่นคงปลอดภัยด้านเครือข่ายคอมพิวเตอร์
- นโยบายการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์
- นโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์
- นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
- นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา
- นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล
- นโยบายการแลกเปลี่ยนสารสนเทศ
- นโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์

ซึ่งมีรายละเอียดดังนี้

นโยบายความมั่นคงปลอดภัยด้านเครือข่ายคอมพิวเตอร์
(Computer Network Security Policy)

๑. วัตถุประสงค์

นโยบายนี้กำหนดขึ้นเพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างถูกต้องและปลอดภัย จึงจำเป็นต้องมีการบริหารจัดการเครือข่ายของ สดช. ให้มีความมั่นคงปลอดภัยด้านความถูกต้อง การเก็บรักษาเป็นความลับ และความพร้อมในการใช้งาน นโยบายดังกล่าวนี้มีผลบังคับใช้กับ “เจ้าหน้าที่” ของ สดช. และหน่วยงานภายนอกที่ขออนุญาตใช้งานระบบสารสนเทศของ สดช.

๒. มาตรฐานทั่วไป

๒.๑. การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน (Operational Procedures and Responsibilities)

๒.๑.๑. ผู้อำนวยการกองที่เป็นเจ้าของระบบงาน ต้องจัดทำคู่มือและขั้นตอนการปฏิบัติงานของระบบงานนั้นๆ โดยมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่าย

๒.๑.๒. ในกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ หน่วยงานที่ดูแลระบบสารสนเทศนั้นต้องทำการบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่นๆ ที่เกี่ยวข้องทราบ

๒.๑.๓. ผู้อำนวยการกองที่เป็นเจ้าของระบบงาน ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบสารสนเทศและเครือข่ายที่หน่วยงานนั้นๆ รับผิดชอบ

๒.๑.๔. ผู้อำนวยการกองที่เป็นเจ้าของระบบงาน ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้ละเมิด

๒.๑.๕. ผู้อำนวยการกองที่เป็นเจ้าของระบบงาน ต้องแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบสารสนเทศออกจากเครื่องที่ทำงานจริงหรือเครื่องให้บริการ

๒.๑.๖. ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอก สดช. หน่วยงานที่รับผิดชอบต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิของผู้ใช้งานที่ได้รับ และตรวจสอบการใช้งานอย่างสม่ำเสมอ

๒.๒. การบริหารจัดการการเปลี่ยนแปลงในการให้บริการต่อหน่วยงานภายนอก (Managing Changes to Third Party Services)

ผู้อำนวยการกอง ที่เป็นเจ้าของระบบงานต้องปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก ได้แก่ การปรับปรุงหรือพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก โดยต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ก่อนจึงจะสามารถดำเนินการได้ รวมทั้งปรับปรุงเอกสารที่เกี่ยวข้องให้ทันสมัย เมื่อมีการเปลี่ยนแปลงสารสนเทศ

๒.๓. การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance)

๒.๓.๑. หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ต้องมีการวางแผนกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต โดยสำรวจความต้องการทรัพยากรสารสนเทศให้ครบถ้วน เพื่อไม่ให้โครงการเกิดความล่าช้าในการจัดซื้อจัดหา และต้องคำนึงถึงความมั่นคงปลอดภัยของสารสนเทศด้วย ซึ่งจะทำให้ระบบมีความมั่นคงปลอดภัยและไม่เกิดค่าใช้จ่ายในภายหลัง

๒.๓.๒. ผู้อำนวยการกองที่เป็นเจ้าของระบบงาน ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน ได้แก่ การตรวจรับระบบตาม TOR ที่ได้กำหนดไว้ เป็นต้น

๒.๔. การป้องกันซอฟต์แวร์และสารสนเทศของ สดช. ให้ปลอดภัยจากการถูกทำลายจากซอฟต์แวร์ที่ไม่ประสงค์ดี (Protection Against Malicious Software)

หน่วยงานต่างๆ ต้องจัดให้มีการติดตั้งและใช้งานซอฟต์แวร์ป้องกันไวรัส เพื่อป้องกันความเสียหายและการรั่วไหลของข้อมูล โดยมีแนวทางปฏิบัติดังนี้

๒.๔.๑. ห้ามนำเครื่องคอมพิวเตอร์ ซอฟต์แวร์หรือข้อมูลที่มีความเสี่ยงต่อการติดมาลแวร์มาติดตั้งใช้งาน

๒.๔.๒. ต้องสำรองข้อมูลสำคัญเก็บไว้ในที่ที่ปลอดภัย ได้แก่ สื่อจัดเก็บข้อมูลแบบพกพา หรือเนื้อที่บนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ สดช. จัดสรรไว้ให้ เพื่อลดปัญหาการกู้คืนสภาพข้อมูลที่ถูกทำลายโดยไวรัส

๒.๔.๓. ห้ามผู้ใช้งานปรับแต่ง หรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันไวรัสที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่ สดช. จัดหาให้

๒.๔.๔. ผู้ใช้งานต้องมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบการ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

๒.๔.๕. ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อสงสัยว่ามีการติดไวรัส

๒.๕. การสำรองข้อมูล

๒.๕.๑. ผู้ดูแลระบบสารสนเทศที่สำคัญนั้นๆ ต้องสำรองข้อมูลที่สำคัญเก็บไว้ตามระยะเวลาที่เหมาะสม

๒.๕.๒. ผู้ดูแลระบบต้องบันทึกรายละเอียดการสำรองข้อมูลโดยมีรายละเอียด เวลาเริ่มต้นและสิ้นสุด ชื่อผู้ทำการสำรองข้อมูล และชนิดของข้อมูลที่บันทึก

๒.๕.๓. กรณีที่เกิดการผิดพลาดในการสำรองข้อมูล ผู้สำรองข้อมูลต้องบันทึกรายละเอียดของข้อผิดพลาดที่เกิดขึ้นพร้อมแนวทางแก้ไข

๒.๕.๔. ผู้ดูแลระบบต้องมีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสม เมื่อระบบงานถูกโจมตี หรือเกิดความเสียหายเพื่อให้สามารถกู้ข้อมูลกลับคืนได้

๒.๕.๕. ผู้ดูแลระบบต้องเข้ารหัสข้อมูลที่สำรองตามชั้นความลับ โดยใช้เทคโนโลยีที่เหมาะสม เพื่อป้องกันข้อมูลสำรองถูกเปิดเผย

๒.๖. การบริหารจัดการเครือข่าย (Network Management)

๒.๖.๑. ผู้ดูแลระบบ ต้องบริหารจัดการความมั่นคงปลอดภัยในเครือข่าย ซึ่งมีแนวทางปฏิบัติดังนี้

๒.๖.๑.๑. **ระบบเครือข่ายภายใน** อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่ายเพื่อการทำงานภายใน สดช. ได้แก่ Router หรือ Switch มีข้อปฏิบัติดังนี้

- อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมโยงเครือข่าย ต้องปิด Service Port ที่ไม่จำเป็น และในการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่าเริ่มต้น ได้แก่ Default Community, Default Username และ Default Password

- การเชื่อมโยงเครือข่ายเพื่อใช้งานระบบต่างๆ จะสามารถกระทำได้ก็ต่อเมื่อได้รับอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ การเชื่อมโยงเครือข่ายเองโดยพลการ หากทำให้เกิดความเสียหายกับระบบเครือข่ายจะต้องถูกลงโทษตามที่กำหนดไว้
- ผู้ดูแลระบบจะต้องมีแผนดำเนินการบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์ เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ
- ผู้ดูแลระบบมีหน้าที่ในการติดตั้งอุปกรณ์ซอฟต์แวร์ระบบ การเข้ารหัสข้อมูลอัตโนมัติหรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่างๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ
- ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

๒.๖.๑.๒. **ระบบ Remote Access** อุปกรณ์ Remote Access Server (RAS) ที่ติดตั้งใช้งานใน Remote Area หรือเพื่อการทำงานกับหน่วยงานภายนอก ได้แก่ Remote Access Server (RAS), Remote VPN, Remote Router มีข้อปฏิบัติดังนี้

- อุปกรณ์ RAS จะต้องทำ Hardening และบันทึกการทำ Configuration Set up ของอุปกรณ์ RAS ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง
- เมื่อเสร็จสิ้นการทดสอบการใช้งานอุปกรณ์ RAS แล้วให้ลบ User/Password ที่ใช้ในงานทดสอบทันที
- อุปกรณ์ RAS ที่สามารถ Management ทาง Remote Terminal ได้จะต้องไม่ใช้ค่าเริ่มต้น ได้แก่ Default Community, Default Username และ Default Password

๒.๖.๑.๓. **อุปกรณ์ Server** อุปกรณ์ Server ที่ติดตั้งเพื่อการทำงานภายใน สดช. มีข้อ ปฏิบัติดังนี้

- ผู้ดูแลระบบต้องเปลี่ยนค่าบัญชีผู้ใช้งานและรหัสผ่านที่ถูกกำหนดมาตั้งแต่เริ่มต้น (Default Username/Default Password)
- ต้องทำ Hardening และบันทึกการทำ Configuration Set up ของอุปกรณ์ Server และจัดทำเป็นเอกสารทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง
- ต้องเปิด Port ที่จำเป็นเท่านั้น ส่วน Port ที่ไม่ใช้งานต้องปิดทั้งหมด
- ต้องบันทึกการติดตั้ง Service Patch ทุกครั้ง

- ต้องไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ
- เมื่อ Log on เพื่อใช้งาน Server ผ่าน Console แล้วเมื่อเลิกใช้งานจะต้อง Logoff User นั้นโดยทันที
- ผู้ดูแลระบบจะต้องสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยเดือนละครั้ง และทดสอบการสำรองข้อมูลอย่างน้อยปีละ ๒ ครั้ง โดยต้องสอดคล้องกับความสำคัญของระบบ

๒.๖.๑.๔. **อุปกรณ์ PC Terminal** มีข้อปฏิบัติดังนี้

- ต้องเปิด Port ที่จำเป็นเท่านั้น ส่วน Port ที่ไม่ใช้งานต้องปิดทั้งหมด
- ต้องติดตั้ง Protocol เฉพาะที่ทำงานร่วมกับ Server เท่านั้น
- ต้องบันทึกการติดตั้ง Service Patch ทุกครั้ง
- เมื่อ Log on เพื่อใช้งาน Server ผ่าน Terminal Console แล้วเมื่อเลิกใช้งานจะต้อง Logoff User นั้นโดยทันที

๒.๖.๒. การป้องกันการใช้งานเครือข่าย

๒.๖.๒.๑. ห้ามนำอุปกรณ์เครือข่ายมาติดตั้งกับระบบเครือข่ายของ สดช. โดยไม่รับอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ

๒.๖.๒.๒. ห้ามผู้ใช้งานเครือข่ายกระทำการใดๆ ที่รบกวนระบบเครือข่าย ได้แก่ การเปิดใช้งาน Service DHCP เพื่อเชื่อมต่อเข้ากับระบบเครือข่ายของ สดช. เอง

๒.๖.๒.๓. ตรวจสอบการเชื่อมต่อเครือข่ายและจำกัดสิทธิ์ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

๒.๖.๒.๔. ตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่ายด้วยอุปกรณ์ไฟล์วอล และระบบตรวจจับการบุกรุก (IPS/IDS)

๒.๖.๒.๕. ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต โดยมีการควบคุมการเข้าถึงพอร์ตที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และเปิดใช้บริการ (Service) ที่จำเป็นเท่านั้น เช่น ssh sftp และ ping เป็นต้น

๒.๖.๒.๖. มีการดูแลตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๒.๖.๒.๗. มีการควบคุมการเข้าถึงระบบสารสนเทศด้วยการพิสูจน์ตัวตน (Authentication) โดยเครื่องคอมพิวเตอร์ของผู้ใช้งานจะต้องมีการกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศและมีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร ก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก สดช. สามารถเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศของ สดช. ได้

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของ สดช. โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สายของ สดช.

๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย มีแนวทางปฏิบัติ ดังนี้

๒.๑. **"ผู้ใช้"** ต้องไม่นำอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless Access Point) มาติดตั้งใช้งานเองโดยไม่ได้รับความเห็นชอบจาก ขศ.

๒.๒. **"ผู้ใช้"** ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ สดช. จะต้องทำการลงทะเบียนกับ **"ผู้ดูแลระบบ"** ของ ขศ. และต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการ ขศ.

๒.๓. **"ผู้ใช้"** จะต้องปฏิบัติตามคำแนะนำการใช้งานของ ขศ. เพื่อการรักษาความมั่นคงปลอดภัยโดยเคร่งครัด

๒.๔. **"ผู้ดูแลระบบ"** ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้ในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๕. **"ผู้ดูแลระบบ"** ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับ/ส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๒.๖. **"ผู้ดูแลระบบ"** ต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและต้องสำรวจว่าสัญญาณรั่วไหลออกไปภายนอก

๒.๗. **"ผู้ดูแลระบบ"** ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณไร้สายมาใช้งาน

๒.๘. **"ผู้ดูแลระบบ"** ต้องเปลี่ยนค่า Login ID และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ Login ID และรหัสผ่านที่มีความปลอดภัยเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๒.๙. **"ผู้ดูแลระบบ"** ต้องมีการติดตั้งอุปกรณ์ป้องกันการเข้าถึงเครือข่าย (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายใน

๒.๑๐. **"ผู้ดูแลระบบ"** ต้องกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สาย ติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

๒.๑๑. **"ผู้ดูแลระบบ"** ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

นโยบายการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์
(Internet and E-mail Policy)

๑. วัตถุประสงค์

นโยบายนี้ ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานรับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์(E-mail) ให้มีการป้องกันการเข้าถึงหรือการเปลี่ยนแปลงแก้ไขข้อความใน E-mail โดยไม่ได้รับอนุญาต และการรักษาข้อมูลและทรัพยากรต่างๆ ของ สดช. ให้มีความมั่นคงปลอดภัย

๒. การใช้งานอินเทอร์เน็ต

๒.๑. **"ผู้ดูแลระบบ"** ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ สดช. จัดสรรไว้เท่านั้น ได้แก่ Proxy, Firewall, IPS-IDS เป็นต้น **"ผู้ใช้"** ต้องไม่ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ได้แก่ ADSL **ยกเว้น**มีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการศูนย์ข้อมูลเศรษฐกิจและสังคมดิจิทัล เป็นลายลักษณ์อักษร

๒.๒. เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์พกพา และอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ ก่อนทำการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการและโปรแกรม Web Browser

๒.๓. ในการรับ/ส่งข้อมูลคอมพิวเตอร์ผ่านทางระบบเครือข่ายอินเทอร์เน็ตจะต้องมีการตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับ/ส่งข้อมูลทุกครั้ง

๒.๔. **"ผู้ใช้"** ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ สดช. เพื่อหาประโยชน์ส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ผิดกฎหมาย เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือ เว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๒.๕. **"ผู้ใช้"** จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ สดช.

๒.๖. **"ผู้ใช้"** ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ผิดกฎหมาย ข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ สดช.

๒.๗. **"ผู้ใช้"** ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ สดช.ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบเครือข่ายอินเทอร์เน็ต

๒.๘. **"ผู้ใช้"** ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านระบบเครือข่ายอินเทอร์เน็ต

๒.๙. **"ผู้ใช้"** ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพบุคคลอื่น ที่เกิดจากการสร้างขึ้น ตัดต่อ แต่งเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้บุคคลอื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๒.๑๐. **"ผู้ใช้"** มีหน้าที่ที่จะตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนระบบเครือข่ายอินเทอร์เน็ต ก่อนนำข้อมูลไปใช้

๒.๑๑. **"ผู้ใช้"** ต้องระมัดระวังการดาวน์โหลดโปรแกรม ซึ่งรวมถึง Patch หรือ Fixes ต่างๆ และรูปภาพ หรือเนื้อหา (Content) ที่มาจากระบบเครือข่ายอินเทอร์เน็ต โดยต้องไม่ละเมิดกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

๒.๑๒. **"ผู้ใช้"** ต้องไม่บอกสถานที่หรือข้อมูลส่วนตัว ได้แก่ ชื่อ ที่อยู่ เบอร์โทรศัพท์ ประกาศผ่านระบบเครือข่ายอินเทอร์เน็ต

๒.๑๓. การใช้งานเว็บบอร์ด (Web board) ของ สดช. "ผู้ใช้" ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ สดช.

๒.๑๔. ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ สดช. การทำลายความสัมพันธ์กับเจ้าหน้าที่และหน่วยงานอื่นๆ

๒.๑๕. หลังจากใช้งานระบบเครือข่ายอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๒.๑๖. ไม่ใช้งานโปรแกรมประเภทติดต่อสื่อสารข้อความ ได้แก่ Facebook, Twitter ในเรื่องส่วนตัว ระหว่างเวลาทำงานหรือเวลา ๘.๓๐-๑๒.๐๐ น. และ ๑๓.๐๐-๑๖.๓๐ น.

๒.๑๗. ไม่ติดตั้งและใช้งานโปรแกรมประเภทตรวจสอบ หรือ รบกวนการทำงานของระบบเครือข่ายคอมพิวเตอร์ ได้แก่ โปรแกรม Bit torrent หรือ โปรแกรมตรวจสอบหรือตรวจจับข้อมูลในระบบเครือข่าย ก่อนได้รับอนุญาตจากผู้มีอำนาจ และ ขศ. เป็นลายลักษณ์อักษร

๒.๑๘. ไม่ควรเข้าใช้งาน Website ที่มีการส่งข้อมูลแบบ Streaming ที่ใช้ Bandwidth สูง ได้แก่ Online Radio, Online TV , Online Video เป็นต้น ในระหว่างเวลาทำงานหรือเวลา ๘.๓๐-๑๒.๐๐ น. และ ๑๓.๐๐-๑๖.๓๐ น. เนื่องจากจะทำให้การรับ-ส่งข้อมูลในระบบเครือข่ายล่าช้าและกระทบต่อการปฏิบัติงานของเจ้าหน้าที่คนอื่น ๆ ทั้งนี้หากหน่วยงานมีความจำเป็นต้องใช้เข้าถึง Website ที่มีการส่งข้อมูลแบบ Streaming ที่ใช้ Bandwidth สูง ในช่วงเวลาทำงาน ให้แจ้ง ขศ. เพื่อพิจารณาดำเนินการต่อไป

๓. การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

๓.๑. "ผู้ดูแลระบบ" ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ สดช. ให้เหมาะสมกับการเข้าใช้ บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ ได้แก่ ในกรณีที่ผู้ใช้งานลาออก ผู้ดูแลระบบจะต้องพิจารณาเพื่อแก้ไขสิทธิ์ในการใช้งานจดหมายอิเล็กทรอนิกส์ของผู้ใช้งานที่ลาออกทันที

๓.๒. "ผู้ดูแลระบบ" ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่ และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของ สดช.

๓.๓. "ผู้ใช้" ที่ต้องการใช้งานจดหมายอิเล็กทรอนิกส์ต้องติดต่อ ขศ. เพื่อกรอกรายละเอียดในแบบฟอร์ม e-mail Account

๓.๔. สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (default password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๓.๕. การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติดังนี้ รหัสผ่านนั้นจะต้องมีทั้งตัวอักษร ตัวเลข และสัญลักษณ์พิเศษ ประสมกัน และกำหนดความยาวของรหัสผ่านอย่างน้อย ๘ ตัวอักษรเพื่อความปลอดภัย

๓.๖. ระบบจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของ "x" หรือ "●" ในการพิมพ์แต่ละตัวอักษร

๓.๗. "ผู้ใช้" ต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์

๓.๘. "ผู้ใช้" ต้องมีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอและเคร่งครัด ได้แก่ เปลี่ยนรหัสผ่านทุก ๖ เดือน

๓.๙. "ผู้ใช้" ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อ สดช. หรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาผลประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของ สดช.

๓.๑๐. "ผู้ใช้" ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์(e-mail Address) ของผู้อื่น เพื่ออ่าน รับ/ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๓.๑๑. "ผู้ใช้" ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ สดช. เพื่อการทำงานของ สดช.

๓.๑๒. "ผู้ใช้" ต้องไม่ประกาศ รหัสผ่าน (Password) ของ e-mail Account ของตนเองผ่านเครือข่ายอินเทอร์เน็ต

๓.๑๓. "ผู้ใช้" จะต้องปฏิบัติตามคำชี้แจงหรือข้อเสนอแนะของ ขศ. อย่างเคร่งครัด ในกรณีที่มีการปรับปรุงหรือตรวจซ่อมเครื่องคอมพิวเตอร์ให้บริการจดหมายอิเล็กทรอนิกส์

๓.๑๔. "ผู้ใช้" หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการ log off ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๓.๑๕. "ผู้ใช้" ต้องไม่ส่งไฟล์ที่มีขนาดใหญ่เกิน ๒๕ เมกกะไบท์

๓.๑๖. "ผู้ใช้" ต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file ได้แก่ .exe, .com เป็นต้น

๓.๑๗. "ผู้ใช้" ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๓.๑๘. "ผู้ใช้" ต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับ/ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของ สดช. ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

๓.๑๙. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อของจดหมายอิเล็กทรอนิกส์

๓.๒๐. "ผู้ใช้" ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๓.๒๑. "ผู้ใช้" ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

นโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์
(Corporate Antivirus for PC and Notebook Computer Policy)

๑. วัตถุประสงค์

นโยบายนี้ได้ถูกจัดทำขึ้นเพื่อต้องการให้เกิดความมั่นคงปลอดภัยของระบบสารสนเทศ สดช. ช่วยลดภาวะเสี่ยงของปัญหาที่จะเกิดขึ้นกับระบบสารสนเทศทั้งในส่วนของอุปกรณ์และระบบฐานข้อมูลของ สดช. ทำให้การทำงานมีความต่อเนื่องไม่เกิดการหยุดชะงัก

๒. แนวทางปฏิบัติการใช้งานระบบป้องกันไวรัส (Corporate Antivirus)

เพื่อลดความเสี่ยงและปัญหาการติดไวรัสในเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์แม่ข่ายของ สดช. รวมทั้งให้มีหลักการปฏิบัติที่สอดคล้องกัน ต้องปฏิบัติดังต่อไปนี้

๒.๑. ให้ระบบ Corporate Antivirus ซึ่งหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เป็นผู้จัดหาเป็นระบบ Antivirus หลักสำหรับเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา(Notebook) (ระบบปฏิบัติการ MS Windows) ที่เป็นทรัพย์สินของ สดช. โดยมีหลักพิจารณาให้ความสำคัญ (High Priority) กับกลุ่มต่อไปนี้เป็นอย่างน้อย

๒.๑.๑. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา(Notebook) ที่ต้องติดต่อใช้งานกับระบบงานสำคัญ และหรือระบบสารสนเทศที่มีข้อมูลความลับของ สดช. ได้แก่ ERP, HR, EIS, MIS, Billing, CRM เป็นต้น

๒.๑.๒. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา(Notebook) ที่ใช้ทำงานกับข้อมูลสำคัญ หรือข้อมูลอันเป็นความลับของ สดช. ได้แก่ การจัดทำข้อกำหนดการทำร่างสัญญาทางกฎหมาย การทำงานด้านบัญชี/การเงิน การประมูล/เปิดซอง เป็นต้น

๒.๑.๓. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา(Notebook) ที่ใช้ควบคุมระบบงานสำคัญ (System Management) ของ สดช.

๒.๑.๔. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา(Notebook) ของผู้บริหารระดับต้นขึ้นไปรวมถึงอุปกรณ์คอมพิวเตอร์ของเลขานุการ/หน้าห้องผู้ใช้งาน

๒.๑.๕. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา(Notebook)ที่ใช้พัฒนาซอฟท์แวร์ หรือใช้ทำงาน System Administration หรือ Network Administration

๒.๑.๖. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา(Notebook) ของผู้ใช้งานที่ต้องทำหน้าที่ติดต่อกับหน่วยงานภายนอก หรือที่ต้องเชื่อมต่อกับทั้ง Intranet และ Internet เพื่อประโยชน์ทางราชการหรือภาพลักษณ์ของ สดช.

