ประกาศสำนักงานปลัดกระทรวงพลังงาน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานปลัดกระทรวงพลังงาน

เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงพลังงานเป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม และตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และที่แก้ไขเพิ่มเติม กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ สำนักงานปลัดกระทรวงพลังงาน จึงออกประกาศดังต่อไปนี้

ข้อ ๑ สำนักงานปลัดกระทรวงพลังงานได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงพลังงาน ดังนี้

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

รายละเอียดตามเอกสารแนบท้ายประกาศ

ข้อ ๒ ให้ข้าราชการ พนักงานราชการ ลูกจ้าง ผู้ปฏิบัติงานภายในสำนักงานปลัดกระทรวงพลังงานและผู้ที่มาติดต่อราชการ ณ สำนักงานปลัดกระทรวงพลังงาน ต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงพลังงานโดยเคร่งครัด

ข้อ ๓ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้มีความทันสมัยเป็นปัจจุบัน และเป็นมาตรฐานที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๔ ตุลาคม พ.ศ. ๒๕๖๓

(นายกุลิศ สมบัติศิริ)
ปลัดกระทรวงพลังงาน

เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานปลัดกระทรวงพลังงาน

กระทรวงพลังงาน
MINISTRY OF ENERGY

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานปลัดกระทรวงพลังงาน

ปีงบประมาณ **2564**

คณะทำงานจัดทำแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานปลัดกระทรวงพลังงาน

คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ให้มีความมั่นคงปลอดภัยและเชื่อถือได้ และในมาตรา ๗ กำหนดให้หน่วยงานของรัฐจัดทำเป็นประกาศ เพื่อตระหนักถึงความสำคัญของการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและการสื่อสารขององค์การ

ตามประกาศคณะกรรมธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล จึงเห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

ตามที่ สป.พน. ได้มีคำสั่งที่ ๕๕/๒๕๖๓ สั่ง ณ วันที่ ๒๖ มีนาคม ๒๕๖๓ แต่งตั้งคณะทำงานจัดทำแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓ สำนักงานปลัดกระทรวงพลังงาน โดยมีอำนาจหน้าที่ ตามข้อ ๒.๓ นำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของสำนักงานปลัดกระทรวงพลังงาน ไปจัดทำแผนการประเมินความเสี่ยงและจัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติต่อระบบสารสนเทศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานปลัดกระทรวงพลังงาน เป็นเอกสารที่จัดทำขึ้นเพื่อเป็นเครื่องมือหนึ่งที่ช่วยให้การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยที่การดำเนินงานดังกล่าว จะเป็นมาตรการหนึ่งที่ช่วยยกระดับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงพลังงาน ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงการดำเนินงานตามกรอบมาตรฐานสากล ISO/IEC 27001 ภายใต้แนวทางที่เป็นมาตรฐานขั้นต่ำซึ่งเพียงพอต่อการดำเนินงาน

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจะช่วยให้สำนักงานปลัดกระทรวงพลังงานลดผลกระทบจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ซึ่งอาจทำให้ระบบสารสนเทศขององค์กรถูกทำลาย บุกรุกหรือถูกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม ตลอดจนช่วยให้สามารถฟื้นฟูระบบสารสนเทศได้อย่างรวดเร็ว

ทั้งนี้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หวังเป็นอย่างยิ่งว่า นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานปลัดกระทรวงพลังงาน ซึ่งมีความสำคัญเป็นอย่างยิ่งในการบริหารจัดการ และแก้ไขปัญหาความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร อีกทั้งยังมีความสำคัญต่อการพัฒนาศักยภาพของระบบรักษาความมั่นคงปลอดภัยของข้อมูล ส่งผลให้เกิดประโยชน์สูงสุดโดยตรงต่อนโยบายและจุดประสงค์หลักด้านเทคโนโลยีสารสนเทศขององค์การ

คณะทำงานจัดทำแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓
สำนักงานปลัดกระทรวงพลังงาน