๒.๒. กำหนดให้หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศร่วมกับหน่วยงานที่เกี่ยวข้องเป็นผู้ประสานงานและดำเนินการที่เกี่ยวข้อง ได้แก่

๒.๒.๑. แจ้งให้หน่วยงานภายใน สดช. รับทราบโดย หนังสือเวียน เสียงตามสาย หรือสื่ออื่นตามความเหมาะสม

๒.๒.๒. หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศเป็นผู้รับผิดชอบดูแล บำรุงรักษา กำกับความทันสมัย Patch ปิดช่องโหว่ในระบบ Corporate Antivirus เสนองบประมาณผ่านหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ปรับเพิ่มลดจำนวน Licenses อนุญาตหรือจำกัดการใช้งานของผู้ใช้งาน และดำเนินการในส่วนที่เกี่ยวข้อง

๒.๒.๓. หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศดำเนินการให้การ Update Virus Signature เป็นไปอย่างอัตโนมัติ และจัดทำ Configuration ของระบบ Antivirus ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

๒.๒.๔. หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศจัดทำสถิติ กราฟ และผลการใช้งาน แล้วส่งไปยังหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เพื่อรวบรวมข้อมูล

๒.๓. หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ จะต้องปฏิบัติตามนโยบายเกี่ยวกับการใช้งานระบบ Antivirus ที่ใช้งานภายใน Intranet ดังนี้

๒.๓.๑ หากเป็น Antivirus ที่ไม่มีลิขสิทธิ์ถูกต้อง สดช. จะไม่อนุญาตให้ใช้งาน ทั้งนี้หน่วยงานต้องหันมาใช้ระบบ Corporate Antivirus ของหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศเป็นหลัก

๒.๓.๒ หากระบบ Antivirus เดิมยังไม่หมดสัญญาการบำรุงรักษา (Virus Signature & Scan Engine Maintenance) อนุโลมให้ใช้งานระบบเดิมต่อไปจนกว่าจะหมดสัญญา โดยเมื่อหมดสัญญาการบำรุงรักษาแล้วต้องพิจารณายกเลิกการใช้งานระบบ Antivirus ที่ไม่มี Maintenance ดังกล่าวและหันมาใช้งานระบบ Corporate Antivirus ของหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ (หากไม่มีปัญหาทางเทคนิคอื่นใด) เนื่องจากระบบ Antivirus ที่ไม่สามารถ Update Signature File หรือ Scan Engine ได้แล้วจะหมดประสิทธิภาพภายในระยะเวลาอันรวดเร็ว

๒.๔. หากมีหน่วยงานใดที่ต้องการใช้งานระบบ Antivirus แต่ไม่สามารถใช้รุ่นหรือ Version ที่หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศมีอยู่ได้ ให้หน่วยงานเสนอการตั้งงบประมาณผ่านหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ และต้องมีความเห็นชอบของหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศประกอบ

๒.๕. กรณี Antivirus ที่ใช้กับระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (ได้แก่ Windows Server, Unix, Linux เป็นต้น) หรือสำหรับอุปกรณ์อื่นที่ไม่ใช่เครื่องคอมพิวเตอร์ (PC) และ เครื่องคอมพิวเตอร์พกพา (Notebook) (ได้แก่ Appliance, Network Equipment เป็นต้น) หากหน่วยงานใดมีความจำเป็นต้องใช้งานภายใน (ไม่ใช่เพื่อการให้บริการลูกค้า) ให้ส่งเรื่องให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ พิจารณาเป็นรายกรณีไป

๒.๖. ในกรณีตรวจพบว่าผู้ใช้งาน หรือ หน่วยงาน ไม่ปฏิบัติตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศสามารถเข้าตรวจสอบสาเหตุได้ และ จะดำเนินการแจ้งผลการตรวจสอบให้แก่ผู้อำนวยการกอง และผู้บริหารระดับสูงด้านสารสนเทศทราบต่อไป

นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal computer)

๑. วัตถุประสงค์

กำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ (User) ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้ต้องทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของ สดช. ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๑. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล มีแนวทางปฏิบัติ ดังนี้

๑.๑. เครื่องคอมพิวเตอร์ที่ สดช. อนุญาตให้ **"ผู้ใช้"** ใช้งาน เป็นสินทรัพย์ของ สดช. ดังนั้นผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ เพื่องานของ สดช.

๑.๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของ สดช. ต้องเป็นโปรแกรมที่ สดช. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑.๓. ไม่อนุญาตให้ **"ผู้ใช้"** ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ส่วนบุคคลของ สดช.

๑.๔. **"ผู้ใช้"** ต้องไม่ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ ที่มีการทำงาน กระทบต่อระบบส่วนกลาง

๑.๕. การตั้งชื่อเครื่องคอมพิวเตอร์ส่วนบุคคลจะต้องตั้งชื่อและกำหนดโดย ขศ. เท่านั้น

๑.๖. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อม จะต้องดำเนินการโดย ขศ. หรือหน่วยงานที่เกี่ยวข้องเท่านั้น

๑.๗. ก่อนใช้งานสื่อบันทึกพกพาต่างๆ ได้แก่ แผ่น CD Flash Drive หรือ External HardDisk เป็นต้น ต้องมีการตรวจสอบเพื่อตรวจหาไวรัสโดยโปรแกรมป้องกันไวรัส

๑.๘. ต้องไม่เก็บข้อมูลสำคัญของ สดช. ไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

๑.๙. ต้องไม่สร้างเส้นทางลัด (Short cut) บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ สดช.

๑.๑๐. **"ผู้ใช้"** มีหน้าที่และรับผิดชอบต่อการดูแลและรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดยต้องปฏิบัติดังนี้

๑.๑๐.๑. ต้องไม่รับประทานอาหารหรือนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณพื้นที่ติดตั้งเครื่องคอมพิวเตอร์

๑.๑๐.๒. ต้องไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์ หรือ Disk Drive

๒. การควบคุมการเข้าถึงระบบปฏิบัติการ มีแนวทางปฏิบัติ ดังนี้

๒.๑. **"ผู้ใช้"** ต้องกำหนดชื่อผู้ใช้งาน (Login) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๒.๒. **"ผู้ใช้"** ต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๒.๓. **"ผู้ใช้"** ต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน และรหัสผ่านเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๒.๔. ในระหว่างเวลาพักกลางวัน และหลังเลิกงาน **"ผู้ใช้"** ต้อง Log out ออกจากเครื่องคอมพิวเตอร์หรือ ล็อคหน้าจอด้วยโปรแกรม Screen Saver

๓. **การใช้รหัสผ่าน (Password)** มีแนวทางปฏิบัติ ดังนี้

๓.๑. **"ผู้ใช้"** ต้องกำหนดรหัสผ่าน ให้มีความยาว ๘ ตัวอักษรและมีส่วนประกอบของอักษรอักขระพิเศษและหรือตัวเลขประสมกัน โดยไม่ใช้ข้อความที่เกี่ยวข้องกับ สดช. หรือข้อความส่วนตัวของผู้ใช้งานซึ่งอาจง่ายแก่การคาดเดา ได้แก่ เลขที่บัตรประกันสังคม รหัสเจ้าหน้าที่ ที่อยู่ ชื่อบุคคลในครอบครัว เป็นต้น และรหัสผ่านต้องไม่ใช้คำศัพท์ที่มาจากพจนานุกรม ชื่อหนัง ชื่อสถานที่หรือชื่อสิ่งลึกลับ เพราะศัพท์ต่างๆ เหล่านี้ ผู้ไม่ประสงค์ดีหรือแฮกเกอร์ (Hackers) สามารถคาดเดาได้ง่าย

๓.๒. **"ผู้ใช้"** ต้องเก็บรหัสผ่านเป็นความลับ และต้องไม่เปิดเผยรหัสผ่านให้ผู้อื่นทราบ

๓.๓. **"ผู้ใช้"** ต้องเก็บรหัสผ่านไว้ในสถานที่ที่ปลอดภัยที่ผู้อื่นไม่สามารถค้นพบได้

๓.๔. **"ผู้ใช้"** ไม่พิมพ์รหัสผ่าน ในขณะที่มีผู้อื่นเห็นการพิมพ์ดังกล่าว

๓.๕. **"ผู้ใช้"** ต้องเปลี่ยนรหัสผ่านของตนเองทุกๆ ๖ เดือน และต้องไม่ตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิม

๔. **การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์** มีแนวทางปฏิบัติ ดังนี้

๔.๑. **"ผู้ใช้"** ต้องทำการปรับปรุง (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๔.๒. **"ผู้ใช้"** ต้องตรวจสอบไวรัสจากสื่อต่างๆ ได้แก่ แผ่น CD Flash Drive หรือ External HardDisk เป็นต้น ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๔.๓. **"ผู้ใช้"** ต้องตรวจสอบก่อนใช้งานไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากระบบเครือข่ายอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส

๔.๔. **"ผู้ใช้"** ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดๆที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๕. **การสำรองข้อมูลและการกู้คืนข้อมูล**

ข้อมูลเป็นสิ่งที่มีความสำคัญต่อการดำเนินงาน จึงต้องมีการสำรองข้อมูลและการกู้คืนข้อมูลอย่างสม่ำเสมอ โดยมีแนวทางปฏิบัติ ดังนี้

๕.๑. **"ผู้ใช้"** ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ส่วนบุคคลไว้บนสื่อบันทึกอื่นๆ ได้แก่ แผ่น CD Flash Drive หรือ External HardDisk เป็นต้น

๕.๒. **"ผู้ใช้"** มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๕.๓. **"ผู้ใช้"** ที่ต้องการเคลื่อนย้ายสื่อสำรองข้อมูลออกนอกสถานที่จะต้องมีการป้องกันการเข้าถึงข้อมูลอย่างมั่นคงปลอดภัย

๕.๔. สื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนข้อมูลสม่ำเสมอ

๕.๕. แผ่นสื่อสำรองข้อมูล ได้แก่ แผ่น CD ที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๖. **การนำออกครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง** มีแนวทางปฏิบัติ ดังนี้

๖.๑. **"ผู้ใช้"** ที่จะนำครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง จะต้องกรอกรายละเอียดตามแบบฟอร์มการนำสินทรัพย์ออกนอกอาคารสถานที่ ให้ถูกต้องและครบถ้วนเท่านั้น ถึงจะอนุญาตให้นำออกครุภัณฑ์คอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงได้

๖.๒. **"ผู้ใช้"** ที่นำออกครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง จะต้องลงชื่อตนเองและพยานในแบบฟอร์มการนำสินทรัพย์ออกนอกอาคารสถานที่ ซึ่งพยานต้องเป็นเจ้าหน้าที่ของ สดช. เท่านั้น เพื่อรับรองการนำออกให้ชัดเจนพร้อมทั้งแนบสำเนาบัตรประจำตัวยืนยันตัวเอง ต่อเจ้าหน้าที่รักษาความปลอดภัย (รปภ.) ทุกครั้ง

๖.๓. **"ผู้ใช้"** ต้องเก็บสำเนาแบบฟอร์มการนำสินทรัพย์ออกนอกอาคารสถานที่ไว้ เพื่อเป็นหลักฐาน

๗. การบำรุงรักษาครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง มีแนวทางปฏิบัติ ดังนี้

๗.๑. ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงจะต้องขึ้นทะเบียนครุภัณฑ์เพื่อความสะดวกในการตรวจสอบและการบำรุงรักษา

๗.๒. ขศ. จะให้บริการเฉพาะครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง ที่ขึ้นทะเบียนครุภัณฑ์แล้วหรืออยู่ระหว่างการส่งมอบแล้วเท่านั้น

๗.๓. หากครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงเกิดการชำรุดเสียหาย ไม่สามารถใช้งานได้ทั้งด้านซอฟต์แวร์หรือฮาร์ดแวร์ **"ผู้ใช้"** มีหน้าที่จะต้องแจ้งให้ ขศ. รับทราบเพื่อดำเนินการแก้ไขต่อไป

๗.๔. หากครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอยู่ในสัญญาหรือระยะเวลาการรับประกันเกิดการชำรุดเสียหาย ขศ. หรือหน่วยงานเจ้าของครุภัณฑ์คอมพิวเตอร์ มีหน้าที่ติดต่อคู่สัญญาหรือผู้แทนจำหน่าย เพื่อดำเนินการตรวจซ่อมตามที่ระบุในสัญญา

๗.๕. หากครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอยู่นอกเหนือหรือพ้นระยะเวลาการรับประกัน ขศ. มีหน้าที่ซ่อมแซมในเบื้องต้นหรือประสานกับหน่วยงานเจ้าของครุภัณฑ์คอมพิวเตอร์ในการดำเนินการซ่อมแซมต่อไป

นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook Computer)

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพา และการนำไปปฏิบัติงานภายนอก สดช. เพื่อเป็นการป้องกันข้อมูล และอุปกรณ์ของ สดช. ให้เกิดความปลอดภัย ผู้ใช้จึงต้องรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ต้องหลีกเลี่ยง ในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

๒. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา มีแนวทางปฏิบัติ ดังนี้

๒.๑. เครื่องคอมพิวเตอร์แบบพกพาที่ สดช. อนุญาตให้ "ผู้ใช้" ใช้งานเป็นสินทรัพย์ของ (สดช.) ดังนั้นผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างระมัดระวัง และเพื่องานของ สดช.

๒.๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของ สดช. ต้องเป็นโปรแกรมที่ สดช. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพา หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๓. การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) แบบพกพาจะต้องกำหนดและตั้งชื่อโดย ขศ.

๒.๔. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดย ขศ. หรือหน่วยงานที่เกี่ยวข้อง

๒.๕. **"ผู้ใช้"** ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๒.๖. ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์ และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๒.๗. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันจากการกระทบกระเทือน ได้แก่ การตกจากโต๊ะทำงานหรือหลุดมือ

๒.๘. ไม่ใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยน

๒.๙. การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องเพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๒.๑๐. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง ได้แก่ ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD เครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๒.๑๑. ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๒.๑๒. การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๒.๑๓. ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์ (Hard Disk) กำลังทำงาน

๒.๑๔. ไม่ใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น ได้แก่ อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ

๒.๑๕. การใช้งานและการเก็บเครื่องคอมพิวเตอร์แบบพกพา ต้องอยู่ในสภาพแวดล้อมที่มีอุณหภูมิที่ไม่สูงกว่า ๓๕ องศาเซลเซียส

๒.๑๖. ไม่วางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ ได้แก่ แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๒.๑๗. ไม่ติดตั้ง หรือวางเครื่องคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน ได้แก่ ในยานพาหนะที่กำลังเคลื่อนที่

๒.๑๘. การเช็ดทำความสะอาดหน้าจอภาพ ต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วน

๓. ความปลอดภัยทางด้านกายภาพ มีแนวทางปฏิบัติ ดังนี้

๓.๑. **"ผู้ใช้"** มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ได้แก่ ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในสถานที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๓.๒. **"ผู้ใช้"** ต้องไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระแทก

๓.๓. **"ผู้ใช้"** ต้องไม่ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Components) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ และการใช้รหัสผ่าน (Password) มีแนวทางปฏิบัติ ดังนี้

๔.๑. **"ผู้ใช้"** ต้องกำหนดชื่อผู้ใช้งาน (Login) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๔.๒. **"ผู้ใช้"** ต้องกำหนดรหัสผ่าน ให้มีความยาวอย่างน้อย ๘ ตัวอักษรและมีส่วนประกอบของอักษร อักขระพิเศษและหรือตัวเลขประสมกัน

๔.๓. **"ผู้ใช้"** ต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที ให้ทำการปิดล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๔.๔. **"ผู้ใช้"** ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๕. **การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์** มีแนวทางปฏิบัติ ดังนี้

๕.๑. **"ผู้ใช้"** ต้องทำการปรับปรุง (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่างๆอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๕.๒. **"ผู้ใช้"** ต้องไม่ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

๕.๓. หาก **"ผู้ใช้"** พบหรือสงสัย ว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) **"ผู้ใช้"** ต้องไม่เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งไม่พึงประสงค์ (Malware) ไปยังเครื่องคอมพิวเตอร์อื่นๆได้

๖. **การสำรองข้อมูลและการกู้คืนข้อมูล** มีแนวทางปฏิบัติ ดังนี้

๖.๑. **"ผู้ใช้"** ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา

๖.๒. **"ผู้ใช้"** ต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อเกิดการรั่วไหลข้อมูล

๖.๓. **"ผู้ใช้"** ที่ต้องการเคลื่อนย้ายสื่อสำรองข้อมูลออกนอกสถานที่จะต้องมีการป้องกันการเข้าถึงข้อมูลอย่างมั่นคงปลอดภัย

๖.๔. สื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนข้อมูลสม่ำเสมอ

๖.๕. แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๗. **การบำรุงรักษาครุภัณฑ์คอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพา** มีแนวทางปฏิบัติ ดังนี้

๗.๑. เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาจะต้องขึ้นทะเบียนครุภัณฑ์เพื่อความสะดวกในการตรวจสอบและการบำรุงรักษา

๗.๒. ขศ. จะให้บริการเฉพาะเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพา ที่ขึ้นทะเบียนครุภัณฑ์แล้วหรืออยู่ระหว่างการส่งมอบแล้วเท่านั้น

๗.๓. หากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาเกิดการชำรุดเสียหาย ไม่สามารถใช้งานได้ทั้งด้านซอฟต์แวร์หรือฮาร์ดแวร์ **"ผู้ใช้"** มีหน้าที่จะต้องแจ้งให้ ขศ. รับทราบเพื่อดำเนินการแก้ไขต่อไป

๗.๔. หากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาอยู่ในสัญญาหรือระยะเวลาการรับประกันเกิดการชำรุดเสียหาย ขศ. หรือหน่วยงานเจ้าของเครื่องคอมพิวเตอร์พกพา มีหน้าที่ติดต่อคู่สัญญาหรือผู้แทนจำหน่าย เพื่อดำเนินการตรวจซ่อมตามที่ระบุในสัญญา

๗.๕. หากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาอยู่นอกเหนือหรือพ้นระยะเวลาการรับประกัน ขศ. หรือหน่วยงานเจ้าของเครื่องคอมพิวเตอร์พกพา มีหน้าที่ซ่อมแซมในเบื้องต้นหรือประสานกับฝ่ายพัสดุ ในการจัดหาอะไหล่ หรือบริษัทในการดำเนินการซ่อมแซมต่อไป

นโยบายการใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ (Portable Device)

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ ได้แก่ คอมพิวเตอร์แท็บเล็ต เป็นต้น และการควบคุมดูแลการนำอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ไปปฏิบัติงานภายนอก สดช. เพื่อเป็นการป้องกันข้อมูล และอุปกรณ์ของ สดช. ให้มีความมั่นคงปลอดภัย "ผู้ใช้" จึงต้องรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ต้องหลีกเลี่ยงในการใช้อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๒. การใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ มีแนวทางปฏิบัติ ดังนี้

๒.๑. อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ที่ สดช. อนุญาตให้ "ผู้ใช้" ใช้งานเป็นสินทรัพย์ของ สดช. ดังนั้นผู้ใช้จึงต้องใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่อย่างระมัดระวัง และเพื่องานของ สดช.

๒.๒. โปรแกรมที่ได้ถูกติดตั้งลงบนอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ของ สดช. ต้องเป็นโปรแกรมที่ สดช. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๓. การเคลื่อนย้ายหรือส่งอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ตรวจซ่อมจะต้องดำเนินการโดย ขศ. หรือหน่วยงานเจ้าของอุปกรณ์

๒.๔. **"ผู้ใช้"** ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัย และมีประสิทธิภาพ

๒.๕. **"ผู้ใช้"** ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ และรักษาสภาพของอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ให้มีสภาพเดิม

๒.๖. **"ผู้ใช้"** ต้องไม่ใส่อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยน

๒.๗. การใช้อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่เป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด **"ผู้ใช้"** ต้องปิดเครื่องเพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๒.๘. ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๒.๙. **"ผู้ใช้"** ต้องไม่ใช้ หรือวางอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ใกล้สิ่งที่เป็นของเหลวความชื้น ได้แก่ อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น

๒.๑๐. การใช้งานและการเก็บอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ ต้องอยู่ในสภาพแวดล้อมที่มีอุณหภูมิที่ไม่สูงกว่า ๓๕ องศาเซลเซียส

๒.๑๑. ไม่วางอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ ได้แก่ แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๒.๑๒. การเช็ดทำความสะอาดหน้าจอภาพ ต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วน

๓. **ความปลอดภัยทางด้านกายภาพ** มีแนวทางปฏิบัติ ดังนี้

๓.๑. **"ผู้ใช้"** มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย และไม่วางเครื่องทิ้งไว้ในสถานที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๓.๒. **"ผู้ใช้"**ต้องไม่เก็บหรือใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระแทก

๓.๓. **"ผู้ใช้"** ต้องไม่ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Components) ที่ติดตั้งอยู่ภายใน รวมถึงอุปกรณ์สำรองไฟฟ้า

๔. **การควบคุมการเข้าถึงระบบปฏิบัติการ และการใช้รหัสผ่าน (Password) มีแนวทางปฏิบัติ ดังนี้**

๔.๑. **"ผู้ใช้"** ต้องกำหนดชื่อผู้ใช้งาน (Login) และรหัสผ่าน (Password) ในการใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่

๔.๒. **"ผู้ใช้"** ต้องกำหนดรหัสผ่านตามรูปแบบเฉพาะของอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ชนิดนั้น ๆ

๔.๓. **"ผู้ใช้"** ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ เชื่อมต่อกับระบบเครือข่ายของ สดช.

๕. **การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์** มีแนวทางปฏิบัติ ดังนี้

๕.๑. **"ผู้ใช้"** ต้องทำการปรับปรุง (Update) ระบบปฏิบัติการ และโปรแกรมใช้งานต่างๆอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๕.๒. หาก **"ผู้ใช้"** พบหรือสงสัย ว่าอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ **"ผู้ใช้"** ต้องไม่เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งไม่พึงประสงค์ (Malware) ไปยังเครื่องคอมพิวเตอร์อื่นๆได้

๖. **การสำรองข้อมูลและการกู้คืนข้อมูล** มีแนวทางปฏิบัติ ดังนี้

๖.๑. **"ผู้ใช้"** ต้องทำการสำรองข้อมูลจากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ โดยวิธีการและสื่อ (Media) ต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

๖.๒. **"ผู้ใช้"** ต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อเกิดการรั่วไหลข้อมูล

๖.๓. **"ผู้ใช้"** ที่ต้องการเคลื่อนย้ายสื่อสำรองข้อมูลออกนอกสถานที่จะต้องมีการป้องกันการเข้าถึงข้อมูลอย่างมั่นคงปลอดภัย

๗. **การบำรุงรักษาอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่** มีแนวทางปฏิบัติ ดังนี้

๗.๑. อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่จะต้องขึ้นทะเบียนครุภัณฑ์เพื่อความสะดวกในการตรวจสอบและการบำรุงรักษา

๗.๒. ขศ. จะให้บริการเฉพาะอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ ที่ขึ้นทะเบียนครุภัณฑ์แล้วหรืออยู่ระหว่างการส่งมอบแล้วเท่านั้น

๗.๓. หากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่เกิดการชำรุดเสียหาย ไม่สามารถใช้งานได้ทั้งด้านซอฟต์แวร์หรือฮาร์ดแวร์ **"ผู้ใช้"** มีหน้าที่จะต้องแจ้งให้ ขศ. รับทราบเพื่อดำเนินการแก้ไขต่อไป

๗.๔. หากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่อยู่ในสัญญาหรือระยะเวลาการรับประกันเกิดการชำรุดเสียหาย ขศ. หรือหน่วยงานเจ้าของครุภัณฑ์มีหน้าที่ติดต่อคู่สัญญาหรือผู้แทนจำหน่าย เพื่อดำเนินการตรวจซ่อมตามที่ระบุในสัญญา

๗.๕. หากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่อยู่นอกเหนือหรือพ้นระยะเวลาการรับประกัน ขศ. มีหน้าที่ซ่อมแซมในเบื้องต้นหรือประสานกับหน่วยงานเจ้าของครุภัณฑ์ ในการดำเนินการซ่อมแซมต่อไป

นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล
(Media Handling Policy)

๑. **วัตถุประสงค์**

นโยบายนี้จัดทำขึ้นเพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายสินทรัพย์สารสนเทศโดยไม่ได้รับอนุญาต

๒. **การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนที่ย้ายได้ (Management of Removable Media)**

เพื่อควบคุมและป้องกันสื่อบันทึกข้อมูลที่สามารถเคลื่อนที่ย้ายได้ มีแนวทางการปฏิบัติดังนี้

๒.๑. ข้อมูลที่มีชั้นความลับ ต้องกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว

๒.๒. ในกรณีที่สื่อบันทึกข้อมูลนั้นไม่ได้ถูกนำมาใช้งานแล้ว ก่อนที่จะนำออกไปจาก สดช. ต้องมั่นใจข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก

๒.๓. ในกรณีที่จำเป็นต้องนำสื่อบันทึกข้อมูลออกไป จะต้องได้รับการอนุมัติจากหน่วยงานที่รับผิดชอบสื่อบันทึกข้อมูลดังกล่าว และต้องบันทึกการโยกย้าย เพื่อใช้ในการตรวจสอบ

๒.๔. สื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต ได้แก่ อุณหภูมิสูงหรือต่ำเกินไป

๒.๕. ในการจัดเก็บสื่อบันทึกข้อมูลที่สำคัญ ต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล ได้แก่ มีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน กำหนดบุคลากรที่มีสิทธิในการใช้งาน เป็นต้น

๒.๖. ถ้าข้อมูลที่ต้องการจัดเก็บมีอายุการจัดเก็บยาวนานกว่าอายุการใช้งานของสื่อบันทึกข้อมูล ต้องจัดเก็บไว้ที่แหล่งอื่น เพื่อป้องกันการสูญหายของข้อมูล

๒.๗. ต้องจัดทำทะเบียนบันทึกข้อมูลของสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เพื่อลดโอกาสการสูญหายของข้อมูล

๒.๘. ตัวอ่านสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ จะต้องใช้เพื่อเหตุผลทางราชการเท่านั้น การมอบอำนาจในระดับต่างๆ ต้องทำเป็นเอกสารอย่างชัดเจน

๓. การกำจัดสื่อบันทึกข้อมูล (Disposal of Media)

การทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีก ต้องเป็นไปอย่างมั่นคงและปลอดภัย เพื่อลดความเสี่ยงของการรั่วไหลข้อมูลของ สดช. ไปยังผู้อื่นที่ไม่ได้รับอนุญาต ซึ่งมีแนวทางปฏิบัติดังนี้

๓.๑. สื่อที่บันทึกข้อมูลที่มีความสำคัญมาก จะต้องมีการทำลายด้วยวิธีการที่ปลอดภัย ได้แก่ การเผาหรือแยกชิ้นส่วนเป็นชิ้นเล็กๆ หรือลบข้อมูลด้วยโปรแกรมอื่นๆที่มิใช่ใน สดช.

๓.๒. กระบวนการต่างๆ ต้องระบุวิธีการกำจัดสื่อบันทึกข้อมูลอย่างชัดเจน เพื่อความปลอดภัยของข้อมูล ได้แก่ ปฏิบัติตามแนวทางความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

๓.๓. เพื่อความสะดวก ต้องรวบรวมสื่อทั้งหมดที่ไม่ต้องการแล้วกำจัดพร้อมกันด้วยวิธีการที่ปลอดภัย

๓.๔. ในกรณีที่เลือกใช้บริการกำจัดสื่อและเอกสาร รวมทั้งอุปกรณ์ต่างๆ จากหน่วยงานภายนอก ต้องระวังในการเลือกใช้บริการ ต้องเลือกหน่วยงานภายนอกที่มีการควบคุมที่ดีและมีประสบการณ์

๓.๕. ในการกำจัดสื่อบันทึกข้อมูล จะต้องมีการบันทึก เพื่อใช้ในการตรวจสอบ

๓.๖. หากไม่มีการกำหนดการกำจัดสื่อบันทึกข้อมูลเป็นการเฉพาะให้วิธีการทำลายข้อมูลตามแนวทางของมาตฐานสากล ได้แก่ DoD 5220.22-M และ SP 800-88 เป็นต้น มาดำเนินการแทน

๓.๗. หากเป็นสื่อบันทึกข้อมูลส่วนบุคคล กระบวนการในการทำลายให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๓๓ และ ๓๗

หมายเหตุ : ข้อมูลที่ไม่มีความสำคัญเมื่อมีการรวบรวมเป็นจำนวนมากๆ อาจจะกลายเป็นข้อมูลที่มีความสำคัญได้ ดังนั้นในการกำจัด ต้องคำนึงถึงข้อมูลที่มีการรวบรวมไว้ด้วย

๔. ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information Handling Procedures)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์ มีแนวทางปฏิบัติดังนี้

๔.๑. ติดป้ายชื่อของสื่อบันทึกข้อมูลทั้งหมด เพื่อระบุประเภท

๔.๒. จำกัดการเข้าถึงหรือควบคุมการใช้งาน

๔.๓. สารสนเทศของผู้ที่ไม่ได้รับอนุญาต

๔.๔. ทำบันทึกข้อมูลเกี่ยวกับผู้ที่มีสิทธิได้รับข้อมูล

๔.๕. ข้อมูลที่ป้อนเข้าสู่ระบบและในระหว่างการประมวลผลต้องมีความครบถ้วน และต้องตรวจสอบผลลัพธ์ที่ออกมาด้วย

๔.๖. ต้องมีการปกป้องข้อมูลที่อยู่ในระหว่างการแสดงผลลัพธ์ออกมาตามระดับความสำคัญ

๔.๗. เก็บรักษาสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต

๔.๘. กระจายข้อมูลให้ผู้ที่มีสิทธิได้รับข้อมูลเท่านั้น

๔.๙. ทบทวนการกระจายข้อมูลและรายชื่อของผู้ที่มีสิทธิได้รับข้อมูลอย่างต่อเนื่อง

หมายเหตุ : กระบวนการเหล่านี้คลอบคลุมทั้งสื่อที่เป็นเอกสาร ระบบคอมพิวเตอร์ ระบบเครือข่าย โทรศัพท์เคลื่อนที่ จดหมายอิเล็กทรอนิกส์ การสื่อสารด้วยเสียง มัลติมีเดีย การบริการของไปรษณีย์ เครื่องถ่ายเอกสาร รวมไปถึงเช็คเปล่าและใบเรียกเก็บเงิน

๕. การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of System Documentation)

มาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต ให้ดำเนินการจัดทำชั้นความลับของเอกสารระบบ และดำเนินการตามนโยบายการจัดหมวดหมู่และการควบคุมสินทรัพย์

นโยบายการแลกเปลี่ยนสารสนเทศ
(Information Exchange Policies)

๑. วัตถุประสงค์

นโยบายนี้จัดทำขึ้นเพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

๒. ข้อระวังสำหรับการแลกเปลี่ยนสารสนเทศ (Information Exchange Policies and Procedures)

เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (ได้แก่ องค์กรและหน่วยงานภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด ต้องพิจารณาดังต่อไปนี้

๒.๑. ในกรณีข้อมูลที่แลกเปลี่ยนเป็นข้อมูลส่วนบุคคล ให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หมวดที่ ๒

๒.๒. การป้องกันจากการถูกดักจับ คัดลอก แก้ไข ส่งผิดเส้นทาง และการทำลายข้อมูล

๒.๓. การตรวจจับและป้องกัน Source Code ที่ไม่พึงประสงค์ ซึ่งอาจถูกส่งผ่านการสื่อสารทางอิเล็กทรอนิกส์

๒.๔. การป้องกันการส่งข้อมูลที่สำคัญด้วยวิธีการแนบเอกสาร (Attachment File)

๒.๕. แนวทางปฏิบัติต้องสอดคล้องกับแนวทางความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

๒.๖. การสื่อสารไร้สาย ต้องคำนึงถึงความเสี่ยงจะที่เกิดขึ้นด้วย

๒.๗. ผู้ใช้งานต้องรับผิดชอบในบทบาทหน้าที่ ไม่ฝ่าฝืนนโยบายหรือกฎระเบียบของ สดช. ได้แก่ การหมิ่นประมาท การข่มขู่หรือก่อกวนความสงบ การปลอมตัว การส่งต่อจดหมายลูกโซ่ การจัดซื้อจัดจ้างนอกเหนือการอนุมัติ เป็นต้น

๒.๘. เทคนิคการเข้ารหัส เพื่อปกป้องความลับ ความสมบูรณ์และความถูกต้องของสารสนเทศ

๒.๙. แนวทางในการเก็บรักษาและทำลายจดหมายทางราชการต้องเป็นไปตามที่กฎหมายกำหนด

๒.๑๐. ไม่ทิ้งเอกสารสำคัญไว้ที่เครื่องถ่ายเอกสาร เครื่องพิมพ์หรือเครื่องโทรสาร ซึ่งผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้

๒.๑๑. ควบคุมและยับยั้งการส่งต่อข้อมูลของอุปกรณ์สื่อสาร เช่นการส่งต่อจดหมายอิเล็กทรอนิกส์อัตโนมัติไปนอก สดช.

๒.๑๒. เตือนผู้ใช้งานให้มีความระมัดระวังไม่ให้ข้อมูลสำคัญรั่วไหลโดยการดักฟังหรือได้ยินแบบไม่ตั้งใจในขณะใช้โทรศัพท์ ได้แก่

๒.๑๑.๑. คนที่อยู่บริเวณใกล้ๆ ในขณะที่ใช้โทรศัพท์เคลื่อนที่
๒.๑๑.๒. การดักฟังหรือการแอบฟังทางสายโทรศัพท์
๒.๑๑.๓. คนที่อยู่ฝั่งตรงข้าม
๒.๑๒. ไม่ทิ้งข้อความสำคัญบนเครื่องตอบรับ ซึ่งอาจจะถูกตอบกลับโดยผู้ที่ไม่ได้รับอนุญาต หรือถูกเก็บบนระบบของสาธารณะ หรือถูกเก็บอย่างไม่ถูกต้องเนื่องจากการโทรที่ผิดพลาด
๒.๑๓. เตือนผู้ใช้งานเกี่ยวกับปัญหาในการใช้เครื่องโทรสาร ได้แก่
๒.๑๓.๑. การเข้าถึงของผู้ที่ไม่ได้รับอนุญาต เพื่อดึงข้อมูลภายในเครื่องที่จัดเก็บไว้
๒.๑๓.๒. การตั้งโปรแกรมในการส่งไปยังเลขหมายปลายทางโดยตั้งใจและไม่ตั้งใจ
๒.๑๓.๓. การส่งเอกสารหรือข้อความผิดเลขหมายโดยการโทรที่ผิดพลาดหรือบันทึกเลขหมายผิด
๒.๑๓.๔. เครื่องโทรสารและเครื่องถ่ายเอกสารรุ่นใหม่จะมีหน่วยความจำในการเก็บเอกสารบางหน้าหรือการส่งที่ผิดพลาด ซึ่งจะถูกพิมพ์ออกมาเมื่อเครื่องทำงานได้ตามปกติ

๓. ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange Agreements)

ในการแลกเปลี่ยนสารสนเทศ ต้องคำนึงถึงข้อตกลงในการแลกเปลี่ยนสารสนเทศดังต่อไปนี้

๓.๑. ในกรณีข้อมูลที่แลกเปลี่ยนเป็นข้อมูลส่วนบุคคล ให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หมวดที่ ๒
๓.๒. การบริหารจัดการในการควบคุมและแจ้งให้ทราบเกี่ยวกับการสื่อสาร การส่งและการรับ
๓.๓. การแจ้งให้ผู้ส่งรับทราบเกี่ยวกับการสื่อสาร การส่งและการรับ
๓.๔. กระบวนการที่สามารถติดตามและปฏิเสธความรับผิดชอบไม่ได้
๓.๕. มาตรฐานทางเทคนิคขั้นต่ำในการบรรจุและส่งออก
๓.๖. สัญญาข้อตกลง
๓.๗. มาตรฐานในการระบุตัวผู้ส่งเอกสาร
๓.๘. ความรับผิดชอบและภาระหน้าที่เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ เช่น การสูญหายของข้อมูล เป็นต้น
๓.๙. ใช้ระบบป้ายชื่อตามข้อตกลงสำหรับข้อมูลที่มีความสำคัญ เพื่อเข้าใจได้ทันทีในความหมายของป้ายชื่อและเป็นการปกป้องสารสนเทศอย่างเหมาะสม
๓.๑๐. ความเป็นเจ้าของและความรับผิดชอบสำหรับการปกป้องข้อมูล ลิขสิทธิ์ การปฏิบัติตามใบอนุญาตการใช้งานซอฟท์แวร์ และค่าตอบแทนต่างๆ
๓.๑๑. มาตรฐานทางเทคนิคในการบันทึกและอ่านข้อมูลสารสนเทศและซอฟท์แวร์
๓.๑๒. การควบคุมพิเศษที่จำเป็นในการปกป้องข้อมูลสำคัญ เช่นการใช้กุญแจเข้ารหัสข้อมูล เป็นต้น

๔. การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical Media in Transit)

เพื่อป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร ต้องพิจารณาดังต่อไปนี้

๔.๑. การส่งสื่อบันทึกข้อมูลที่มีข้อมูลส่วนบุคคลอยู่ ให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หมวดที่ ๒

๔.๒. ใช้วิธีการขนส่งหรือพนักงานส่งของที่เชื่อถือได้

๔.๓. รายชื่อของพนักงานส่งหรือบริษัทส่งของต้องได้รับการอนุมัติจากผู้บริหาร

๔.๔. กระบวนการตรวจสอบพนักงานส่งของต้องมีการปรับปรุงอย่างสม่ำเสมอ

๔.๕. การบรรจุภัณฑ์ต้องป้องกันความเสียหายในระหว่างการส่ง โดยเป็นไปตามข้อกำหนดของผู้ผลิต ตัวอย่างการป้องกันปัจจัยทางกายภาพที่จะมีผลต่อการกู้คืนข้อมูล ได้แก่ ความร้อน ความชื้นและสนามแม่เหล็ก

๔.๖. การควบคุมที่จำเป็นในการปกป้องข้อมูลสำคัญจากการเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต

๔.๕.๑. ใช้ตู้ที่มีกุญแจล็อค

๔.๕.๒. ส่งด้วยมือตนเองและลงบันทึกการรับ-ส่ง เพื่อสามารถตรวจสอบได้

๔.๕.๓. บางกรณีอาจจะต้องใช้วิธีการแยกส่งออกหลายๆ ส่วนและหลายๆ เส้นทาง เพื่อกระจายความเสี่ยง

๕. การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)

การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) ต้องพิจารณาถึงความมั่นคงปลอดภัยดังต่อไปนี้

๕.๑. การส่งข้อความทางอิเล็กทรอนิกส์ หากเป็นข้อมูลส่วนบุคคล ให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หมวดที่ ๒

๕.๒. ตรวจสอบที่อยู่ปลายทางของผู้รับ และการส่งข้อความว่ามีความถูกต้องหรือไม่ ก่อนที่จะส่งข้อความ

๕.๓. ผู้ให้บริการส่งข้อความทางอิเล็กทรอนิกส์ ต้องมีความน่าเชื่อถือและสามารถใช้บริการได้

๕.๔. ข้อกำหนดทางกฎหมาย เช่นการใช้ลายมือชื่ออิเล็กทรอนิกส์

๕.๕. การใช้บริการแบบสาธารณะ ต้องระวังในการรับ-ส่งข้อมูลที่เป็นความลับของ สดช. ได้แก่ การ Chat การแชร์ไฟล์ เป็นต้น

๕.๖. ในการส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) ต้องจัดส่งโดยใช้ช่องทางที่ สดช. กำหนด

นโยบายสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ
(Publicly Available Information)

การยืนยันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ ครอบคลุมถึงซอฟท์แวร์ ข้อมูลและสารสนเทศอื่นๆ ที่ต้องการความถูกต้องในระดับสูงที่จะถูกเผยแพร่ออกสู่สาธารณะ จะต้องมีวิธีการในการตรวจสอบ ได้แก่ ลายมือชื่ออิเล็กทรอนิกส์ รวมถึงการตรวจสอบการเข้าถึงข้อมูลจากเครือข่ายสาธารณะ ข้อมูลที่เผยแพร่ต้องจะมีการตรวจสอบความผิดพลาดต่างๆ และได้รับการอนุมัติก่อน ซึ่งผู้เผยแพร่ข้อมูลต้องพิจารณาดังต่อไปนี้

- สารสนเทศนั้นต้องเป็นไปตามกฎหมายที่เกี่ยวข้องกับการปกป้องข้อมูล
- สารสนเทศที่นำเข้าและประมวลผลโดยระบบจะต้องสมบูรณ์และถูกต้องตามสภาวะกาล
- สารสนเทศสำคัญจะต้องถูกปกป้องในระหว่างที่มีการรวบรวม ประมวลผลและจัดเก็บ
- ต้องไม่มีเส้นทางเชื่อมโยง (Link) จากหน้าเว็บไซต์เข้าสู่ระบบงานคอมพิวเตอร์ภายในของ สดช.

นโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์
(Social Media Policy)

๑. วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแลการเผยแพร่ข้อมูลและการเข้าถึงสื่อเครือข่ายสังคมออนไลน์ของ สดช. รวมถึงบริการอิเล็กทรอนิกส์ตลอดจนการแสดงความคิดเห็นของบุคลากรใน สดช ผ่านสื่อเครือข่ายสังคมออนไลน์ให้เป็นไปอย่างถูกต้องเหมาะสม มีความเป็นระเบียบเรียบร้อยและเกิดประโยชน์สูงสุด ดังนั้น สดช. จึงเห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ให้เป็นไปในทางสร้างสรรค์ โดยมีวัตถุประสงค์ ดังนี้

๑.๑ เพื่อให้ สดช.มีการกำหนดขอบเขตของการใช้สื่อสังคมออนไลน์ทั้งในระดับตัวบุคคล และระดับองค์กร

๑.๒ เพื่อสร้างและรักษาภาพลักษณ์ของบุคลากรและการดำเนินงานของ สดช.

๑.๓ เพื่อลดความเสี่ยงหรือหลีกเลี่ยงปัญหาอันอาจจะเกิดขึ้นจากการใช้สื่อสังคมออนไลน์

๑.๔ เพื่อป้องกันการเปิดเผยข้อมูลความลับในทุกระดับทั้ง สดช. บริการอิเล็กทรอนิกส์ ผู้มีส่วนได้ส่วนเสีย รวมถึงบุคลากรใน สดช.

๒. ขอบเขตของนโยบาย

ภายใต้นโยบายนี้ การเข้าถึงสื่อเครือข่ายสังคมออนไลน์ และการเผยแพร่ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง ข้อมูลใด ๆ หรือแสดงความคิดเห็นส่วนตัวผ่านสื่อสังคมออนไลน์ มีผลบังคับเหมือนกับการเผยแพร่ข้อมูลหรือแสดงความคิดเห็นผ่านทางช่องทางอื่นๆ โดยการใช้งานสื่อสังคมออนไลน์ทุกประเภท จะต้องปฏิบัติและสอดคล้องตามแนวนโยบายของสดช. ได้แก่ พรบ.ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ พ.ร.บ. ว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฉบับ พ.ศ. ๒๕๖๐ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และฉบับแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ อย่างเคร่งครัด

๓. องค์ประกอบของนโยบาย

๓.๑ แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ทั่วไป

๓.๒ แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ในระดับบุคคล

๓.๓ แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ในระดับองค์กร

แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ทั่วไป

๑. หลักการและแนวปฏิบัติทั่วไป

๑.๑ สดช.อนุญาตให้ใช้ระบบเครือข่ายสาหรับเข้าถึงสื่อสังคมออนไลน์ประเภทเว็บไซต์ที่ไม่มีเนื้อหาขัดต่อกฎหมาย ศีลธรรม

๑.๒ บุคลากรของ สดช. สามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์ เพื่อประโยชน์ในการเผยแพร่ประชาสัมพันธ์ที่เกี่ยวข้องกับสดช. ติดต่อสื่อสารระหว่างกัน แต่ต้องแยกแยะให้ชัดเจนว่าข้อความใดเป็น "ข่าวประชาสัมพันธ์" ข้อความใดเป็น "ความคิดเห็น" "ความคิดเห็นส่วนบุคคล" "การแลกเปลี่ยนข่าวสารส่วนตัว" "การเผยแพร่ข่าวสารเรื่องงาน" หรืออื่นๆ และความคิดเห็นดังกล่าวต้องคำนึงถึงประโยชน์สาธารณะด้วย

๑.๓ การเผยแพร่ประชาสัมพันธ์ที่ประชาสัมพันธ์ในนามของสดช. ผู้เผยแพร่ต้องแสดงตำแหน่ง หน้าที่สังกัด ให้ชัดเจน เพื่อความน่าเชื่อถือ และเพื่อให้ผู้ที่ติดตามสามารถใช้ดุลพินิจในการติดตามได้

๑.๔ พึงระมัดระวังการใช้ถ้อยคำและภาษา ที่อาจเป็นการดูหมิ่น ทั้งการหมิ่นประมาทบุคคลอื่นหรือหมิ่นประมาทองค์กรและต้องใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์ ไม่ขัดต่อกฎหมาย

๑.๕ พึงงดเว้นการนำรูปบุคคลอื่น รูปบุคคลสาธารณะ หรือรูปที่สร้างความเสียหายให้แก่บุคคลอื่น องค์กร และสังคม มาแสดงว่าเป็นรูปของตนเอง

๑.๖ พึงงดเว้นการโพสข้อมูล ลามกอนาจาร และอื่นๆ ที่ไม่เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วยุหรือขัดต่อจริยธรรม ได้แก่ การเมือง ศาสนา ชนชาติ เป็นต้น

๑.๗ พึงงดเว้นการอ้างอิงหรือเปิดเผยถึงข้อมูลผู้มีส่วนได้ส่วนเสีย ตลอดจนผู้มีส่วนเกี่ยวข้องอย่างเปิดเผยก่อนได้รับอนุญาต

๑.๘ สดช. หรือ หน่วยงานที่สังกัด อาจใช้รูปสัญลักษณ์ เครื่องหมายแสดงสังกัดได้ แต่ต้องคานึงถึงความเหมาะสมในการใช้งาน

๑.๙ การใช้สื่อสังคมออนไลน์ที่แสดงสังกัดหน่วยงานภายในสดช. ต้องแจ้งให้ผู้บังคับบัญชาทราบก่อนทุกครั้ง

๑.๑๐ การใช้สื่อเครือข่ายสังคมออนไลน์จะต้องไม่รบกวนการปฏิบัติงานหรือหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

๒. หลักการส่งต่อข้อมูล

๒.๑. ต้องส่งข้อมูลเฉพาะบุคคลที่รู้จัก แสดงตัวตน ตำแหน่ง หน้าที่การงาน สถานะที่ชัดเจนเท่านั้น

๒.๒. ต้องตรวจสอบที่มาและความถูกต้องของข้อมูล ก่อนทำการส่งต่อข้อมูลลงในสื่อสังคมออนไลน์

๒.๓. งดเว้นการส่งต่อข้อมูลของสดช. ที่มีชั้นความลับทุกกรณี

๒.๔. งดเว้นการส่งต่อข้อมูลหรือข้อความที่เป็นเท็จ

๒.๕. การเผยแพร่และส่งต่อข้อมูลส่วนบุคคลต้องคำนึงถึง สิทธิของเจ้าของข้อมูลส่วนบุคคล และบทกำหนดโทษตามที่ พรบ.คุ้มครองข้อมูลส่วนบุคคล กำหนดไว้

๓. หลักความรับผิดชอบ

หากพบข้อมูลใดๆ ที่ไม่เหมาะสม หรือไม่ถูกต้อง (ได้แก่ สิ่งที่เป็นลิขสิทธิ์ของผู้อื่น หรือการแสดงความคิดเห็นที่เป็นการหมิ่นประมาท) ต้องดำเนินการลบข้อมูลดังกล่าวออกทันที เพื่อลดโอกาสที่จะเกิดข้อขัดแย้งทางกฎหมาย และผลกระทบด้านลบต่อ สดช.