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

คำนิยาม

สป.พน.	หมายถึง	สำนักงานปลัดกระทรวงพลังงาน
ผู้บริหารระดับสูง	หมายถึง	ผู้บริหารระดับสูง ได้แก่ ปลัดกระทรวงพลังงาน รองปลัดกระทรวงพลังงาน ผู้ช่วยปลัดกระทรวงพลังงาน ผู้ตรวจราชการพลังงาน เป็นต้น
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง	หมายถึง	ผู้มีอำนาจสูงสุดในด้านระบบสารสนเทศของ สป.พน. มีบทบาทหน้าที่ในการกำหนดนโยบายและมาตรฐานเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ การวางแผนแม่บทและการติดตามการพัฒนาระบบสารสนเทศ การกำกับดูแลการปฏิบัติงานสารสนเทศ การประเมินและตรวจสอบคุณภาพของงานสารสนเทศ และการรายงานผลการปฏิบัติงานสารสนเทศแก่ผู้บริหารระดับสูง
ผู้อำนวยการ	หมายถึง	ผู้อำนวยการกอง/สำนัก/ศูนย์
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ผอ.ศทส.)	หมายถึง	ผู้มีอำนาจในด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พน. ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
ผู้บังคับบัญชา	หมายถึง	ผู้มีอำนาจสั่งการตามโครงสร้างของ สป.พน.
หัวหน้ากลุ่ม	หมายถึง	หัวหน้ากลุ่มงาน/ฝ่าย
ผู้ดูแลศูนย์ข้อมูล	หมายถึง	เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร
ผู้ดูแลระบบ	หมายถึง	เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

เจ้าหน้าที่	หมายถึง	ข้าราชการ พนักงานราชการ เอกชนที่จ้างมาดำเนินงาน และเจ้าหน้าที่ประจำโครงการของ สป.พน.
ผู้ใช้งาน	หมายถึง	บุคคลที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของ สป.พน. โดยมีสิทธิและหน้าที่ตามที่ สป.พน. ได้กำหนดไว้
เจ้าของระบบงาน	หมายถึง	ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลและพัฒนาระบบของ สป.พน.
เจ้าของข้อมูลและสารสนเทศ	หมายถึง	ผู้ที่เป็นผู้สร้างข้อมูลและสารสนเทศ
สิทธิของผู้ใช้งาน	หมายถึง	สิทธิที่เกี่ยวข้องกับระบบสารสนเทศของ สป.พน.
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)	หมายถึง	หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายสารสนเทศภายใน สป.พน.
บุคคลภายนอก	หมายถึง	บุคคลที่ไม่ใช่ข้าราชการและเจ้าหน้าที่ของ สป.พน. ซึ่ง สป.พน. อนุญาตให้มีสิทธิในการเข้าถึงและใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของ สป.พน. โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่ ภายใต้สัญญา/ข้อตกลง และต้องรับผิดชอบในการรักษาความลับของข้อมูล
ศูนย์ข้อมูล	หมายถึง	ห้องเซิร์ฟเวอร์ ห้องเก็บอุปกรณ์ ภายใน ชั้น ๓ ศูนย์เอนเนอร์ยี่คอมแพล็กซ์ อาคารบี
หน่วยงานดูแลรับผิดชอบด้านตรวจสอบภายใน	หมายถึง	หน่วยงานของ สป.พน. ที่มีหน้าที่รับผิดชอบในการสอบทานให้ดำเนินไปภายใต้มาตรฐานและแนวทางการปฏิบัติที่ได้กำหนดไว้ในนโยบายความมั่นคงปลอดภัยสารสนเทศของ สป.พน.
หน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร	หมายถึง	หน่วยงานของ สป.พน. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการจัดการประชุม สัมมนา หรืออบรมให้ความรู้แก่บุคลากรใหม่และผู้ใช้งาน เกี่ยวกับวิธีปฏิบัติงานเพื่อสร้างความมั่นคงปลอดภัยให้กับสารสนเทศของ สป.พน.