๔. ข้อสงวนสิทธิ์

๔.๑. สดช. ไม่รับผิดชอบต่อผลของการกระทำที่เกิดจากผู้ใช้งาน และ/หรือบัญชีผู้ใช้งานที่ฝ่าฝืนต่อนโยบายนี้

๔.๒. หากสดช. ตรวจสอบพบว่าบัญชีผู้ใช้งานใดละเมิดต่อนโยบายนี้ สดช.ขอสงวนสิทธิ์ในการระงับ และ/หรือยกเลิกบัญชีผู้ใช้งานอินเตอร์เน็ต และ/หรือหยุดให้บริการแก่ผู้ใช้งานนั้น

๔.๓. หากการกระทำอันฝ่าฝืนต่อนโยบายนี้เป็นความผิดตามกฎหมาย ให้สดช.ดำเนินคดีตามกฎหมายโดยลำดับต่อไป

แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ในระดับบุคคล

การนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรใน สดช. มีแนวนโยบายและแนวปฏิบัติดังนี้

๑. กรณีใช้ชื่อบัญชีผู้ใช้งาน (user account) ที่ระบุถึงต้นสังกัด ผู้ใช้งานพึงใช้ความระมัดระวังในการปฏิบัติตามข้อบังคับจริยธรรม หลักเกณฑ์ และแนวปฏิบัติของสดช.ที่กำกับดูแลตามที่ระบุไว้ในขอบเขตของนโยบาย โดยเฉพาะความถูกต้องและการใช้ภาษาที่เหมาะสม

๒. กรณีใช้ชื่อบัญชีผู้ใช้งานที่ระบุถึงตัวตนอันอาจทำให้ผู้ติดตาม (followers) หรือเพื่อนในเครือข่าย (friends) เข้าใจได้ว่าเป็นบุคลากรในสดช. ผู้ใช้งานพึงระมัดระวังการนำเสนอข้อมูลข่าวและการแสดงความคิดเห็นที่อาจนำไปสู่ ความเสียหายขององค์กร สังคม และบุคคลอื่น

๓. หากการโพสข้อมูลข่าวสารหรือความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรใน สดช. เกิดความผิดพลาด จนก่อให้เกิดความเสียหายต่อ องค์กร สังคม และบุคคลอื่น ผู้ใช้งานต้องแสดงความรับผิดชอบต่อ องค์กร สังคม และบุคคลอื่นที่ได้รับความเสียหาย ทั้งนี้ ต้องให้ผู้ที่ได้รับความเสียหายได้มีโอกาสชี้แจงข้อมูลข่าวสารในด้านของตนด้วย

แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์เพื่อประชาสัมพันธ์ในระดับองค์กร

การใช้สื่อสังคมออนไลน์เพื่อประชาสัมพันธ์ในระดับองค์กร ต้องที่จะคำนึงถึงรายละเอียดดังนี้

๑. การตั้งค่าบนสื่อสังคมออนไลน์ขององค์กร การใช้ชื่อหรือตราสัญลักษณ์ขององค์กร เพื่อเปิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ โดยมีวัตถุประสงค์เพื่อการประชาสัมพันธ์ เผยแพร่ข้อมูลข่าวสาร หรือการสื่อสารภายในองค์กร จะต้องผ่านการรับทราบและเห็นชอบจาก CIO / ผู้อำนวยการศูนย์สารสนเทศขององค์กรก่อน

๒. การนำเสนอข่าวโดยการใช้สื่อสังคมออนไลน์ขององค์กร ต้องมีหลักในการอ้างอิงถึงองค์กร ดังนี้

๒.๑. ชื่อองค์กรที่เผยแพร่ข้อมูลข่าวสาร

๒.๒. รายละเอียด สัญลักษณ์ หรือชื่อย่อ ที่แสดงถึงองค์กร

๒.๓. ชื่อหน่วยงานที่รับผิดชอบในการประชาสัมพันธ์ข้อมูลข่าวสาร

๓. การปกป้องข้อมูลที่เป็นความลับขององค์กร ในกรณีที่มีบัญชีผู้ใช้งานขององค์กร ต้องมีการตั้งค่าความเป็นส่วนตัว (Privacy) เพื่อป้องกันไม่ให้บุคคลอื่นโพสต์ข้อความหรือเข้าถึงข้อมูลที่มีชั้นความลับ โดยมีการกำหนดให้อยู่ในวงจำกัดเท่านั้น และต้องให้ความระมัดระวังในการโพสต์ข้อความเฉพาะกลุ่มหรือส่วนบุคคลที่ไม่ต้องการเผยแพร่ให้สาธารณะชนรับรู้

๔. การนำเสนอข้อมูลข่าวสารขององค์กรผ่านสื่อสังคมออนไลน์ ต้องเป็นไปตามข้อบังคับจริยธรรม หลักเกณฑ์ และแนวปฏิบัติขององค์กรที่กำกับดูแลตามที่ระบุไว้ในขอบเขตของนโยบาย

๕. การนำเสนอข้อมูลข่าวสารขององค์กร ผ่านสื่อสังคมออนไลน์ ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อมูล ต้องให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

๖. ต้องแยกบัญชีผู้ใช้สื่อสังคมออนไลน์แบบส่วนตัวกับแบบองค์กรที่ทำหน้าที่ประชาสัมพันธ์องค์กรออกจากกัน

๗. หลีกเลี่ยงการสื่อสารข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง และข้อมูลใด ๆ ขององค์กรหรือที่เกี่ยวข้องกับองค์กรที่ก่อให้เกิดความขัดแย้ง หรือโต้แย้งในสังคม ขัดต่อหลักกฎหมายทั้งในประเทศและในระดับสากล

หมวด ๗
การควบคุมการเข้าถึง
(Access Control)

มีจุดประสงค์ เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร โดยประกอบด้วย

- นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
- นโยบายการบริหารจัดการรหัสผ่าน
- นโยบายการควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
(IT Access Control Policy)

๑. วัตถุประสงค์

นโยบายนี้ระบุถึงข้อกำหนดเพื่อควบคุมสำหรับการเข้าถึงระบบสารสนเทศของ สดช. เพื่อให้มีความมั่นคงปลอดภัย และป้องกันไม่ให้ผู้ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบได้

๒. กระบวนการความมั่นคงปลอดภัยด้านสารสนเทศของการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๒.๑. สถานที่ตั้งของระบบสารสนเทศที่สำคัญ ต้องมีการควบคุมการเข้าออกที่รัดกุมและให้เฉพาะบุคคลที่ได้รับอนุญาตและมีความจำเป็นเท่านั้นสามารถเข้าใช้งานได้ เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์บางอย่างของสำนักงานที่ไม่มี “เจ้าหน้าที่” ดูแล

๒.๒. ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบและข้อมูลให้เหมาะสมกับการใช้บริการและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิอย่างสม่ำเสมอ

๒.๓. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงบริการได้

๒.๔. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของ สดช. และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลที่สำคัญ ทั้งนี้ผู้ที่สามารถใช้ซอฟต์แวร์หรือฮาร์ดแวร์ในการตรวจตราและเฝ้าระวังในระบบเครือข่ายหรือระบบงานใดๆ ต้องเป็นผู้ที่ได้รับอนุญาตจากหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ อย่างถูกต้องเท่านั้น

๒.๕. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ หากมีปัญหาเกิดขึ้น

๒.๖. ในการขออนุญาตเข้าสู่ระบบงานต่างๆ จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ กำหนดให้มีการลงนามอนุมัติและเก็บเอกสารดังกล่าวไว้เป็นหลักฐาน

๒.๗. เจ้าของข้อมูลและเจ้าของระบบงานนั้นๆ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๒.๘. ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชา เจ้าของข้อมูลและเจ้าของระบบงานก่อนตามความจำเป็นในเข้าใช้ระบบงานคอมพิวเตอร์ของ สดช.

๓. การบริหารจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

๓.๑. การลงทะเบียนผู้ใช้งาน (User Registration)

ผู้อำนวยการกองแต่ละหน่วยงาน และหัวหน้าหน่วยงานดูแลรับผิดชอบการบริหารงานบุคคลและสวัสดิการ ต้องร่วมกันจัดทำระเบียบปฏิบัติในการลงทะเบียนผู้ใช้งานใหม่ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ นอกจากนี้ ต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้งานทันที ในกรณีที่มีการลาออกหรือเปลี่ยนตำแหน่งงานภายใน สดช.

๓.๑.๑ ผู้ใช้งานต้องกรอกข้อมูลในแบบฟอร์มขอใช้งานระบบสารสนเทศ เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๓.๑.๒ ผู้อำนวยการกอง ทำการพิจารณาอนุมัติโดยต้องเป็นไปตามหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย และนำส่งให้เจ้าของระบบดำเนินการต่อไป

๓.๑.๓ เจ้าของระบบต้องทำการพิจารณาอนุมัติโดยคำนึงถึงเหตุผล ความจำเป็นและหน้าที่ความรับผิดชอบของผู้ใช้งานว่ามีความจำเป็นต้องเข้าถึงระบบที่ตัวเองดูแลรับผิดชอบและเหมาะสมตามความรับผิดชอบหรือไม่

- ระบุชื่อบัญชีผู้ใช้งานแยกเป็นรายบุคคล ไม่ซ้ำซ้อนกัน
- จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

๓.๑.๔ เจ้าของระบบ ตั้งค่าต่าง ๆ ในระบบตามรายละเอียดในแบบฟอร์ม พร้อมทำการทดสอบระบบต่าง ๆ เพื่อให้แน่ใจว่า สิทธิที่ทำการกำหนดเป็นไปตามคำร้องขอจากผู้ใช้งาน

๓.๒. การบริหารจัดการสิทธิการใช้งานระบบ (Privilege Management)

๓.๒.๑. ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน ได้แก่ กำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศระบบงานตามความจำเป็นขั้นต่ำเท่านั้น

๓.๒.๒. ผู้ใช้งานต้องได้รับการอนุมัติสิทธิให้เสร็จสมบูรณ์ก่อน จึงจะสามารถเข้าใช้งานระบบได้

๓.๒.๓. ผู้ดูแลระบบ ต้องจัดทำบัญชีผู้ใช้งาน

๓.๒.๔. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่งและกำนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๒.๕. ยกเลิก เพิกถอน สิทธิการเข้าถึงระบบสารสนเทศและการตัดออกจากบัญชีผู้ใช้งานเมื่อมีการเปลี่ยนตำแหน่งหรือสิ้นสุดการจ้าง

๓.๓. การบริหารจัดการรหัสผ่านของผู้ใช้งาน (User Password Management)

เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ ผู้ใช้งานต้องปฏิบัติตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

๓.๔. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

ผู้ดูแลระบบ เจ้าของข้อมูลและเจ้าของระบบงาน ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่เหมาะสม โดยต้องมีการสอบทานความเหมาะสมของสิทธิของผู้ใช้งานในการเข้าใช้ข้อมูลอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงหรือควบคุมการใช้งานสารสนเทศจากผู้ที่ไม่ได้รับอนุญาต ต้องพิจารณาดังต่อไปนี้

๔.๑. ในกรณีที่อนุญาตให้ Protocol บางประเภทสามารถเข้าถึงระบบเครือข่ายของ สดช. จะต้องมีมาตรการการป้องกันล่วงหน้าและขั้นตอนการปฏิบัติงานโดยเฉพาะ

๔.๒. แม้ว่าจะมีการติดตั้ง Router และ Firewall เพื่อรักษาความปลอดภัยของระบบคอมพิวเตอร์แล้วก็ตาม การแก้ไขหรือเปลี่ยนแปลง Router และ Firewall ในภายหลังอาจก่อให้เกิดความเสี่ยงต่อระบบงานได้ เพื่อลดความเสี่ยงต่างๆ ทุกครั้งที่มีการเปลี่ยนแปลง Router และ Firewall จะต้องปฏิบัติตามนโยบายการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ

๔.๓. ห้ามทำ Packet Forwarding หรือ Re-routing สำหรับ Server ที่มีการติดตั้ง Protocol ที่สามารถทำได้ ได้แก่ กำหนดให้ FTP ไม่สามารถทำ IP Forwarding หรือ Passive mode ได้

๔.๔. หมายเลขเครือข่ายภายใน (Internal Network Address) ของ สดช. จำเป็นต้องมีการป้องกัน มิให้ส่วนงานที่เชื่อมต่อจากภายนอกสามารถมองเห็นได้ เพื่อป้องกันไม่ให้ Hackers หรือผู้ที่ไม่เกี่ยวข้องสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบงานเครือข่ายและส่วนประกอบของคอมพิวเตอร์ของ สดช. ได้โดยง่าย

๔.๕. ต้องกำหนด Access Control List ของ อุปกรณ์ Firewall และ Router ให้ป้องกันการส่งข้อมูลที่มาจากการปลอมแปลงหมายเลข IP Address และ หมายเลขของอุปกรณ์ (MAC Address)

๔.๖. สำหรับข้อมูลที่ผ่านเข้าและส่งออกจากระบบเครือข่าย สดช. ต้องส่งข้อมูลผ่าน Firewall เพื่อป้องกันการเชื่อมต่อจากผู้ที่ไม่ได้รับอนุญาต โดยกำหนดให้ผู้ดูแลระบบเครือข่ายเป็นผู้อนุมัติการเชื่อมต่อระบบเครือข่ายจากภายนอกของ สดช.

๔.๗. การเข้าสู่ระบบเครือข่ายของ สดช. ผ่านอินเทอร์เน็ต จะต้องมีการพิสูจน์ตัวตน และได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านระบบสารสนเทศก่อน

๔.๘. ระบบเครือข่ายทั้งหมดของ สดช. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก สดช. ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering ได้แก่ การใช้ Firewall หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

๔.๙. ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายัง สดช. โดยต้องกำหนดให้การเชื่อมต่อนี้เข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะกับระบบงานที่กำหนดไว้เท่านั้น และไม่

อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่าย สดช. ได้โดยอิสระ

๔.๑๐. ผู้ดูแลระบบต้องจัดแบ่งระหว่างเครือข่ายภายในและเครือข่ายภายนอก (Segregation in Networks) โดยพิจารณาจากบริการเครือข่ายของกลุ่มผู้ใช้งานทั้งสองฝ่าย โดยใช้ระบบหรืออุปกรณ์ป้องกันการบุกรุกด้วยการใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่น ๆ

๕. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก สดช. (User Authentication for External Connections)

ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก สดช. สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของ สดช. ได้

๕.๑. ผู้ใช้งานทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบเสียก่อน

๕.๒. การเข้าสู่ระบบของ สดช. ต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย ๑ วิธี เช่นการใช้บัญชีผู้ใช้ร่วมกับรหัสผ่าน เป็นต้น

๕.๓. ต้องแจ้งเป็นลายลักษณ์อักษรให้กับบุคคลที่ใช้บริการด้านสารสนเทศตามสัญญา ถึงความสำคัญที่มีต่อการรักษาความปลอดภัยของข้อมูลสารสนเทศ ซึ่งแต่ละบุคคลต้องลงนามในเอกสารสัญญาเรื่องการไม่เปิดเผยข้อมูลของ สดช. และจัดเก็บเอกสารไว้ในแฟ้มสัญญา

๕.๔. การเข้าสู่ระบบของ สดช. จากอินเทอร์เน็ต หรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องมีบัญชีรายชื่ออยู่ในทะเบียนผู้ใช้งาน และเพื่อเพิ่มความปลอดภัยในการเข้าสู่ระบบต้องมีการใช้วิธีการเข้ารหัส (Cryptographic) ร่วมกับการควบคุม

๖. การควบคุมอุปกรณ์ที่ผู้ดูแลระบบได้ติดตั้งไว้สำหรับการเข้าถึงจากภายนอก (Remote Diagnostic Port Protection)

ผู้อำนวยการกองแต่ละหน่วยงาน ต้องกำหนดให้มีการควบคุมการใช้งานอุปกรณ์ที่ผู้ดูแลระบบได้ติดตั้งไว้ภายใน สดช. เพื่อใช้ในการดูแลรักษาระบบจากภายนอก โดยมีแนวทางปฏิบัติดังนี้

๖.๑. การเข้าสู่ระบบเครือข่ายของ สดช. จากระยะไกลนั้น ก่อให้เกิดช่องโหว่ที่มีความเสี่ยงสูงต่อความมั่นคงปลอดภัยของข้อมูลและทรัพยากร การควบคุมผู้ใช้งานที่เข้าสู่ระบบจากระยะไกล จึงต้องมีมาตรการความมั่นคงปลอดภัยด้านสารสนเทศที่เพิ่มขึ้นจากมาตรการเข้าสู่ระบบภายใน สดช. ดังนี้

(๑) ปิดการใช้งานพอร์ตสายแลนที่ไม่ใช้งาน

(๒) ปิดการใช้งานปลั๊กไฟที่ไม่ใช้งาน

(๓) เปิดให้ใช้งานพอร์ตหรือบริการที่ได้รับอนุญาตเป็นลายลักษณ์อักษรเท่านั้น โดยมีการกำหนดระยะเวลาเปิดใช้งานอย่างจำกัด

(๔) ปิดกั้นการใช้งานพอร์ต USB ในอุปกรณ์ที่มีข้อมูลสำคัญ

๖.๒. วิธีใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลของ สดช. จากระยะไกลได้นั้น ต้องได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามนโยบายฯ ทุกเรื่องที่เกี่ยวข้องกับการเข้าสู่ระบบและข้อมูลของ สดช. เมื่อติดต่อจากระยะไกล นอกจากนี้เจ้าของข้อมูลมีหน้าที่ดูแลรักษาและเปลี่ยนแปลงรายชื่อของ

ผู้ใช้งานที่สามารถเข้าสู่ระบบจากระยะไกลให้ถูกต้องและเหมาะสม สามารถให้หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศตรวจสอบความถูกต้องได้

๖.๓. ต้องมีการกำหนดวิธีการพิสูจน์ตัวตน (Authentication Requirements)

๖.๔. ก่อนจะกำหนดสิทธิของผู้ใช้งานในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงรายละเอียดที่เกี่ยวข้อง ได้แก่ ระยะเวลาที่จะทำการ Remote หมายเลข IP ของเครื่องคอมพิวเตอร์ต้นทาง (Source IP Address) หมายเลข IP ของเครื่องคอมพิวเตอร์ปลายทาง (Destination IP Address) ที่จะ Remote เหตุผลหรือความจำเป็นรวมทั้งหลักฐานอย่างพอเพียงและต้องได้รับอนุมัติจากฝ่ายที่เป็นเจ้าของข้อมูลอย่างเป็นทางการเท่านั้น

๖.๕. ต้องควบคุม Port ที่ใช้ในการ Remote เข้าสู่ระบบงานของ สดช. อย่างรัดกุม ผู้ใช้งานที่มีความจำเป็นที่จะใช้งาน Remote ต้องได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ

๖.๖. ไม่ควรนำซอฟต์แวร์การควบคุมจากระยะไกลได้แก่ Team Veiwer PC-Anywhere หรือ Carbon copy มาใช้กับคอมพิวเตอร์ของ สดช. เพราะซอฟต์แวร์ดังกล่าวสามารถเป็นช่องทางให้ผู้ที่ไม่ประสงค์ดีเข้ามายังเครือข่ายของ สดช. และได้สิทธิพิเศษในการเข้าสู่ระบบ ทั้งนี้หากมีความจำเป็นต้องใช้ซอฟต์แวร์การควบคุมระยะไกลดังกล่าว ต้องได้รับอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามนโยบายฯ ทุกเรื่องที่เกี่ยวข้องกับการเข้าสู่ระบบและข้อมูลของ สดช.

๖.๗. การอนุญาตให้ผู้ดูแลระบบต่างๆ เข้าสู่ระบบข้อมูลของ สดช. จากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และต้องไม่เปิด Port เพื่อการซ่อมบำรุงระบบจากระยะไกลทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องถูกปิดไม่ให้สามารถใช้การได้และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น เมื่อผู้จัดจำหน่ายระบบทำการซ่อมบำรุงเสร็จเรียบร้อยแล้ว Port ดังกล่าวจะต้องทำการปิดไม่ให้ใช้การได้อีกครั้ง

๗. ความมั่นคงปลอดภัยสำหรับการให้บริการเครือข่าย (Security of Network Services)

ผู้อำนวยการกองแต่ละหน่วยงานและผู้ดูแลระบบ ต้องจัดทำข้อกำหนดหรือสัญญาด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่าง สดช. กับเจ้าหน้าที่ผู้ปฏิบัติงานภายใน สดช. ซึ่งมีแนวทางปฏิบัติดังนี้

๗.๑. ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิของผู้ใช้งาน เพื่อควบคุม "เจ้าหน้าที่" ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๗.๒. ผู้ดูแลระบบต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๗.๓. ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย(Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ "เจ้าหน้าที่" สามารถใช้เส้นทางอื่น ๆ ได้ ดังนี้

๗.๓.๑ ห้ามให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) และแผนผังเครือข่าย (Network diagram)

๗.๓.๒ อนุญาตใช้เส้นทางเครือข่าย เพื่อเชื่อมเครือข่ายปลายทางเฉพาะผ่านช่องทางที่กำหนดไว้

๗.๔. ระบบเครือข่ายทั้งหมดของ สดช. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก สดช. ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering ได้แก่ การใช้ Firewall หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

๗.๕. ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายัง สดช. โดยต้องกำหนดให้การเชื่อมต่อนี้เข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะกับระบบงานที่กำหนดไว้เท่านั้น และไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่าย สดช. ได้โดยอิสระ

๘. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๘.๑. ผู้ดูแลระบบต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย โดยมีแนวทางปฏิบัติดังนี้

๘.๑.๑. ต้องไม่แสดงรุ่น (Version)ของโปรแกรมจนกว่าจะ Log On เสร็จสิ้นสมบูรณ์

๘.๑.๒. ต้องไม่แสดง Help ระหว่าง Log On ซึ่งอาจช่วยให้ Hacker ค้นหาช่องทางเข้าได้

๘.๑.๓. ตรวจสอบความถูกต้องของข้อมูลนำเข้าเฉพาะเมื่อการนำเข้าเสร็จสิ้นสมบูรณ์แล้ว ถ้ามีความผิดพลาด ระบบต้องไม่แสดงว่าข้อมูลนำเข้าส่วนไหนไม่ถูกต้อง

๘.๑.๔. จำกัดจำนวนครั้งของการพยายามเข้าใช้ระบบ ได้แก่ ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง เป็นต้น และต้องพิจารณาเพิ่มเติมประเด็นต่อไปนี้

- บันทึกการพยายามทั้งที่สำเร็จและไม่สำเร็จ
- หลังจาก Log On ผิดพลาด บังคับระยะเวลาทิ้งช่วงก่อนที่จะยอมให้ทำต่อไป
- ตัดการเชื่อมโยงเครือข่าย
- ส่งข้อความเตือนไปยังหน้าจอของระบบ ถ้าความพยายามในการ Log On หลายครั้ง เกินจำนวนครั้งมากที่สุดที่ยอมรับได้
- กำหนดรหัสผ่านให้เหมาะสมกับความยาวของรหัสผ่านและมูลค่าของระบบที่จะต้องได้รับการป้องกัน

๘.๑.๕. จำกัดจำนวนครั้งสูงสุดในการ Log On ผิดพลาด ถ้าเกินกว่านั้นระบบต้องหยุดการให้ Log On

๘.๑.๖. ต้องแสดงข้อมูลต่อไปนี้หลังจากที่ Log On สำเร็จ

- วันที่และเวลาของการ Log On ครั้งที่แล้ว
- รายละเอียดของการพยายาม Log On ที่ไม่สำเร็จ ตั้งแต่การ Log On ครั้งที่แล้ว หรือสามารถค้นหาข้อมูลการ Log On ที่ผ่านมาได้

๘.๒. ผู้ดูแลระบบต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ มีแนวทางปฏิบัติดังนี้

๘.๒.๑. ต้องบังคับใช้สำหรับผู้ใช้งานทุกประเภท

๘.๒.๒. User ID ของผู้ใช้งานต้องสามารถตรวจสอบร่องรอยกิจกรรมของผู้ใช้งานแต่ละคนได้ในภายหลัง

๘.๒.๓. กิจกรรมงานประจำต้องไม่ดำเนินการโดยผู้ใช้งานที่ได้สิทธิพิเศษ

๘.๒.๔. กรณีที่จำเป็นต้องตรวจยืนยันตัวตนอย่างเข้มงวด อาจใช้วิธีอื่นแทนการใช้รหัสผ่านในการตรวจยืนยันตัวตนได้ ได้แก่วิธีการใช้การเข้ารหัสเพื่อรักษาความลับโดยใช้สมาร์ทการ์ด หรือ วิธีการทางไบโอเมตริก เป็นต้น

๘.๓. ผู้ดูแลระบบต้องมีการบริหารจัดการรหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

๘.๔. ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว มีแนวทางปฏิบัติดังนี้

๘.๔.๑. การใช้ยูทิลิตี้ต้องมีการระบุตัวตน ตรวจสอบยืนยัน และการควบคุมสิทธิของผู้ใช้งาน

๘.๔.๒. แยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมประยุกต์

๘.๔.๓. จำกัดการใช้งานของระบบยูทิลิตี้ให้เฉพาะสำหรับผู้ใช้งานที่จำเป็น

๘.๔.๔. การให้สิทธิการใช้ยูทิลิตี้แบบเฉพาะกิจ

๘.๔.๕. ต้องจำกัดสิทธิการใช้งานระบบยูทิลิตี้

๘.๔.๖. การยกเลิกระบบยูทิลิตี้ที่ไม่ได้ใช้งานหรือไม่จำเป็น

๘.๔.๗. ต้องไม่ให้สิทธิการใช้ยูทิลิตี้กับผู้ใช้งานที่มีสิทธิเข้าถึงระบบโปรแกรมประยุกต์

๘.๔.๘. ห้ามติดตั้งและใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์

๘.๕. ผู้ดูแลระบบต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้งานเมื่อไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้ มีแนวทางปฏิบัติดังนี้

๘.๕.๑. มีกลไกในการเคลียร์ Session เมื่อไม่ได้ใช้งานมาเป็นระยะเวลาที่กำหนด (Time-out)

๘.๕.๒. Time-out ต้องกำหนดให้เหมาะสมกับความเสี่ยงนั้น ประเภทข้อมูลที่เกี่ยวข้องและระบบซอฟต์แวร์นั้นๆ ซึ่งกำหนดการใช้งานเป็นระยะเวลา ๑ ชั่วโมงต่อการใช้งาน ๑ ครั้ง

๘.๖. ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง มีแนวทางปฏิบัติดังนี้

๘.๖.๑. ตัดการเชื่อมต่อเมื่อใช้งานได้ระยะหนึ่ง ซึ่งได้กำหนดไว้ล่วงหน้า

๘.๖.๒. จำกัดการเชื่อมต่อเครือข่ายให้เฉพาะภายในระยะเวลาทำการ โดยกำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง

๘.๖.๓. ให้ตรวจสอบยืนยันตัวตนใหม่ทุกช่วงเวลาที่กำหนด

๙. การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๙.๑. ผู้ดูแลระบบต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอปพลิเคชันตามนโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ โดยต้องแยกตามประเภทของผู้ใช้งาน การจำกัดสิทธิของผู้ใช้งาน ต้องพิจารณาอยู่บนพื้นฐานความจำเป็นของระบบซอฟต์แวร์แต่ละระบบ โดยมีแนวทางปฏิบัติดังนี้

๙.๑.๑. เตรียมหน้าจอหรือเมนูสำหรับควบคุมการเข้าถึงระบบของผู้ใช้งานแต่ละกลุ่ม โดยต้องแสดงข้อมูลที่ถูกต้องและเหมาะสมกับผู้ใช้งานแต่ละกลุ่ม

๙.๑.๒. ควบคุมสิทธิการเข้าถึงข้อมูลของผู้ใช้งานแต่ละกลุ่ม

๙.๑.๓. ควบคุมสิทธิการเข้าถึงข้อมูลของระบบซอฟต์แวร์อื่น

๙.๒. เจ้าของระบบงานต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ โดยมีแนวทางปฏิบัติดังนี้

๙.๒.๑. ต้องระบุให้ชัดเจนว่าระบบโปรแกรมประยุกต์ดังกล่าว มีความสำคัญ (Important) มีความเสียงที่จะเกิดผลกระทบสูง (Sensibility) ต่อหน่วยงาน อย่างไรและเจ้าของระบบต้องจัดทำรายละเอียดดังกล่าวเป็นเอกสาร

๙.๒.๒. เมื่อจำเป็นต้องใช้ระบบร่วมกันกับระบบอื่นหรือผู้ใช้งานอื่น จะต้องมีการระบุความเสี่ยงและมีการยอมรับโดยเจ้าของระบบนั้น

๑๐. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๑๐.๑ สร้างความตระหนักรู้ให้เกิดความเข้าใจในมาตรการป้องกัน

๑๐.๒ ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๑๐.๓ ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๑๐.๔ ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สาคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

นโยบายการบริหารจัดการรหัสผ่าน
(Password Management Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการใช้รหัสผ่าน

๒. การบริหารจัดการรหัสผ่าน

๒.๑. รหัสผ่านเป็นวิธีพื้นฐานในการระบุตัวตน ดังนั้นจึงต้องมีการควบคุมที่เข้มงวดเพื่อให้มั่นใจว่าผู้ที่เข้ามาใช้ระบบนั้นคือบุคคลที่มีสิทธิเข้าสู่ระบบข้อมูลของ สดช. จริง

๒.๒. ผู้ใช้งานระบบต้องลงนามยินยอมในสัญญาเรื่องการเก็บรักษารหัสผ่านไว้เป็นความลับ ซึ่งข้อความดังกล่าวรวมอยู่ในเงื่อนไขการจ้างงาน

๒.๓. สำหรับผู้ใช้งานรายใหม่จะได้รับรหัสผ่านเริ่มแรกในการผ่านเข้าระบบและเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที และต้องเปลี่ยนรหัสผ่านตามระยะเวลาอย่างน้อยปีละ ๒ ครั้ง

๒.๔. รหัสผ่านชั่วคราวจะมีการนำมาใช้สำหรับผู้ใช้งานที่ลืมรหัสผ่านและมีหลักฐานพิสูจน์ตนได้ว่าเป็นผู้ใช้งานที่มีสิทธิใช้งานระบบจริง ได้แก่ ตรวจสอบบัตร "เจ้าหน้าที่" เป็นต้น รหัสผ่านดังกล่าวต้องใช้อย่างระมัดระวังและจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๒.๕. ไม่ส่งรหัสผ่านผ่านเครือข่าย โดยไม่เข้ารหัสเพื่อรักษาความลับก่อน

๒.๖. ต้องกำหนดให้ผู้ใช้งานป้อน User ID และรหัสผ่านในการใช้งาน เพื่อป้องกันการปฏิเสธความรับผิดชอบ

๒.๗. กำหนดให้ผู้ใช้งานสามารถกำหนดรหัสผ่านของตนเองได้และมีกระบวนการตรวจสอบอีกครั้งก่อนยืนยันการเปลี่ยนรหัสผ่านเพื่อป้องกันความผิดพลาด

๒.๘. แนะนำให้ผู้ใช้งานกำหนดรหัสผ่านที่มีคุณภาพ ต้องมีการแนะนำว่ารหัสผ่านที่ผู้ใช้งานกำหนดนั้นอยู่ในระดับอ่อน ปานกลาง หรือแข็งแกร่ง เป็นต้น

๒.๙. ต้องมีการบันทึกประวัติการเปลี่ยนรหัสผ่านเพื่อป้องกันการใช้ซ้ำ

๒.๑๐. ต้องไม่แสดงรหัสผ่านที่พิมพ์ลงไปหรือซ่อนไม่ให้มองเห็นหรือเข้าใจได้

๓. การใช้งานรหัสผ่าน

๓.๑. เก็บรหัสผ่านไว้เป็นความลับ

๓.๒. ไม่เก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ในรูปแบบที่สามารถอ่านได้ หรือไม่เก็บรักษารหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถเห็นหรือเข้าถึงได้ง่าย ได้แก่ บนเครื่องคอมพิวเตอร์ บนโต๊ะทำงาน เป็นต้น และต้องเก็บข้อมูลรหัสผ่านไว้ต่างหากจากข้อมูลอื่น

๓.๓. ไม่พิมพ์รหัสผ่านในขณะที่มีผู้อื่นเห็นการพิมพ์ดังกล่าว

๓.๔. ไม่ทำการใดๆ เพื่อให้ตนเองทราบถึงบัญชีผู้ใช้งานหรือรหัสผ่านของผู้อื่น

๓.๕. เปลี่ยนรหัสผ่านส่วนของตนเองในครั้งแรกของการใช้งาน ไม่ว่าระบบจะบังคับให้มีการเปลี่ยนรหัสผ่านหรือไม่ก็ตาม และไม่ตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิม

๓.๖. เมื่อผู้ใช้งานตรวจพบ หรือสงสัยว่ารหัสผ่านของผู้ใช้งาน ถูกนำไปใช้โดยผู้อื่น ผู้ใช้งานต้องรายงานเหตุการณ์ให้ผู้ดูแลระบบทราบ และให้ดำเนินการเปลี่ยนรหัสผ่านทันที

๓.๗. ถ้าพบว่า รหัสผ่านของตนถูกล็อคโดยไม่ทราบสาเหตุ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบ

๓.๘. ในกรณีที่ได้รับความช่วยเหลือในการแก้ไขปัญหาและต้องการให้ใส่รหัสผ่าน ผู้ใช้งานต้องไม่ให้รหัสผ่านแก่ผู้ช่วยเหลือ แต่ต้องใส่รหัสผ่านด้วยตนเอง

๔. การกำหนดรหัสผ่าน

๔.๑. การกำหนดรหัสผ่านต้องไม่ใช้คำศัพท์ที่มาจากพจนานุกรม, ชื่อหนัง, ชื่อสถานที่หรือชื่อสิ่งลึกลับ และต้องไม่ใช้ข้อมูลที่เกี่ยวข้องกับ สดช. หรือเป็นข้อมูลส่วนตัวของผู้ใช้งานซึ่งอาจง่ายแก่การคาดเดา (ได้แก่ รหัส"เจ้าหน้าที่", ที่อยู่, ชื่อบุคคลในครอบครัว เป็นต้น)

๔.๒. ต้องไม่กำหนดรหัสผ่านที่ประกอบด้วยตัวอักษรหรือตัวเลขที่เรียงซ้ำกันเกินกว่า ๓ ตัว หรือเรียงกันตามลำดับ ได้แก่ aaaabbbb, 11111111, abcdefg

๔.๓. รหัสผ่านที่ดีต้องมีลักษณะดังนี้

๔.๓.๑. ต้องมีความยาวอย่างน้อย ๘ ตัวอักษรหรือตามที่ผู้ดูแลระบบกำหนด

๔.๓.๒. ต้องมีส่วนประกอบของอักษร อักขระพิเศษหรือตัวเลขประสมกันตามลักษณะดังนี้

๔.๓.๒.๑. ตัวอักษรใหญ่ ได้แก่ A, B, C, ...

๔.๓.๒.๒. ตัวอักษรเล็ก ได้แก่ a, b, c, ...

๔.๓.๒.๓. ตัวเลข ได้แก่ 0, 1, 2, ...

๔.๓.๒.๔. สัญลักษณ์พิเศษ ได้แก่ !, @, # , $, ...

๕. การเปลี่ยนรหัสผ่าน

๕.๑. รหัสผ่านเข้าสู่ระบบ (ได้แก่ root, NT Admin ฯลฯ) ต้องเปลี่ยนอย่างน้อยทุก ๖ เดือน

๕.๒. รหัสผ่านของระบบที่ให้บริการลูกค้าจะต้องเป็นส่วนหนึ่งของการจัดการฐานข้อมูลรหัสผ่านส่วนกลาง

๕.๓. รหัสผ่านของผู้ใช้งานต้องเปลี่ยนอย่างน้อยทุก ๖ เดือน

๖. การยกเลิกรหัสผ่าน

รหัสผ่านของผู้ใช้งานที่ลาออก สิ้นสุดการจ้างงานหรือย้าย ต้องดำเนินการยกเลิกสิทธิ (Disable) ของผู้ใช้งานในระบบทันที ส่วนการลบข้อมูลผู้ใช้จะพิจารณาเป็นแต่ละกรณี

นโยบายการควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking Policy)

๑. วัตถุประสงค์

นโยบายนี้จัดทำขึ้นเพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

๒. อุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communications)

เพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (ได้แก่ Notebook , Tablet และ Smart Phone เป็นต้น) ต้องพิจารณาดังต่อไปนี้

๒.๑. ในกรณีที่มีการใช้งานเครื่องคอมพิวเตอร์แบบพกพาที่เป็นสินทรัพย์ของ สดช. จะต้องปฏิบัติตามนโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook Computer Policy) อย่างเคร่งครัด

๒.๒. อุปกรณ์สื่อสารประเภทพกพาที่ได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศแล้วเท่านั้นที่จะสามารถเข้าถึงข้อมูลสารสนเทศของ สดช. ได้

๒.๓. อุปกรณ์สื่อสารประเภทพกพาจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

๒.๔. ไม่เก็บข้อมูลสำคัญของ สดช. ไว้บนอุปกรณ์สื่อสารประเภทพกพา แต่ถ้าไม่สามารถจัดเก็บบนเครื่องคอมพิวเตอร์ส่วนบุคคลของ สดช. ที่ใช้งานอยู่ได้ ข้อมูลที่จัดเก็บบนอุปกรณ์สื่อสารประเภทพกพา จะต้องมีวิธีการป้องกันบุคคลอื่น ๆ เข้าถึงข้อมูลสำคัญดังกล่าว ได้แก่ การใช้รหัสผ่าน (Password) ในการป้องกันเป็นต้น

๒.๕. ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

๒.๖. ผู้ใช้งานอุปกรณ์สื่อสารประเภทพกพา ต้องระวังการแอบดูข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต

๒.๗. คอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายอื่น ๆ ได้แก่ อุปกรณ์ทวนสัญญาณเครือข่ายไร้สาย (wireless Repeater) ที่ต้องการเชื่อมต่อกับระบบของ สดช. จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ

๒.๘. กรณีที่อุปกรณ์สื่อสารประเภทพกพาเป็นสมบัติของ สดช. การคืนเครื่องหรือส่งซ่อม ให้ผู้ใช้งานทำสำเนาข้อมูลจากอุปกรณ์สื่อสารประเภทพกพาเก็บไว้ทั้งหมด และลบข้อมูล

ทั้งหมดที่มีอยู่บนอุปกรณ์สื่อสารประเภทพกพา ก่อนส่งให้หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ

๒.๙. อุปกรณ์สื่อสารประเภทพกพา ได้แก่ เครื่องคอมพิวเตอร์แบบพกพา (Notebook), Tablet หรือ Smart Phone ต้องมีกระบวนการเพื่ออัพเดทระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ของ สดช.

๒.๑๐. หากผู้ใช้งานหมดสภาพการเป็น "เจ้าหน้าที่" ของ สดช. สิทธิในการใช้งานอุปกรณ์สื่อสารประเภทพกพาที่เป็นสมบัติของ สดช. เป็นอันสิ้นสุดลงทันที

๒.๑๑. สดช. อาจดำเนินการทางวินัย แพ่ง หรืออาญา กับผู้ที่ล่วงละเมิดโดยการใช้อุปกรณ์สื่อสารประเภทพกพาของ สดช. เพื่อเข้าถึง ล่วงละเมิดใช้งาน หรือล่วงละเมิดเผยแพร่ ข้อมูลสารสนเทศที่เป็นความลับโดยที่ผู้นั้นไม่มีสิทธิอันชอบ

หมวด ๘
การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
(Information System Acquisition, Development and Maintenance)

มีจุดประสงค์ เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ ป้องกันความผิดพลาด การสูญหายและการเปลี่ยนแปลงสารสนเทศ หรือการใช้งานสารสนเทศผิดวัตถุประสงค์ รักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยวิธีการเข้ารหัสข้อมูล สร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์ สารสนเทศ และไฟล์ต่างๆ ของระบบที่ให้บริการ ลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆโดยประกอบด้วย

- นโยบายการพัฒนาระบบสารสนเทศ
- นโยบายการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ

นโยบายการพัฒนาระบบสารสนเทศ
(IT Systems Development Policy)

๑. วัตถุประสงค์

เพื่อลดความเสี่ยงต่อการเสียหายหรือการเปลี่ยนแปลงแก้ไขข้อมูลและระบบสารสนเทศ ที่มีความสำคัญต่อการปฏิบัติราชการของ สดช.

๒. ความมั่นคงปลอดภัยด้านสารสนเทศในการพัฒนาระบบสารสนเทศ

๒.๑. หน่วยงานที่ดูแลระบบสารสนเทศ จะต้องทำการวิเคราะห์ระบบสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่างๆ ดังนี้

- มาตรการปฏิบัติก่อนเกิดความเสียหาย ได้แก่ การสำรองข้อมูล ระบบเครือข่ายสำรอง เป็นต้น
- มาตรการปฏิบัติหลังเกิดความเสียหาย ได้แก่ แผนการกู้คืน ระยะเวลาในการกู้คืน เป็นต้น

๒.๒. การพัฒนาระบบสารสนเทศต้องมีการควบคุม เพื่อให้เกิดความถูกต้องและเหมาะสมของข้อมูลที่นำเข้าและผลลัพธ์ที่ได้จากระบบ จึงจำเป็นที่จะต้องมีระบบการตรวจทานความถูกต้องของข้อมูลที่ดี เพื่อลดความเสี่ยงของการนำข้อมูลเข้าและการประมวลผลข้อมูล

๒.๓. หากระบบสารสนเทศที่พัฒนาขึ้น มีความเกี่ยวข้องกับการดำเนินงานขององค์กร การเงิน สุขภาพ ชีวิต ทรัพย์สิน ภาพลักษณ์ขององค์กร หน่วยงานเจ้าของระบบ ต้องทำการประเมินความเสี่ยง (Risk Evaluation) เพื่อให้ทราบถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินงานขององค์กร รวมทั้งและต้องจัดทำข้อตกลงในการให้บริการ (Service Level Agreement) ของระบบสารสนเทศที่พัฒนาด้วย

๒.๔. หน่วยงานภายใน สดช. ที่มีการพัฒนาระบบสารสนเทศ และอยู่ภายใต้โดเมนเนม onde.go.th (sub domain) ต้องแจ้งข้อมูลเกี่ยวกับระบบสารสนเทศนั้นให้ ขศ. ดังนี้

- รายชื่อผู้ดูแลรับผิดชอบระบบสารสนเทศ พร้อมเบอร์โทรศัพท์ และ อีเมล์
- ชื่อหน่วยงาน

- หมายเลข IP Address และสถานที่ติดตั้งระบบสารสนเทศ
- รายละเอียดทางเทคนิค ได้แก่ ระบบปฏิบัติการที่ใช้ ระบบฐานข้อมูล เทคโนโลยีหรือภาษาคอมพิวเตอร์ที่ใช้พัฒนาระบบสารสนเทศ เป็นอย่างน้อย

๒.๕. หน่วยงานภายใน สดช. ที่มีการพัฒนาระบบสารสนเทศที่ให้บริการในลักษณะ Web Application และอยู่ภายใต้โดเมนเนม onde.go.th (sub domain) จะต้องให้บริการผ่าน Protocal HTTPS โดยหน่วยงานสามารถขอใบรับรองอิเล็กทรอนิกส์ จาก ขศ.

๒.๖. หน่วยงานภายใน สดช. ที่มีการพัฒนาระบบสารสนเทศในลักษณะ Web Application หรือ Mobile Application จะต้องควบคุมการพัฒนาระบบสารสนเทศให้เป็นไปตามมาตรฐานการเขียน code ที่ดี (security coding) ได้แก่ OWAPS เป็นต้น

๒.๗. การพัฒนาระบบฐานข้อมูลของระบบสารสนเทศนั้น หากฐานข้อมูลดังกล่าวมีการจัดเก็บข้อมูลส่วนบุคคล ต้องพิจารณาถึง การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล การลบหรือทำลายข้อมูลส่วนบุคคล และ การรักษาความมั่นคงปลอดภัยของข้อมูล ให้เป็นไปตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒.๘. การตรวจสอบข้อมูลนำเข้า (Input Data Validate)
ในกรณีที่เจ้าของข้อมูลต้องการนำข้อมูลเข้าไปยังระบบสารสนเทศ ก่อนที่จะนำเข้า ต้องตรวจสอบข้อมูลว่าเป็นข้อมูลที่ถูกต้อง ครบถ้วนและไม่ก่อให้เกิดความเสียหายต่อระบบ และในกรณีที่เป็นข้อมูลส่วนบุคคล ผู้เก็บรวบรวมต้องแจ้งให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลข้อมูลส่วนบุคคล โดยให้เป็นไปตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒.๙. การควบคุมข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of Internal Processing)
ในกรณีที่เจ้าของข้อมูลมีการนำข้อมูลเข้าไปยังระบบสารสนเทศ ในระหว่างการประมวลผลจะต้องกำหนดกลไกสำหรับการตรวจสอบว่า ข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ ได้แก่ อาจมีสาเหตุจากความผิดพลาดในการประมวลผล การกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น

๒.๑๐. การตรวจสอบความถูกต้องของข้อความ (Message Integrity)
เจ้าของข้อมูลต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอปพลิเคชัน (เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง) รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต

๒.๑๑. การตรวจสอบข้อมูลผลลัพธ์ (Output Data Validation) ก่อนนำข้อมูลออกจากระบบต้องปฏิบัติดังนี้

- มีการอนุญาตจากเจ้าของข้อมูลให้นำข้อมูลออกจากระบบได้
- มีการตรวจสอบความถูกต้องของข้อมูล
- มีกระบวนการบันทึกโดยเข้ารหัสข้อมูล สามารถพิสูจน์และรับรองข้อมูล ในกรณีที่เป็นข้อมูลในชั้นความลับ

๓. **มาตรการการเข้ารหัสข้อมูล (Cryptographic controls)**

๓.๑. ต้องมีการกำหนดชั้นความลับของข้อมูลและสารสนเทศ เพื่อให้ทราบถึงสถานะและการดำเนินการในการเข้ารหัสข้อมูลสารสนเทศที่ใช้

๓.๒. เจ้าของข้อมูลต้องกำหนดให้มีการเข้ารหัสข้อมูลตามมาตรฐานสากล ได้แก่อัลกอริทึม RSA, AES,IDEA เป็นต้น และต้องมีการกำหนดชั้นความลับของข้อมูลและสารสนเทศ เพื่อให้ทราบถึงสถานะและการดำเนินการในการเข้ารหัสข้อมูลสารสนเทศที่ใช้

๓.๓. อัลกอริทึมที่เรียกใช้ต้องรองรับโปรแกรมประยุกต์ที่นำไปใช้งานได้ ได้แก่ PGP (Pretty Good Privacy), SSL (Secure Socket Layer), TLS (Transport Layer Security) เป็นต้น

๓.๔. ความยาวของคีย์ในการเข้ารหัสต้องไม่น้อยกว่า 56 บิตสำหรับการเข้ารหัสแบบสมมาตร (Symmetric) และแบบอสมมาตร (Asymmetric) ต้องมีความยาวไม่น้อยกว่าตามที่ตกลงกันไว้

๓.๕. เจ้าของข้อมูลต้องมีการทบทวนมาตรฐานของคีย์ที่เข้ารหัสในทุกๆปี เพื่อให้สอดคล้องกับความปลอดภัย และประสิทธิภาพของเครื่องที่ดำเนินงาน

๓.๖. กรณีที่ไม่ทราบหรือต้องการข้อมูลเกี่ยวกับการเข้ารหัสเพิ่มเติม ให้ติดต่อมาที่หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ

๓.๗. ข้อมูลที่มีการเข้ารหัส ต้องจัดให้มีกระบวนการในการบริหารจัดการกุญแจ (Key Management) ที่มีประสิทธิภาพ โดยการดำเนินการเกี่ยวกับกุญแจทุกประเภท ได้แก่ การสร้าง การจัดเก็บ การจัดส่ง และการเปลี่ยน ต้องกระทำอย่างปลอดภัยและมีการควบคุมที่เหมาะสม

๔. **ความมั่นคงปลอดภัยด้านสารสนเทศของแฟ้มข้อมูลระบบ (Security of System Files)**

๔.๑. หลักการควบคุมการติดตั้งซอฟต์แวร์ (Control of Operational Software)
ผู้อำนวยการกองต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ให้สอดคล้องกับหลักเกณฑ์การติดตั้งระบบสารสนเทศใหม่

๔.๒. หลักการป้องกันข้อมูลจริงที่ใช้ในการทดสอบระบบ (Protect of System Test Data)
ข้อมูลจริงที่จะนำใช้ทดสอบระบบ ต้องได้รับอนุญาตจากผู้อำนวยการกองที่รับผิดชอบในการรักษาข้อมูลนั้นๆ ก่อน เมื่อใช้งานเสร็จจะต้องลบข้อมูลจริงออกจากระบบทดสอบทันที และบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ทดสอบอะไรบ้าง รวมถึงวันเวลาและหน่วยงานที่ทดสอบ แจ้งไปยังผู้อำนวยการกองที่รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

๔.๓. หลักการควบคุมการใช้งานซอฟต์แวร์ไลบารี่ (Access Control to Program Source Library)
ผู้อำนวยการกองและหน่วยงานเจ้าของระบบต้องมีการควบคุมการใช้งานไลบารี ซึ่งประกอบด้วย Source Code ของระบบที่ใช้งานจริงหรือระบบที่ให้บริการ โดยมีแนวทางปฏิบัติดังนี้

- ห้ามเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริง และต้องเก็บไว้ในที่ปลอดภัย
- ผู้อำนวยการกองที่รับผิดชอบต้องแต่งตั้งผู้มีอำนาจในการดูแลและปรับปรุงไลบารี่
- ระหว่างทดสอบต้องไม่เก็บ Source Code ที่ใช้ทดสอบรวมกับไลบารี่ที่ใช้งานได้จริง

๔.๔. การเผยแพร่ไฟล์เอกสารดิจิทัลที่มีชั้นความลับ ได้แก่เอกสารราชการ ที่มีการประทับลับ และลับมาก ผ่านสื่อออนไลน์ ได้แก่ เว็บไซต์ หรือโมบายแอปพลิเคชั่น จะต้องได้รับอนุญาตจากผู้อำนวยการหน่วยงานเป็นอย่างน้อย จึงสามารถเผยแพร่เอกสารผ่านสื่อออนไลน์ได้

๕. ขั้นตอนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการพัฒนาระบบ (Security in Development and Support Processes)

๕.๑. การตรวจสอบซอฟต์แวร์ที่จัดหามาใช้งาน
ผู้อำนวยการกองหรือหน่วยงานที่เกี่ยวข้องต้องมีการตรวจสอบหรือทดสอบซอฟต์แวร์ที่จัดหามาใช้งานก่อนติดตั้ง เพื่อป้องกันตัว Source Code ที่ไม่พึงประสงค์แฝงตัวมากับตัวซอฟต์แวร์นั้น (Covert Channel and Trojan Code)

๕.๒. การควบคุมการว่าจ้างพัฒนาระบบ (Outsourced Software Development)
ผู้อำนวยการกองหรือหน่วยงานที่ว่าจ้างการพัฒนาระบบ ต้องมีการทำสัญญาว่าจ้างการพัฒนาระบบ ซึ่งต้องครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบโดยละเอียดก่อนติดตั้งใช้งานจริง การรับรองคุณภาพของระบบ รวมถึงการกำหนดขอบเขตในการจ้างพัฒนาระบบ

๕.๓. การตรวจสอบระบบสารสนเทศทั้งหมดที่เกี่ยวข้อง (Technical Review of Operating System Changes)
ผู้อำนวยการกองหรือหน่วยงานที่ว่าจ้างการพัฒนาระบบ ต้องตรวจสอบระบบสารสนเทศที่เกี่ยวข้องภายหลังที่ได้ติดตั้งระบบใหม่ เพื่อให้ทราบถึงผลกระทบจากการพัฒนาระบบและเป็นไปตามเงื่อนไขในการว่าจ้าง พร้อมทั้งมีการตรวจสอบจากหน่วยงานที่เกี่ยวข้องหลังจากการติดตั้งระบบใหม่หรือการปรับปรุง โดยแจ้งไปยังผู้อำนวยการกองที่รับผิดชอบ และเก็บรายละเอียดตัวเอกสารไว้เป็นหลักฐาน

๖. การติดตั้งระบบสารสนเทศใหม่

หน่วยงานที่จะนำระบบใหม่มาติดตั้งจะต้อง แจ้งรายละเอียดของระบบงานให้ ศท ทราบดังนี้

๖.๑. รายการอุปกรณ์ที่จะนำมาติดตั้งพร้อมกับรายละเอียดคุณลักษณะเฉพาะของอุปกรณ์ ชื่อรุ่น ยี่ห้อ และหมายเลขครุภัณฑ์

๖.๒. รายการซอฟต์แวร์แพคเกจที่จะนำมาติดตั้ง พร้อมกับรายละเอียด ยี่ห้อ เวอร์ชั่น ประเภทซอฟต์แวร์และหมายเลขครุภัณฑ์

๖.๓. รายการของระบบงานที่พัฒนาใหม่ ประกอบด้วย ชื่อระบบงาน หรือชื่อโครงการ ภาษาที่ใช้ในการพัฒนา เครื่องมือในการพัฒนา ชื่อซอฟต์แวร์และเวอร์ชั่นของระบบฐานข้อมูลที่ใช้

๖.๔. ชื่อโครงการ เลขที่สัญญา และหน่วยงานที่รับผิดชอบ พร้อมรายชื่อ เบอร์โทรศัพท์ อีเมล์ของผู้ประสานงานด้านนโยบายและด้านเทคนิค

๖.๕. วันที่ เวลา ที่ติดตั้งระบบงาน และวันที่ เวลาเปิดใช้งาน

๖.๖. กรณีการติดตั้งระบบงานที่มีการเชื่อมต่อออนไลน์ จะต้องผ่านการทดสอบความมั่นคงปลอดภัยของซอสโค้ด และมีหลักฐานการตรวจสอบความมั่นคงปลอดภัยและจะต้องไม่มีช่องโหว่ระดับความเสี่ยงสูง (Critical Risk) หรือมีหลักฐานแสดงว่าได้ดำเนินการแก้ไขแล้วจึงสามารถเปิดใช้งานได้

นโยบายการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ
(IT change management policy)

๑. วัตถุประสงค์

การเปลี่ยนแปลงระบบงานทางราชการใดๆ จะต้องมีการควบคุม เพื่อไม่ให้มีผลกระทบต่อโปรแกรมประยุกต์(Application Software) โปรแกรมระบบ (System Software) ระบบเครือข่าย (Network System) หรือการเปลี่ยนแปลงอื่นๆ ที่เกิดจากการเปลี่ยนแปลงระบบงาน ได้แก่ การพัฒนาระบบ การทดสอบระบบ จะต้องอยู่ภายใต้การควบคุมที่เหมาะสมและเพียงพอ โดยวิธีการดังกล่าวจะช่วยให้ระบบสารสนเทศนั้นๆ สามารถทำงานเข้ากันได้ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์

การเปลี่ยนแปลงแก้ไข ต้องมีคำขอการเปลี่ยนแปลงอย่างเป็นทางการ ซึ่งมีการอนุมัติโดยผู้บริหารที่มีอำนาจอนุมัติการเปลี่ยนแปลงระบบงานนั้นๆ

๒. ความต้องการในการขอให้มีการเปลี่ยนแปลง

๒.๑. ผู้ร้องขอ ต้องดำเนินการตามกระบวนการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริงหรือใช้งานอยู่แล้วโดยทำหนังสือแจ้งไปยังหน่วยงานเจ้าของข้อมูล หน่วยงานเจ้าของระบบงาน และหรือหน่วยงานที่เกี่ยวข้องทุกส่วนให้รับทราบก่อนทำการแก้ไขซอฟต์แวร์นั้น และต้องมีการอนุมัติโดยผู้มีอำนาจในการลงนามในแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form by User) แบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ จะต้องมีข้อมูลที่จำเป็นดังนี้

- คำขอให้แก้ไขต้องมาจาก**ผู้มีสิทธิ**
- เหตุผลการปฏิบัติราชการที่ต้องมีการเปลี่ยนแปลง
- ลักษณะของข้อบกพร่องที่ทำให้ต้องมีการเปลี่ยนแปลง (ถ้ามี)
- ทรัพยากรที่จำเป็นต้องใช้ในการเปลี่ยนแปลงระบบงาน
- รายละเอียดการทดสอบ (Test Script)
- กระบวนการนำระบบเดิมที่ใช้งานได้กลับมาใช้ใหม่ ในกรณีที่ระบบใหม่มีปัญหา
- ต้องได้รับการอนุมัติคำขอโดยผู้มีอำนาจ
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
- ต้องเก็บรายละเอียดของคำขอไว้เป็นหลักฐาน

๒.๒. ผู้อำนวยการกอง เจ้าของข้อมูล (Information Owner) และผู้อำนวยการกอง เจ้าของระบบงาน (Application Owner) ที่เกี่ยวข้องกับการเปลี่ยนแปลงนั้นๆ จะต้องพิจารณาเหตุผลทางราชการของคำขอเปลี่ยนแปลง และทำการลงนามอนุมัติในคำขอเปลี่ยนแปลง

๒.๓. ทุกครั้งที่มีการเปลี่ยนแปลงระบบงาน จะต้องมีการจัดเตรียมและปรับปรุงคู่มือในการใช้งานระบบงานและคู่มือในการอบรมให้กับผู้ใช้งาน ต้องมีการจัดทำและปรับปรุงให้สอดคล้องกับการเปลี่ยนแปลงระบบงานอยู่เสมอ

๓. การกำหนดบทบาทและหน้าที่การเปลี่ยนแปลง

๓.๑. ต้องมีการกำหนดบทบาทและความรับผิดชอบของแต่ละบุคคลที่เกี่ยวข้องกับกระบวนการควบคุมการเปลี่ยนแปลงอย่างชัดเจน เพื่อการควบคุมที่ดี ต้องไม่ทำโดยบุคคลเดียวกัน

๓.๒. ต้องมีการกำหนดผู้รับผิดชอบระบบอย่างชัดเจน และเมื่อมีการเปลี่ยนแปลงผู้รับผิดชอบหรือบทบาทความรับผิดชอบ จะต้องแจ้งให้ ศูนย์ข้อมูลเศรษฐกิจและสังคมดิจิทัล (ขศ.) ทราบอย่างชัดเจน

๓.๓. โปรแกรมที่ใช้งานจริงสำหรับระบบงานนั้นๆ ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิในการโอนย้ายโปรแกรมที่พร้อมใช้งานไปยังส่วนที่ใช้งานจริง

๓.๔. ต้องแบ่งแยกส่วนที่ใช้สำหรับงานต่อไปนี้ออกจากกัน ได้แก่ ส่วนการพัฒนาระบบงาน ส่วนที่ใช้สำหรับโอนย้ายโปรแกรมก่อนการย้ายเข้าส่วนที่ใช้งานจริง ส่วนที่ใช้ทดสอบระบบสำหรับผู้ใช้งาน และส่วนที่ใช้งานจริง ในแต่ละส่วนต้องมีการควบคุมการเข้าใช้งานที่ดี

หมายเหตุ ถ้าไม่สามารถแบ่งแยกส่วนที่ใช้สำหรับทดสอบระบบงาน (ได้แก่ ระบบงานบนเครื่อง Mainframe ที่ไม่คุ้มที่จะแยกเครื่องเพื่อการทดสอบระบบกับเครื่องที่ใช้พัฒนาระบบได้) ให้แยกส่วนที่ใช้สำหรับการทดสอบระบบโดยผู้ใช้งานออกจากส่วนที่ใช้พัฒนาระบบงาน

๔. การเปลี่ยนแปลงระบบคอมพิวเตอร์ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูล

๔.๑. การเปลี่ยนแปลงต่อระบบคอมพิวเตอร์ ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูล จะต้องได้รับอนุมัติจากผู้อำนวยการกองที่ดูแลระบบงานนั้นๆ เป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการหยุดชะงักของการปฏิบัติราชการ หรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

๔.๒. การเปลี่ยนแปลงระบบงานใดๆ ต้องไม่รบกวนหรือขัดขวางการปฏิบัติงานของระบบงานปัจจุบัน และการเปลี่ยนแปลงดังกล่าวนั้น จะต้องสามารถใช้งานร่วมกับข้อมูลและระบบงานที่มีการใช้อยู่ในปัจจุบันได้ด้วย

๔.๓. การเปลี่ยนแปลงอุปกรณ์หรือสื่อที่ใช้ในการจัดเก็บข้อมูล ต้องทำการลบข้อมูลที่ไม่ใช้งานแล้วทั้งหมดของ สดช. อย่างถาวรออกจากอุปกรณ์หรือสื่อที่ใช้สำหรับเก็บข้อมูลที่มีการเปลี่ยนแปลง

๔.๔. มีกระบวนการทำลาย หรือจำหน่ายอุปกรณ์เสื่อมสภาพหรือหมดอายุ

๔.๕. ผู้รับผิดชอบระบบต้องแจ้ง ขศ. เมื่อมีอุปกรณ์เครือข่าย หรือ เครื่องแม่ข่ายของระบบงานใหม่มาติดตั้ง

๕. การเปลี่ยนแปลง Source Code

๕.๑. สำหรับ Source Code ที่ใช้งานจริงต้องมั่นใจว่า Source Code ทั้งหมดมีการจัดเก็บไว้ในที่เดียวกัน ซึ่งการเปลี่ยนแปลงจะต้องได้รับอนุมัติให้ทำการแก้ไขแล้วเท่านั้น เมื่อมีการแก้ไขโปรแกรม จะมีการนำเอา Source Code จากที่จัดเก็บไปทำการแก้ไข การเปลี่ยนแปลงแก้ไข Source Code ที่ใช้งานจริงต้องมีการควบคุม Version ของ Source Code อย่างเคร่งครัด

๕.๒. ผู้ทำหน้าที่ในการเปลี่ยนแปลงแก้ไขต้องถูกจำกัดสิทธิในการเข้าถึงส่วนระบบงานที่ใช้จริง ผู้ทำการแก้ไขจะได้รับอนุญาตให้ทำการคัดสำเนา Source Code เพื่อใช้ในการแก้ไขพัฒนา

โปรแกรมในส่วนที่ใช้สำหรับการพัฒนาระบบงาน และทำการย้ายโปรแกรมที่แก้ไขเสร็จเข้าสู่ส่วนที่ใช้สำหรับโอนย้ายโปรแกรม ก่อนการย้ายเข้าส่วนที่ใช้งานจริงเท่านั้น

๕.๓. กรณีการแก้ไขซอสโค้ดของระบบงานที่มีการเชื่อมต่อออนไลน์ จะต้องผ่านการทดสอบความมั่นคงปลอดภัยของซอสโค้ด และมีหลักฐานการตรวจสอบความมั่นคงปลอดภัยและจะต้องไม่มีช่องโหว่ระดับความเสี่ยงสูง (Critical Risk) หรือมีหลักฐานแสดงว่าได้ดำเนินการแก้ไขแล้วจึงสามารถเปิดใช้งานได้

๖. การควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ (Restrictions on Changes to Software Packages)

ผู้ดูแลระบบหรือหน่วยงานที่ดูแลระบบต้องจัดให้มีการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจที่จัดซื้อ โดยมีแนวทางปฏิบัติดังนี้

๖.๑. หลีกเลี่ยงการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ

๖.๒. ในกรณีที่หลีกเลี่ยงไม่ได้ในการเปลี่ยนแปลงแก้ไข ให้ขออนุญาตเจ้าของลิขสิทธิ์เพื่อเปลี่ยนแปลงแก้ไข หรือมอบให้ผู้ขายดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจให้

๖.๓. ในการเปลี่ยนแปลงซอฟต์แวร์แพ็กเกจ ให้ฝ่ายที่รับผิดชอบเก็บตัวซอฟต์แวร์ต้นฉบับไว้อีกชุดหนึ่ง

๖.๔. ตัวซอฟต์แวร์แพ็กเกจที่แก้ไขจะต้องได้รับการตรวจสอบเป็นอย่างดีว่าจะไม่มีผลกระทบต่อระบบ

๖.๕. กรณีมีการ Update Patch หรือ มีการแก้ไขช่องโหว่ ของซอฟต์แวร์แพ็กเกจ จะต้องทำการทดสอบผลกระทบจากการ Update Patch ดังกล่าวก่อนจะนำไปใช้งานกับระบบงานจริง

๗. การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ หน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยงและหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ร่วมกันกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว ซึ่งมีแนวทางปฏิบัติดังต่อไปนี้

๗.๑. ต้องกำหนดหน้าที่ความรับผิดชอบที่ชัดเจน ได้แก่ การเฝ้าระวังภัยคุกคาม การประเมินความเสี่ยงของภัยคุกคาม การ Patch ปิดช่องโหว่ในระบบ การตรวจสอบสินทรัพย์ที่ได้จัดหมวดหมู่ไว้ เป็นต้น

๗.๒. เจ้าของระบบงานต้องวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาด ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศทุก ๑๒ เดือน

๗.๓. ในกรณีที่จะทำการ Update Patch ของระบบสำคัญๆ จะต้องดำเนินการสำรองข้อมูล Source Code และ จัดเก็บค่าคอนฟิคของระบบ รวมทั้งต้องมีการทดสอบและประเมินก่อนว่าจะไม่ก่อให้เกิดความเสียหายต่อระบบ แต่ถ้าไม่สามารถ Update Patch ได้ ก็ให้พิจารณาดังต่อไปนี้

๗.๒.๑. ปิด Service หรือการทำงานที่เกี่ยวข้องกับช่องโหว่ ในกรณีที่ Service ดังกล่าวส่งผลกระทบร้ายแรงต่อระบบเครือข่ายคอมพิวเตอร์หรือระบบงานคอมพิวเตอร์อื่น ๆ

๗.๒.๒. ปรับปรุงหรือเพิ่มระดับ Security ในการเข้าถึงที่บริเวณรอบนอกเครือข่าย ได้แก่ เพิ่ม Firewall หรือ IPS(Intrusion Prevention System) เป็นต้น

๗.๒.๓. เพิ่มการเฝ้าระวัง เพื่อตรวจจับหรือป้องกันการโจมตีเครือข่าย

๗.๒.๔. สร้างความตระหนักเกี่ยวกับช่องโหว่ที่เกิดขึ้น

๗.๒.๕. เก็บ Log ของเหตุการณ์ที่เกิดขึ้นทั้งหมดเพื่อใช้ในการตรวจสอบ

๗.๒.๖. กระบวนการบริหารจัดการช่องโหว่ที่มีดำเนินการ ได้แก่ การเฝ้าระวัง ต้องมั่นใจว่ามีประสิทธิภาพและประสิทธิผล

๗.๒.๗. ระบบที่มีความเสี่ยงสูงจะต้องมีการเตรียมการเป็นอันดับแรกตามลำดับความสำคัญ

๘. แนวทางปฏิบัติของการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (โดยผู้ใช้งาน)

๘.๑. ผู้ร้องขอจะต้องกรอกรายละเอียดลงในแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form by User) โดยผ่านการอนุมัติจากผู้บังคับบัญชา และ/หรือ Process Owner ส่งแบบคำขอฯไปยังหน่วยงานผู้ดูแลระบบ ได้แก่ หน่วยงานระบบด้าน Hardware, Software, Database, Network เป็นต้น

๘.๒. ในกรณีเร่งด่วน อนุโลมให้ผู้ร้องขอ ส่งแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form by User) ทางโทรสารก่อนการส่งต้นฉบับ

๘.๓. หน่วยงานผู้ดูแลระบบกำหนดหมายเลขคำขอเมื่อได้รับแจ้ง โดยใช้ชื่อย่อหน่วยงาน หมายเลข/ปีพ.ศ. ได้แก่ ลป.๑/๒๕๕๔

๘.๔. หน่วยงานผู้ดูแลระบบ พิจารณาตามคำขอ โดยศึกษา วิเคราะห์ ผลกระทบจากการแก้ไข แนวทางในการกลับคืนสู่สภาพเดิม (Recovery) กำหนดแนวทางการดำเนินงาน ระยะเวลา และผู้ดำเนินการแก้ไข ได้แก่ ผู้วิเคราะห์ ผู้จัดทำหรือปรับปรุงโปรแกรม ผู้ทดสอบระบบ เป็นต้น

๘.๕. หน่วยงานผู้ดูแลระบบ แจ้งผลการวิเคราะห์กลับไปยังผู้อนุมัติแบบคำขอฯ เพื่อรับทราบ และ/หรือยืนยัน พร้อมให้แจ้งรายชื่อผู้ดำเนินการทำ User Acceptance Test (UAT) ในกรณีที่หน่วยงานผู้ดูแลระบบเป็นผู้ร้องขอ ที่มีผลกระทบต่อระบบโดยรวม ได้แก่ การเปลี่ยนแปลงเวอร์ชันโปรแกรม การแก้ไขระบบเครื่อง Server อุปกรณ์เครือข่าย ฯลฯ จะต้องมีการทดสอบยอมรับระบบ (UAT) ก่อนนำไปในระบบใช้งานจริงเสมอ โดยหน่วยงานผู้ดูแลระบบแจ้งหน่วยงานที่เกี่ยวข้องทราบ เพื่อร่วมดำเนินการทำ UAT ต่อไป

๘.๖. หน่วยงานผู้ดูแลระบบต้องดำเนินการให้ผู้ร้องขอ และ/หรือผู้ใช้งานที่เกี่ยวข้องทำการทดสอบยอมรับระบบ (UAT) พร้อมลงนาม

๘.๗. หน่วยงานผู้ดูแลระบบต้องดำเนินการ ให้ผู้ร้องขอ และ/หรือ ผู้รับผิดชอบดูแลข้อมูล (Data Owner) ดำเนินการแปลงข้อมูล (Data Conversion) (ถ้ามี) โดยผู้รับผิดชอบดูแลข้อมูล (Data Owner) ต้องจัดเตรียม ตรวจสอบ รับรองความถูกต้องของข้อมูลทั้งก่อนและหลังนำเข้าระบบ

๘.๘. หลังจากผ่านการทดสอบการยอมรับระบบ หน่วยงานผู้ดูแลระบบ จะต้องจัดทำคู่มือระบบงาน (Systems Manual) และ/หรือ จัดการอบรมการใช้งาน/จัดทำคู่มือการใช้งาน (User/Operation Manual) ให้กับผู้ใช้งาน

๘.๙. หน่วยงานผู้ดูแลระบบ แจ้งผู้เกี่ยวข้องนำส่วนที่เปลี่ยนแปลงแก้ไขเข้าสู่ระบบใช้งานจริง (Production) และแจ้งกลับผู้ร้องขอ

๘.๑๐. Process Owner และหน่วยงานผู้ดูแลระบบ ติดตามตรวจสอบ (Monitor and Track Error) ว่าระบบสามารถทำงานได้ถูกต้องตามวัตถุประสงค์ภายในระยะเวลาที่เหมาะสม

๘.๑๑. เมื่อได้ดำเนินงานแล้ว หน่วยงานผู้ดูแลระบบต้องจัดเก็บเอกสารที่เกี่ยวข้อง ได้แก่ แบบคำขอฯ แนวทางการดำเนินงาน รายละเอียดการดำเนินงาน เอกสารการทดสอบ คู่มือ ฯลฯ ให้สามารถใช้อ้างอิงได้

๙. แนวทางปฏิบัติของการเปลี่ยนแปลง/แก้ไขระบบ (โดยผู้ดูแลระบบ)

๙.๑. ผู้ดูแลระบบ กรอกรายละเอียดลงในแบบฟอร์มการเปลี่ยนแปลง/แก้ไขระบบเครือข่าย (Change Request Form by Admin) โดยผ่านการอนุมัติจากผู้บังคับบัญชา

๙.๒. ผู้ดูแลระบบ ต้องระบุรายละเอียดในการเปลี่ยนแปลง/แก้ไขระบบเครือข่ายอย่างชัดเจน ได้แก่ วันเวลาที่แจ้ง รายละเอียดของผู้ดูแลระบบ สถานที่ปฏิบัติงานแก้ปัญหา วิธีการแจ้งปัญหา/สาเหตุการแก้ไข รายละเอียดของการปฏิบัติงาน ระยะเวลาในการแก้ไข ระบบที่ได้รับผลกระทบ

๙.๓. ผู้ดำเนินการแก้ไขต้องมีการเตรียมแผนสำรองฉุกเฉิน ในกรณีที่การเปลี่ยนแปลง/แก้ไขระบบเครือข่ายนั้นเกิดปัญหา เมื่อเกิดการล้มเหลวในการเปลี่ยนแปลง/แก้ไขระบบเครือข่าย ผู้ดำเนินการแก้ไขจะต้องสามารถเปลี่ยนกลับมาใช้ระบบเดิมได้ตามปกติ

๙.๔. ผู้ดำเนินการแก้ไขต้องมีการทดสอบให้มั่นใจก่อนใช้งานระบบจริง

๙.๕. เมื่อได้ดำเนินงานแล้ว ผู้ดำเนินการแก้ไขต้องลงนามและจัดเก็บเอกสารที่เกี่ยวข้อง ได้แก่ แบบฟอร์มฯ ที่ผู้แจ้งปัญหาหรือผู้ดูแลระบบแจ้งมา เอกสารหรือรายละเอียดของระบบทั้งก่อนและหลังการแก้ไข เป็นต้น เพื่อให้สามารถใช้อ้างอิงได้

แบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (โดยผู้ใช้งาน)

(Change Request Form By User)

(สำหรับผู้ดูแลระบบ) หมายเลขคำขอ _____

(สำหรับผู้ร้องขอ)

วันที่_____

ชื่อผู้ร้องขอ_____

ส่วน _____ ฝ่าย _____ โทรศัพท์ _____ โทรสาร _____

ชื่อระบบ _____

เหตุผลและความจำเป็น_____

_____

_____

รายละเอียดความต้องการ

_____

_____

_____

เอกสารแนบ_____ ฉบับ

ระดับความเร่งด่วน ☐ ด่วน (Emergency) ☐ ปกติ (Normal)

วันที่ต้องการใช้งาน_____

ลงนามผู้ร้องขอ _____ ลงนามผู้อนุมัติ (ผู้บังคับบัญชา)_____

( ) ( )

ตำแหน่ง _____ ตำแหน่ง _____

(สำหรับผู้ดูแลระบบ)

ลงนามผู้มอบหมาย _____ ลงนามผู้รับมอบ _____

( ) ( )

ตำแหน่ง _____ ตำแหน่ง _____

ลงวันที่ _____ ลงวันที่ _____

วิเคราะห์ผลกระทบ

1. ประเภทของผลกระทบ ☐ Application, Software ☐ Network Configuration
☐ System Configuration ☐ System Software Upgrade
☐ Other _____

2. Module/Screen/Table/File/etc. Effect

_____

_____

_____

_____

3. Document

Effect _____

_____

_____

_____

4. รายละเอียดผลกระทบในการดำเนินงาน

_____

_____

_____

_____

กำหนดระยะเวลาการดำเนินงาน (Time Estimate)

กระบวนการ	ระยะเวลาในการดำเนินการ(วัน)		วันที่เริ่ม/วันที่แล้วเสร็จ	ผู้รับผิดชอบ	ลงนาม
	คาดว่าจะแล้วเสร็จ	เวลาที่ใช้จริง			
วิเคราะห์ออกแบบ					
พัฒนา/แก้ไข					
ทดสอบ					

UAT				(ผู้ใช้งาน) (ผู้ดูแลระบบ)	
Data Conversion				(ผู้ดูแลข้อมูล) (ผู้ดูแลระบบ)	
จัดทำ/ปรับปรุงเอกสารที่เกี่ยวข้อง/อบรม					
สรุป (Total Time)					

แนวทางการกลับคืนสู่สภาพเดิม _____

_____

_____

_____

_____

งบประมาณที่ใช้ _____

ความเห็นและทางเลือกอื่นที่เป็นไปได้ _____

_____

การอนุมัติการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ

☐ อนุมัติ ☐ ไม่อนุมัติ ☐ อื่นๆ _____

ลงนาม _____

( )

เหตุผล _____

_____

ตำแหน่ง _____

ลงวันที่ _____

(สำหรับหน่วยงานเจ้าของกระบวนงาน (Process Owner))

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ลงนาม _____ เหตุผล _____

( )

ตำแหน่ง _____

ชื่อผู้ดำเนินการ UAT _____ ลงวันที่

_____

(สำหรับผู้ร้องขอ)

ชื่อผู้ดำเนินการ UAT _____

ลงนาม _____

( )

ตำแหน่ง _____

ลงวันที่ _____

(สำหรับผู้ดูแลข้อมูล (Data Owner)) กรณีที่มีการแปลงข้อมูล

ชื่อผู้ดำเนินการ Data Conversion _____

ลงนาม _____

( )

ตำแหน่ง _____

ลงวันที่ _____

(สำหรับผู้ดูแลระบบ , Process Owner และผู้ร้องขอ)

วันที่เริ่มใช้งานจริง _____ อ้างอิงเอกสาร _____ Process Owner ลงนาม _____ ( ) ตำแหน่ง _____ ลงวันที่ _____	ผู้ดูแลระบบลงนาม _____ ( ) ตำแหน่ง _____ ลงวันที่ _____ ผู้ร้องขอลงนาม _____ ( ) ตำแหน่ง _____ ลงวันที่ _____

(ลงนามครบแล้ว ส่งเรื่องคืนให้ผู้ดูแลระบบจัดเก็บ)

<u>การเตรียม/ตรวจสอบ/รับรองความถูกต้องของข้อมูล</u>

ชื่อผู้ดำเนินการ _____ ลงนาม _____

ชื่อผู้อนุมัติ _____ ลงนาม _____

ผู้ดูแลระบบจัดทำเอกสารที่เกี่ยวข้องฯ เรียบร้อยวันที่ _____ ลงนาม _____

เอกสารที่เกี่ยวข้อง _____

_____

_____

_____

แบบฟอร์มการเปลี่ยนแปลง/แก้ไขระบบ (โดยผู้ดูแลระบบ)

(Change Request Form By Admin)

ระบบ _____

วันที่แจ้ง/ตรวจพบ _____ เวลา _____

รายละเอียดการแจ้งปัญหา

หน่วยงานภายใน

ชื่อผู้แจ้ง / ผู้ดูแลระบบ _____

ส่วน _____ ฝ่าย _____

โทร. _____

หน่วยงานภายนอก

ชื่อหน่วยงาน _____

ชื่อผู้แจ้ง / ผู้ดูแลระบบ _____

สถานที่ติดต่อ _____

โทร. _____

สถานที่ปฏิบัติงานแก้ปัญหา _____

แจ้ง ☐ หนังสือ _____ ☐ อื่นๆ _____

ปัญหา/สาเหตุการแก้ไข

_____

_____

_____

รายละเอียดของการปฏิบัติงาน

รายการดำเนินการแก้ไข
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

ลักษณะโครงสร้างของระบบ

ระยะเวลาในการแก้ไข

_____

_____

ระบบที่ได้รับผลกระทบ

_____

_____

_____

_____

_____

ผู้ดำเนินการแก้ไข _____ส่วน _____

ฝ่าย _____ โทร _____

ลงนามผู้ดำเนินการ _____

(_____)

_____/_____/_____

ผู้อนุมัติการแก้ไข _____ส่วน _____

ฝ่าย _____โทร _____

ลงนามผู้อนุมัติ

_____

(_____)

_____/_____/_____

หมวด ๙

การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident Management)

มีจุดประสงค์ เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ สดช. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของ สดช. โดยมีนโยบายดังนี้

นโยบายการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident Management Policy)

๑. วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ สดช. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของ สดช.

๒. การตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่นอกเหนือจากการควบคุมและการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟท์แวร์ (Responding to Security Incidents and Malfunctions)

เพื่อลดความเสียหายจากเหตุการณ์ละเมิดความมั่นคงปลอดภัยและการทำงานของระบบที่บกพร่อง ได้แก่ ไวรัสคอมพิวเตอร์แพร่กระจาย ระบบถูกบุกรุก ภัยคุกคามทางไซเบอร์ เป็นต้น โดยให้ดำเนินการดังนี้

๒.๑. "ผู้ใช้งาน" ต้องรายงานเหตุการณ์ต่าง ๆ ที่เกิดขึ้นให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบโดยเร่งด่วนดังนี้

- รายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events)
- รายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)
- รายงานการทำงานที่บกพร่องหรือทำงานผิดปกติของซอฟต์แวร์ (Reporting Software Malfunctions)

๒.๒. ในกรณีที่ไม่สามารถติดต่อ "ผู้ดูแลระบบ" ได้ในขณะนั้น ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้น และรายงานให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ทราบด้วย

๒.๓. "ผู้ดูแลระบบ" ร่วมกับ "หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ" ต้องประเมินขอบเขต (Scope) และความรุนแรง (Severity) ของปัญหา โดยหากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้าง รุนแรง หรือมีผลต่อชื่อเสียงของ สดช. จะต้องรายงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบโดยด่วน เพื่อหาแนวทางแก้ไขและป้องกันไม่ให้เกิดเหตุการณ์ดังกล่าวในครั้งต่อไป

๒.๔. ในกรณีที่ความเสียหายจากเหตุการณ์ละเมิดความมั่นคงปลอดภัย เกิดขึ้นกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของ สดช. และมีเหตุสงสัยว่าเป็นภัยคุกคามทางไซเบอร์ ให้ดำเนินการตาม ขั้นตอนการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือแผนรับมือภัยคุกคามทางไซเบอร์ ของ สดช.

๓. การบริหารจัดการและการปรับปรุงแก้ไขต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่นอกเหนือจากการควบคุม (Management of Information Security Incidents and Improvements)

เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่นอกเหนือจากการควบคุม ต้องยึดหลักปฏิบัติดังต่อไปนี้

๓.๑. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures) ผู้อำนวยการกองที่มีระบบงานสารสนเทศอยู่ในความดูแล ต้องมีการกำหนดหน้าที่ความรับผิดชอบและกำหนดขั้นตอนปฏิบัติ เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่นอกเหนือจากการควบคุม และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

๓.๒. การเรียนรู้จากสถานการณ์ด้านความมั่นคงปลอดภัยที่นอกเหนือจากการควบคุม (Learning from Security Incidents)

๓.๒.๑. "ผู้ดูแลระบบ" ต้องบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

๓.๒.๒. "ผู้ดูแลระบบ" มีหน้าที่จัดทำสรุปรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัย ให้ผู้บังคับบัญชาและหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ อย่างน้อยเดือนละ ๑ ครั้ง

๓.๒.๓. หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ และหน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง ต้องร่วมกันวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาด ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศทุก ๑๒ เดือน

๓.๓. การเก็บรวบรวมหลักฐาน (Collection of Evidence)

๓.๓.๑. หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่า ได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบองค์กร และกฎหมาย (ระยะเวลา ๙๐ วัน หรือ ๑ ปี เป็นต้น)

๓.๓.๒. หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องศึกษาถึงลักษณะของหลักฐานที่มีความสมบูรณ์และมีคุณภาพ เพื่อสามารถนำไปใช้ในกระบวนการของศาลได้

๔. การรายงานเหตุการณ์น่าสงสัย

๔.๑. "ผู้ใช้งาน" มีหน้าที่รับผิดชอบในการรายงานเหตุการณ์ทันทีที่สงสัยว่าเป็นเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล

๔.๒. ถ้าหากพบเหตุการณ์ที่น่าสงสัยให้ทำการรายงานต่อผู้ดูแลระบบ หรือผู้อำนวยการกองทันที ได้แก่เหตุการณ์ต่อไปนี้

๔.๒.๑. พบว่ารหัสผ่านส่วนบุคคลของตนถูกล็อค โดยไม่ทราบสาเหตุ

๔.๒.๒. เวลาการเข้าใช้งานระบบครั้งล่าสุด (Last Logon Time) ที่ผิดปกติ

๔.๒.๓. พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน ได้แก่ มีไฟล์ที่ไม่รู้จัก การเปลี่ยนแปลงของค่าต่างๆ

๔.๒.๔. มีการไม่ปฏิบัติตามขั้นตอนความมั่นคงปลอดภัย

๔.๒.๕. พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล

๔.๒.๖. พบหรือคาดว่าข้อมูลในระบบจะถูกทำลาย แก้ไข หรือลบทิ้ง

๔.๒.๗. มีความพยายามที่จะเข้าใช้อย่างระบบอย่างผิดวิธี ไม่ว่าจะสำเร็จหรือไม่

๔.๒.๘. การให้บริการของระบบเกิดการชะงัก หรือไม่สามารถให้บริการ

๔.๒.๙. เกิดการละเมิดสิทธิเข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล

๔.๒.๑๐. การแก้ไขค่าความปลอดภัยในระบบได้แก่ Hardware, Software หรือ Firmware โดยผู้ใช้งานไม่ทราบ

Incident Response Report

วันที่ .....

วันที่ตรวจพบ.....เวลา.....

ผู้ตรวจพบ.....ฝ่าย.....

อาการ/สิ่งที่พบ

.....

.....

.....

สาเหตุ

.....

.....

.....

.....

การตรวจสอบแก้ไข

.....

.....

.....

.....

.....

ผลกระทบ

.....

.....

.....

.....

ผลการดำเนินการแก้ไข

.....

.....

.....

วันที่สิ้นสุดการแก้ปัญหา

.....

หมวด ๑๐
การบริหารความต่อเนื่องในการดำเนินงาน
(Government Continuity Management)

มีจุดประสงค์ เพื่อป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมต่างๆ ทางราชการ ป้องกันกระบวนการปฏิบัติราชการที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม โดยมีนโยบายดังนี้

นโยบายแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ
(IT Contingency Plan Policy)

๑. วัตถุประสงค์

ข้อมูลเป็นสินทรัพย์ที่สำคัญที่สุด ต้องจะทำการสำรองข้อมูลและเก็บรักษาข้อมูลของระบบสารสนเทศที่สำคัญต่อการปฏิบัติราชการของ สดช. ไว้ พร้อมทั้งทำการกู้คืนข้อมูล เพื่อให้การปฏิบัติราชการของ สดช. เป็นไปอย่างต่อเนื่อง นโยบายนี้เป็นส่วนหนึ่งของการสนับสนุนแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ และหน่วยงานที่รับผิดชอบระบบและข้อมูลจะต้องปฏิบัติอย่างเคร่งครัด เพื่อทำให้การปฏิบัติราชการของ สดช. เป็นไปอย่างมีประสิทธิภาพ ประสิทธิผล และอย่างต่อเนื่อง

๒. คำแถลงนโยบาย

๒.๑. ขั้นตอนเตรียมการของแผนรองรับเหตุการณ์ฉุกเฉิน

๒.๑.๑. สดช. ต้องจัดตั้งคณะทำงานแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงานเจ้าของข้อมูล เจ้าของระบบงาน หน่วยงานที่ดูแลระบบเครือข่าย เป็นต้น

๒.๑.๒. คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละหนึ่งครั้ง

๒.๑.๓. กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ต้องประกอบด้วยหัวข้อหลัก ดังนี้

- การวิเคราะห์ผลกระทบของปฏิบัติราชการ (Impact Analysis)
- การประเมินความเสี่ยงและการควบคุม (Risk Analysis &Control)
- การวางกลยุทธ์สำหรับแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ (IT Contingency Plan Strategy Development)
- การพัฒนาแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ (IT Contingency Plan Development)
- การประชาสัมพันธ์แผนรองรับเหตุการณ์ฉุกเฉินและการฝึกอบรม
- การทดสอบ ปรับปรุงแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

๒.๑.๔. แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ต้องพิจารณา ดังนี้

- การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการปฏิบัติราชการและการให้บริการของ สดช.
- การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย ได้แก่ กำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
- การดำเนินการเพื่อให้สามารถปฏิบัติราชการได้อย่างต่อเนื่อง ได้แก่ การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
- การกลับคืนสู่การทำงานปกติ เพื่อให้งานของ สดช. กลับสู่สภาวะปกติ ได้แก่ การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

๒.๒. แนวทางปฏิบัติของการสำรองข้อมูลและการกู้คืนข้อมูล

๒.๒.๑. เจ้าของข้อมูลต้องตรวจสอบว่าข้อมูลสำคัญทั้งหมดที่เกี่ยวข้องกับปฏิบัติราชการของ สดช. ได้มีการสำรองข้อมูลอย่างสม่ำเสมอและต่อเนื่องตามแนวทางปฏิบัติของ สดช. เจ้าของข้อมูลแต่ละระบบจึงมีหน้าที่ที่จะต้องประสานงานกับหน่วยงานดูแลข้อมูลที่เกี่ยวข้องเพื่อให้แน่ใจได้ว่าข้อมูลและฐานข้อมูลได้มีการสำรองข้อมูลเอาไว้อย่างครบถ้วนและเตรียมพร้อมเพื่อนำกลับมาใช้เมื่อเกิดเหตุการณ์ฉุกเฉิน

๒.๒.๒. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของสำนักงาน ซึ่งได้จากการวิเคราะห์ผลกระทบเชิงธุรกิจ (Business Impact Analysis: BIA)

๒.๒.๓. หน่วยงานที่รับผิดชอบการสำรองข้อมูล ต้องทำการทดลองนำเอาสื่อที่สำรองข้อมูลไว้มาทดสอบอย่างน้อยปีละครั้ง เพื่อให้มั่นใจได้ว่าสามารถนำข้อมูลกลับมาใช้ได้อีกเมื่อเกิดเหตุการณ์ฉุกเฉิน

๒.๒.๔. การทดสอบการนำข้อมูลกลับมาใช้นั้นให้ใช้ข้อมูลสำรองที่ได้จากของระบบงานจริงและกระทำบนระบบสำหรับการทดสอบเท่านั้น

๒.๓. แนวทางปฏิบัติของการเก็บรักษาข้อมูลและสารสนเทศ

๒.๓.๑. เจ้าของข้อมูลเป็นผู้จัดเก็บรักษาข้อมูลเกี่ยวกับระบบ ซึ่งได้แก่ ข้อมูลเกี่ยวกับระบบปฏิบัติการ (OS) ระบบเครือข่าย และซอฟต์แวร์ระบบงาน (ทั้ง Source Code และ Executable Files) โดยให้เป็นไปตามความต้องการที่เจ้าของข้อมูลในระบบนั้นกำหนด จำนวนครั้งและระยะเวลาในการเก็บรักษาข้อมูลดังกล่าวต้องสอดคล้องกับการประเมินความเสี่ยงของข้อมูลนั้นๆ ด้วย

๒.๓.๒. ก่อนที่จะมีการปรับปรุงหรือเปลี่ยนแปลงระบบ หน่วยงานที่รับผิดชอบต้องทำการสำรองข้อมูลของระบบทุกครั้ง

๒.๓.๓. ถ้าการสำรองข้อมูลถูกดำเนินการที่เซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์หลัก (Host) และเป็นข้อมูลของระบบงานที่สำคัญจะต้องเพิ่มจำนวนครั้งในการสำรองข้อมูลของเซิร์ฟเวอร์นั้นด้วย

๒.๓.๔. ข้อมูลและสารสนเทศที่มีความสำคัญมากต่อการปฏิบัติราชการของ สดช. จะต้องทำการสำรองข้อมูลไว้ทุกวัน และข้อมูลสำรองดังกล่าวต้องมีการจัดเก็บไว้นอก

อาคารที่ตั้งศูนย์คอมพิวเตอร์หลักอย่างเหมาะสม โดยตรวจสอบให้แน่ใจว่าสถานที่นั้นมีความปลอดภัย

๒.๓.๕. ระบบข้อมูลที่สำคัญทั้งหมดของ สดช. ต้องมีระบบการประมวลผลสำรอง ระบบเครือข่ายสำรอง เพื่อป้องกันการพึ่งพาระบบหลักเพียงระบบเดียว ในกรณีที่ระบบหนึ่งไม่สามารถทำงานได้ สามารถใช้งานอีกระบบหนึ่งได้ทันทีเพื่อให้งานหลักของ สดช. ดำเนินต่อไปได้

๒.๓.๖. ข้อมูลและสารสนเทศที่ถูกจัดประเภทเป็นข้อมูลธรรมดา ซึ่งไม่ส่งผลกระทบต่อการดำเนินกิจการของ สดช. จำนวนครั้งในการสำรองข้อมูลนั้นขึ้นอยู่กับการพิจารณาของเจ้าของข้อมูล และข้อมูลดังกล่าวจะถูกนำไปจัดเก็บในสถานที่ๆ มีความปลอดภัย

ตัวอย่างโครงสร้างของแผนกู้คืนระบบสารสนเทศ

โครงสร้างของแผนกู้คืนระบบสารสนเทศนี้จัดทำขึ้นเพื่อให้หน่วยงานใน สดช. ใช้เป็นแนวทางในการจัดทำแผนกู้คืนระบบสารสนเทศที่มีประสิทธิภาพ เพื่อเตรียมรองรับเหตุการณ์และลดผลกระทบต่างๆที่อาจเกิดขึ้น รวมทั้งการฟื้นฟูระบบสารสนเทศของ สดช. ให้กลับคืนสู่สภาพปกติได้ภายในเวลาที่เหมาะสม ซึ่งทำให้ สดช. ดำเนินงานได้อย่างต่อเนื่องหรือได้รับผลกระทบน้อยที่สุดหลังจากเกิดเหตุการณ์หยุดชะงัก หน่วยงานของ สดช. ต้องพิจารณาปรับใช้ให้เหมาะสมกับสถานการณ์ในปัจจุบันด้วย

โดยทั่วไป ตัวอย่างโครงสร้างของแผนกู้คืนระบบสารสนเทศต้องมีเนื้อหาครอบคลุมเรื่องต่าง ๆ ดังนี้

๑. **ชื่อแผนกู้คืนระบบ.....** (ระบุชื่อแผน)

๒. **วัตถุประสงค์ในการจัดทำแผนกู้คืน** ระบุวัตถุประสงค์ของแผน ความเสียงและผลกระทบที่อาจจะเกิดขึ้นต่อ สดช. และหน่วยงานภายนอกที่เกี่ยวข้อง รวมทั้งผลลัพธ์ที่คาดหวังจากการนำแผนดังกล่าวมาใช้

๓. **ขอบเขตของแผนกู้คืน** ระบุขอบเขตของระบบงาน รายละเอียดของกระบวนการทำงาน และส่วนงานที่แผนดังกล่าวมีผลบังคับใช้ รวมทั้งรายละเอียดกระบวนการทำงาน (Work flow)

๔. **รายละเอียดของระบบสารสนเทศ** ระบุชื่อ และโครงสร้างของระบบสารสนเทศ โครงสร้างระบบรักษาความปลอดภัย และการติดต่อสื่อสาร

๕. **การกำหนดผู้รับผิดชอบสั่งการ** ระบุผู้มีอำนาจตัดสินใจ และสั่งการในการนำแผนมาปฏิบัติ โครงสร้างการบังคับบัญชา (ผู้สั่งการ และผู้รับผิดชอบ) บทบาทหน้าที่ และขอบเขตอำนาจความรับผิดชอบ รวมทั้งการกำหนดผู้รับผิดชอบแทนในกรณีที่ผู้สั่งการในลำดับแรกไม่สามารถปฏิบัติงานได้

๖. **สถานที่ปฏิบัติงานทดแทน** ระบุสถานที่ที่ใช้ปฏิบัติงานแทนในกรณีเกิดภัยพิบัติ จนเป็นเหตุให้ไม่สามารถใช้สถานที่ทำงานเดิมได้

๗. **การบันทึกการเปลี่ยนแปลงของแผน** ระบุวันที่ ชื่อผู้จัดทำหรือแก้ไข ชื่อผู้ตรวจทาน และรายละเอียดโดยย่อ เมื่อมีการแก้ไขแผน

๘. **กำหนดแผนการปฏิบัติงาน** ระบุสถานการณ์และเงื่อนไขในการปฏิบัติงานตามแผน รายละเอียดขั้นตอน ทรัพยากรที่ใช้ และข้อจำกัดในการปฏิบัติโดยละเอียด ซึ่งต้องมีแนวปฏิบัติที่ครอบคลุมการวางแผนที่สำคัญ ๔ ด้าน ดังนี้

๘.๑. ***การเตรียมความพร้อมก่อนเกิดเหตุการณ์ความเสียหาย*** การกำหนดกระบวนการป้องกันและควบคุมความเสียง เพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย

๘.๒. ***การตอบสนองต่อเหตุการณ์ฉุกเฉิน*** เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย รวมทั้งผลกระทบอื่น ในขณะที่มีเหตุการณ์ความเสียหายเกิดขึ้น โดยมีกระบวนการดังนี้

๘.๒.๑. *เงื่อนไขการเริ่มปฏิบัติตามแผน* กำหนดหรือระบุเงื่อนไข สถานการณ์

๘.๒.๒. *ระบุขั้นตอนการดำเนินการพื้นฐาน* ประเมินสถานการณ์เบื้องต้น สถานที่ สาเหตุ และขอบเขตความเสียหาย ระบุวิธีการปฏิบัติงานเพื่อระงับเหตุการณ์ความเสียหาย วิธีการดำเนินงานต่างๆ ที่เกี่ยวข้อง แนวทางการเก็บรักษาข้อมูล เอกสาร ความปลอดภัยของผู้ปฏิบัติงาน การเคลื่อนย้ายอพยพ "เจ้าหน้าที" และทรัพยากรทางเทคโนโลยีสารสนเทศที่จำเป็น

๘.๒.๓. *ระบุแผนปฏิบัติการด้านการติดต่อสื่อสาร* กำหนดวิธีการติดต่อสื่อสารและประสานงานกับหน่วยงาน หรือบุคคลอื่นที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อแจ้งสถานการณ์ และแนวทางการดำเนินงาน หรือสถานที่ติดต่องานฉุกเฉิน รวมทั้งจัดทำรายชื่อของหน่วยงาน หรือผู้ที่มีหน้าที่รับผิดชอบในการดำเนินการช่วยเหลือยุติเหตุการณ์ความเสียหายทั้งภายในและภายนอก สดช.

๘.๒.๔. *ระบุความต้องการใช้ทรัพยากรต่างๆ* ระบุความต้องการทรัพยากรที่มีความจำเป็น จำนวนแรงงาน สถานที่ ระบบการสื่อสารโทรคมนาคม สาธารณูปโภค อุปกรณ์ และเครื่องมือต่างๆให้ชัดเจน

๘.๓. ***การดำเนินการเพื่อให้สามารถปฏิบัติราชการได้อย่างต่อเนื่อง*** เป็นแผนปฏิบัติการต่อเนื่องจากแผนในข้อ ๘.๒ เพื่อให้ระบบเทคโนโลยีที่สนับสนุนการดำเนินงานของ สดช. มีความต่อเนื่องไม่หยุดชะงัก หรือสามารถกลับคืนมาในระยะเวลาการกู้คืนที่กำหนด และไม่ก่อให้เกิดผลกระทบต่อเนื่องอื่นๆ โดยมีรายละเอียดดังนี้

๘.๓.๑. *เงื่อนไขการเริ่มปฏิบัติตามแผน* กำหนด หรือระบุเงื่อนไข เหตุการณ์

๘.๓.๒. *ระบุขั้นตอนการดำเนินการพื้นฐาน* กำหนดลำดับขั้นตอน ลำดับความสำคัญและระยะเวลาในการกู้ระบบ ระบุวิธีการปฏิบัติงาน วิธีการนำระบบข้อมูลสำรองมาใช้งาน เพื่อให้เกิดการปฏิบัติงานต่อเนื่องได้โดยทันที

๘.๓.๓. *ระบุแผนปฏิบัติการด้านการติดต่อสื่อสาร* กำหนดวิธีการติดต่อสื่อสารและประสานงานกับหน่วยงาน หรือบุคคลอื่นที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อแจ้งข้อเท็จจริง และแนวทางการดำเนินงาน หรือสถานที่ติดต่องานชั่วคราว

๘.๓.๔. *ระบุความต้องการใช้ทรัพยากรต่างๆ* ระบุความต้องการทรัพยากรที่มีความจำเป็นหากมีการกู้ระบบที่ต้องใช้ระยะเวลานาน จำนวนแรงงาน สถานที่ปฏิบัติงานสำรอง ระบบการสื่อสารโทรคมนาคม สาธารณูปโภค อุปกรณ์และเครื่องมือต่างๆ

๘.๔. ***การกลับคืนสู่การทำงานปกติ*** เพื่อฟื้นฟูและจัดระบบงานให้กลับเข้าสู่การดำเนินงานตามปกติ รวมทั้งการสรุปประเมินความเสียหายที่เกิดขึ้น และแนวทางการป้องกันในอนาคตด้วย โดยมีรายละเอียดดังนี้

๘.๔.๑. *ระบุขั้นตอนการดำเนินการ* ระบุวิธีการปฏิบัติงานเพื่อฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ กระบวนการควบคุมการติดตั้ง การตั้งค่าและทดสอบระบบที่ถูกกู้คืนมาหรือทดแทนใหม่ การรายงานสรุปความเสียหายต่อผู้บังคับบัญชา

๘.๔.๒. *ระบุรายชื่อผู้ที่เกี่ยวข้อง* จัดทำรายชื่อของหน่วยงาน หรือผู้ที่มีหน้าที่รับผิดชอบทั้งจากภายในและภายนอก สดช. ในการดำเนินการช่วยเหลือ เพื่อฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ

๙. การประชาสัมพันธ์แผนรองรับเหตุการณ์ฉุกเฉินและการฝึกอบรม

ระบุขั้นตอนและวิธีการประชาสัมพันธ์ให้แก่ "เจ้าหน้าที่"ของ สดช. และจัดฝึกอบรมให้แก่หน่วยงานและ "เจ้าหน้าที" ผู้มีส่วนเกี่ยวข้อง ให้รับทราบถึงวัตถุประสงค์ ขั้นตอนการปฏิบัติงาน การประสานงาน การติดต่อสื่อสารระหว่างกลุ่ม ขั้นตอนการรายงาน ระบบรักษาความปลอดภัย และหน้าที่ความรับผิดชอบของตนเองตามแผนอย่างชัดเจน

๑๐. การทดสอบ ปรับปรุงและสอบทานแผนฉุกเฉิน

๑๐.๑. การทดสอบ

๑๐.๑.๑. *กำหนดเวลาการทดสอบแผน* กำหนดการทดสอบแผนกู้คืนที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้น จนสิ้นสุดกระบวนการทดสอบ

๑๐.๑.๒. *กำหนดเหตุการณ์จำลองที่จะใช้ทดสอบ และรายละเอียด* ในการกำหนดรายละเอียดของเหตุการณ์จำลอง ต้องระบุวัตถุประสงค์ ขอบเขตของระบบงานหรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผน

๑๐.๑.๓. *กำหนดทรัพยากรต่างๆ ที่ใช้ในการทดสอบแผน* กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุม ประสานงาน และรับผิดชอบในการจัดการทดสอบแผนกู้คืน รวมถึงสถานที่ และอุปกรณ์เครื่องมือต่างๆ และงบประมาณที่ต้องใช้ด้วย

๑๐.๑.๔. *กำหนดเกณฑ์การประเมินผล* กำหนดผู้รับผิดชอบในการประเมินผล เกณฑ์การประเมินผล ซึ่งอาจมีความแตกต่างกันไปตามลักษณะของระบบงาน กระบวนการทำงาน และวัตถุประสงค์ของการทดสอบในแต่ละครั้ง

๑๐.๒. การปรับปรุงและสอบทานแผน

๑๐.๒.๑. *กำหนดเวลาการทบทวนแผน* กำหนดแผนงาน แนวทาง และระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

๑๐.๒.๒. *กำหนดผู้รับผิดชอบในการสอบทาน* ต้องกำหนดผู้สอบทานแผน เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่างๆ ในการจัดทำแผน

๑๑. *รายละเอียดเพิ่มเติม* รายละเอียดอื่นๆ ที่ต้องมีในแผนกู้คืนระบบสารสนเทศ มีดังนี้

๑๑.๑. รายชื่อ ที่อยู่ และหมายเลขโทรศัพท์ของ "เจ้าหน้าที่" ที่มีหน้าที่รับผิดชอบในการปฏิบัติตามแผน

๑๑.๒. รายชื่อหน่วยงาน สถานที่ตั้ง และหมายเลขโทรศัพท์ขององค์กรภายนอกที่เกี่ยวข้อง

๑๑.๓. รายละเอียดการปฏิบัติตามแผน (Checklist)

๑๑.๔. รูปแบบรายงานต่างๆ ที่จำเป็น

หมวด ๑๑
การปฏิบัติตามข้อกำหนด
(Compliance)

มีจุดประสงค์ เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อปฏิบัติราชการน้อยที่สุด โดยมีนโยบายดังนี้

นโยบายการปฏิบัติตามข้อกำหนดทางกฎหมาย
(Compliance with Legal Requirements Policy)

๑. วัตถุประสงค์

เพื่อเป็นแนวทางในการปฏิบัติสำหรับการใช้งานซอฟต์แวร์ของ สดช. และของบุคคลที่สามซึ่งมีการนำมาใช้ภายใน สดช. รวมถึงเรื่องของการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมายและข้อกำหนดในการใช้ซอฟต์แวร์ของผู้ใช้งาน และผู้ที่เกี่ยวข้องกับ สดช.

๒. การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)

หน่วยงานดูแลรับผิดชอบด้านกฎหมาย ต้องระบุข้อกำหนดทางด้านกฎหมาย ระเบียบปฏิบัติและสัญญาว่าจ้าง รวมทั้งสัญญาที่ทำกับหน่วยงานภายนอก ที่เกี่ยวข้องกับการดำเนินงานหรือการปฏิบัติราชการของ สดช. ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

๓. การปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ในการใช้งานสินทรัพย์ทางปัญญา (Compliance with Intellectual property rights (IPR)) มีแนวทางปฏิบัติดังนี้

๓.๑. การจัดซื้อและการนำซอฟต์แวร์ของบุคคลที่สามมาใช้ใน สดช. ต้องเป็นไปตามข้อตกลงเรื่องการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมาย (Licensing Agreement) ที่ได้ทำไว้กับเจ้าของลิขสิทธิ์

๓.๒. ผู้ที่ใช้ซอฟต์แวร์บนระบบสารสนเทศของ สดช. ต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

๓.๓. มีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับ ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ และต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ มีการตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้อง

๓.๔. ซอฟต์แวร์ที่พัฒนาขึ้นโดย/หรือเพื่อ สดช. ถือเป็นสินทรัพย์ของ สดช. ซึ่งครอบคลุมถึงซอฟต์แวร์หรือระบบงานที่พัฒนาโดยบุคคลภายนอกเพื่อให้กับ สดช. ทั้งนี้เพื่อเป็นการป้องกันข้อพิพาทในเรื่องกรรมสิทธิ์ของซอฟต์แวร์ที่อาจเกิดขึ้นหลังจากเสร็จสิ้นโครงการ

๓.๕. ซอฟต์แวร์ที่ถูกพัฒนาโดย "เจ้าหน้าที่ (Officer)" ของ สดช. ในระหว่างเวลาทำงานถือเป็นสินทรัพย์ของ สดช.

๓.๖. เครื่องคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์แบบพกพา และเครื่องเซิร์ฟเวอร์ โดยผู้ใช้งานหรือเจ้าของระบบสารสนเทศ จะต้องตรวจสอบการใช้งานซอฟต์แวร์เป็นประจำว่าได้มีการปฏิบัติตามข้อตกลงเรื่องการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมายซอฟต์แวร์ทั้งหมด

๓.๗. หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศและผู้ดูแลระบบ ต้องคอยตรวจสอบซอฟต์แวร์ ถ้าหากพบว่ามีการละเมิดข้อตกลงจะต้องประสานงานกับเจ้าของระบบสารสนเทศเพื่อทำการยกเลิกการติดตั้งหรือลบทิ้ง

๓.๘. การ Download โปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่างๆจาก Vendor ต้องเป็นไปโดยไม่ละเมิดสินทรัพย์ทางปัญญา

๓.๙. การติดตั้งซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์ระบบงาน (Operating System and Application Software) ต้องกระทำโดยเจ้าหน้าที่ของหน่วยงานที่ได้รับอนุญาตเท่านั้น ถ้ามีการติดตั้งซอฟต์แวร์ใดๆ ในเครื่องคอมพิวเตอร์ของ สดช. โดยไม่ได้รับอนุญาต แล้วเกิดข้อพิพาทเกี่ยวกับกฎหมายลิขสิทธิ์และรายละเอียดข้อบังคับต่างๆ ของผู้ผลิตซอฟต์แวร์นั้นๆ ทาง ***"สดช. จะไม่ขอรับผิดชอบไม่ว่ากรณีใดๆ"***

๓.๑๐. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของ สดช. เป็นโปรแกรมที่ สดช. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๔. การป้องกันข้อมูลสำคัญของ สดช. (Protection of Organizational Records)

เพื่อเป็นการป้องกันข้อมูลสำคัญของ สดช. หน่วยงานต่างๆ ต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ สดช. ได้แก่

- นโยบายความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
- นโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์
- นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
- นโยบายการแลกเปลี่ยนสารสนเทศ
- นโยบายการควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กรเป็นต้น

๕. การป้องกันข้อมูลส่วนตัวและการเข้ารหัส มีแนวทางการปฏิบัติดังนี้

๕.๑. ผู้ดูแลระบบ ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัวของ "เจ้าหน้าที่" ได้แก่ ข้อมูลในจดหมายอิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล เป็นต้น เพื่อใช้เป็นหลักฐานอ้างอิงในทางกฎหมายในกรณีที่มีข้อพิพาทกัน

๕.๒. ผู้ดูแลระบบ ต้องศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายของประเทศ เกี่ยวกับการเข้ารหัสข้อมูล รวมทั้งเมื่อจำเป็นต้องโยกย้ายข้อมูลที่เข้ารหัสไว้ หรืออุปกรณ์ หรือเครื่องมือหรือระบบที่ใช้ในการเข้ารหัสข้อมูลไปยังอีกประเทศหนึ่ง ให้ศึกษาและปฏิบัติตามข้อกำหนด หรือกฎหมายของประเทศนั้นด้วย

๖. การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities) มีแนวทางปฏิบัติดังนี้

๖.๑. อุปกรณ์ประมวลผลสารสนเทศของ สดช. มีไว้เพื่อใช้ในกิจการของ สดช. เท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บริหาร สดช.

๖.๒. อุปกรณ์ประมวลผลสารสนเทศที่ สดช. เช่ามาใช้งาน ต้องกำหนดให้มีหน่วยงานระดับผู้อำนวยการกองขึ้นไปเป็นผู้รับผิดชอบ และหน่วยงานที่เช่า จะต้องจัดทำบัญชีรายการของอุปกรณ์ประมวลผลสารสนเทศที่เช่ามาใช้งาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและสินทรัพย์ของ สดช.

๖.๓. ผู้อำนวยการกองแต่ละหน่วยงาน ต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของ สดช. ได้แก่ Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน โดยต้องปฏิบัติตามระเบียบในการใช้งานการยืม-คืน

๖.๔. ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่างๆ เมื่อมีการเปลี่ยนแปลง เพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของ สดช.

๖.๕. ผู้ใช้งานต้องไม่ทำการแก้ไขเปลี่ยนแปลง หรืออนุญาตให้ผู้ที่ไม่ได้รับอนุญาตทำการแก้ไขเปลี่ยนแปลงโปรแกรมหรืออุปกรณ์ประมวลผลสารสนเทศในเครื่องที่ตนรับผิดชอบ

๖.๖. ไม่อนุญาตให้ผู้ใช้งานติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องของ สดช. การเปลี่ยนแปลงต่อระบบคอมพิวเตอร์ ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูล จะต้องได้รับอนุมัติจากผู้อำนวยการกองที่ดูแลระบบงานนั้นๆ เป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการหยุดชะงักหรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

๖.๗. อุปกรณ์ประมวลผลสารสนเทศจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

๖.๘. อุปกรณ์ประมวลผลสารสนเทศที่ สดช. จัดซื้อ/จัดหา ต้องมีกระบวนการเพื่ออัพเดทระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ของ สดช.

๗. การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of Cryptographic Controls)

หน่วยงานต่างๆ ซึ่งเป็นเจ้าของข้อมูล ต้องใช้มาตรการการเข้ารหัสข้อมูล (Cryptographic controls) ตามที่ได้กำหนดในนโยบายการพัฒนาระบบสารสนเทศ

๘. การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)

ผู้อำนวยการกอง แต่ละหน่วยงาน ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยของ สดช.

๙. การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical compliance checking)

เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคของ สดช. จึงต้องปฏิบัติตามแนวทางดังต่อไปนี้

๙.๑. ผู้ดูแลระบบต้องดูแลรักษา ตรวจสอบแก้ไข และเสนอ สดช. ให้ปรับปรุงระบบสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อให้ระบบสามารถใช้งานได้ดี มีเสถียรภาพ มีความมั่นคงปลอดภัย และมีประสิทธิภาพอยู่เสมอ

๙.๒. ผู้ดูแลระบบต้องขออนุญาตผู้อำนวยการกองในกรณีที่มีการร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ในการประเมิน ตรวจสอบ ทดสอบ หาจุดอ่อน ช่องโหว่ อันเกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศ และทำการแก้ไขอย่างรวดเร็ว

๙.๓. ผู้อำนวยการกองแต่ละหน่วยงาน ต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ตามระยะเวลาที่กำหนดไว้ เพื่อตรวจสอบและแก้ไขปัญหาช่องโหว่ที่เกิดขึ้น

๙.๔. ในกรณีที่มีการเคลื่อนย้าย ผู้ที่รับผิดชอบในการย้ายสถานที่ทำงาน ต้องตรวจสอบความเรียบร้อยครั้งสุดท้ายทันทีหลังจากที่ทำการย้ายของเสร็จสิ้น รวมทั้งตรวจสอบพื้นที่และสินทรัพย์ด้วย การย้ายสถานที่ทำงาน เป็นช่วงเวลาที่ต้องระวังเรื่องการรักษาความปลอดภัยที่อาจมีการมองข้ามได้ โดยเฉพาะช่วงเวลาที่ต้องเร่งจัดการย้ายให้เสร็จสิ้น จึงต้องให้ความระมัดระวัง เพราะอาจมีการผ่อนปรนมาตรการรักษาความปลอดภัยต่อข้อมูลที่มีความสำคัญหรือต่อระบบเครือข่ายของ สดช. ได้

๙.๕. ผู้ใช้งานต้องมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบการ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

๙.๖. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด ได้แก่ การตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส หลีกเลี่ยงในการเปิดไฟล์ที่เป็น Executable file ได้แก่ .EXE, .COM

๙.๗. ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่างๆ ได้แก่ Thump Drive หรือ SDCard ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๙.๘. ต้องมีการตรวจสอบการใช้งานระบบ (Monitoring System Use) อย่างสม่ำเสมอ เพื่อตรวจสอบการใช้งานสินทรัพย์สารสนเทศ โดยต้องมีการประเมินความเสี่ยงและปฏิบัติตามที่กฎหมายกำหนด

๙.๙. การเข้าสู่ระบบของ สดช. จากอินเทอร์เน็ต หรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องตรวจสอบผู้ใช้งานจากสิ่งที่รู้อยู่ ได้แก่ รหัสผ่าน และเพื่อเพิ่มความปลอดภัยการพิสูจน์ตนต้องมีการใช้วิธีการเข้ารหัส (Cryptographic) ร่วมกับการควบคุม

๙.๑๐. ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอก สดช. หน่วยงานที่รับผิดชอบต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิที่ได้รับ และตรวจสอบการใช้งานอย่างสม่ำเสมอ

๑๐. มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)

ผู้อำนวยการกองที่ดูแลระบบงานสำคัญหรือระบบสารสนเทศที่มีข้อมูลความลับของ สดช. ได้แก่ ระบบบริหารทรัพยากรบุคคล ระบบบริหารงบประมาณ ระบบศูนย์ปฏิบัติการของ สดช ฯลฯ เป็นต้น ต้องวางแผนการตรวจประเมินระบบทั้งหมด โดยการตรวจประเมินที่จะดำเนินการ จะต้องมีผลกระทบต่อระบบและกระบวนการดำเนินงานของ สดช. น้อยที่สุด ดังนี้

การประเมินความเสี่ยงด้านสารสนเทศ

(๑) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Risk Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ตรวจสอบ ประเมิน และส่งผลการตรวจประเมินความเสี่ยงที่ดาเนินการโดย ผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal Auditor)

แนวทางในการบริหารจัดการความเสี่ยงที่ต้องพิจารณา

(๑) ต้องจัดทารายงานในการบริหารจัดการความเสี่ยงพร้อมข้อเสนอแนะ

(๒) ต้องทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

(๓) ต้องทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๑๑ การป้องกันเครื่องมือสำหรับ