หน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง	หมายถึง	หน่วยงานของ สป.พน. ที่มีหน้าที่รับผิดชอบในการวิเคราะห์และประเมินความเสี่ยงระบบสารสนเทศของ สป.พน. ที่เกี่ยวกับการบริหารงานราชการเพื่อให้ สป.พน. มีคุณภาพ มีประสิทธิภาพในการปฏิบัติราชการมากยิ่งขึ้น และลดโอกาสที่จะเกิดความเสียหายได้
หน่วยงานดูแลรับผิดชอบด้านกฎหมาย	หมายถึง	หน่วยงานของ สป.พน. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการดำเนินการยกร่างกฎหมาย พิจารณา และให้คำปรึกษาตอบข้อหารือที่เกี่ยวกับกฎหมาย ระเบียบ คำสั่ง บันทึกสั่งการ ดำเนินการเกี่ยวกับนิติกรรมของ สป.พน. ดำเนินการบอกกล่าว ทวงถาม รวบรวมพยานหลักฐานเพื่อดำเนินคดี ดำเนินการสอบสวนข้อเท็จจริงและหาผู้รับผิดทางแพ่ง ให้คำปรึกษาทางกฎหมายแก่ เจ้าหน้าที่ ของ สป.พน. ตลอดจนประสานงานกับหน่วยงานต่าง ๆ ในเรื่องที่เกี่ยวข้อง
หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	หมายถึง	หน่วยงานของ สป.พน. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการกำหนดนโยบายและแนวทางปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ ติดต่อประสานงานความร่วมมือทางด้านความมั่นคงปลอดภัยระหว่างองค์กร วางแผนควบคุมระบบความมั่นคงปลอดภัยสารสนเทศและการเตือนภัย รวมถึงการวิเคราะห์หาวิธีการแก้ไขช่องโหว่ของระบบสารสนเทศ และรายงานเกี่ยวกับการฝ่าฝืนนโยบายดังกล่าวไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง
หน่วยงานดูแลรับผิดชอบการบริหารงานบุคคลและสวัสดิการ	หมายถึง	หน่วยงานของ สป.พน. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการสรรหา เจ้าหน้าที่ ใหม่ การตรวจสอบคุณสมบัติของผู้สมัคร การกำหนดเงื่อนไขการจ้างงาน การลงนามมิให้เปิดเผยความลับของ สป.พน.
หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่	หมายถึง	หน่วยงานของ สป.พน. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ควบคุมการเข้า-ออกอาคารและสำนักงาน จัดเตรียมการป้องกันต่อภัยคุกคามต่าง ๆ ทั้งจากมนุษย์และธรรมชาติ เช่น ไฟไหม้ น้ำท่วม และแผ่นดินไหว เป็นต้น

หน่วยงานภายนอก	หมายถึง	องค์กรซึ่ง สป.พน. อนุญาตให้มีสิทธิในการเข้าถึงและใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของ สป.พน. ภายใต้สัญญา/ข้อตกลง โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล
ทรัพย์สิน	หมายถึง	ทรัพย์สินที่จับต้องได้และหมายรวมไปถึงข้อมูลและระบบสารสนเทศอื่น ๆ ของ สป.พน. เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
ข้อมูลคอมพิวเตอร์	หมายถึง	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
สารสนเทศ	หมายถึง	ข้อเท็จจริงที่ได้จากการนำข้อมูลคอมพิวเตอร์มาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบ ที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
ระบบเทคโนโลยีสารสนเทศ	หมายถึง	ระบบงานของ สป.พน. ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่ สป.พน. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร
ระบบคอมพิวเตอร์	หมายถึง	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
อินเทอร์เน็ต	หมายถึง	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของ สป.พน. เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเครือข่าย	หมายถึง	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ สป.พน. เช่น ระบบ LAN อินทราเน็ตและอินเทอร์เน็ต เป็นต้น
ระบบ LAN และ อินทราเน็ต	หมายถึง	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานของสป.พน. เข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
จดหมายอิเล็กทรอนิกส์	หมายถึง	ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง
แชร์แวร์	หมายถึง	โปรแกรมที่ผู้ผลิตหรือผู้ที่ได้ลิขสิทธิ์โปรแกรมนั้น ๆ ยินยอมให้สามารถทดลองใช้โปรแกรม ซึ่งอาจจะใช้งานได้ครบตามความสามารถทั้งหมดของโปรแกรมหรือเพียงบางส่วน แต่มีกำหนดระยะเวลาหรือจำนวนการใช้งาน เมื่อครบตามที่ได้ตกลงกันไว้จะไม่สามารถใช้โปรแกรมต่อได้ ต้องสั่งซื้อโปรแกรมจากผู้ผลิตเพื่อใช้งานต่อไป
ฟรีแวร์	หมายถึง	โปรแกรมที่ผู้ผลิตหรือผู้ที่ได้ลิขสิทธิ์โปรแกรมนั้น ๆ ยินยอมให้มีการคัดลอก และนำไปใช้ได้โดยไม่คิดค่าใช้จ่าย
ซอฟต์แวร์ยูทิลิตี้	หมายถึง	เป็นโปรแกรมประเภทหนึ่งที่ถูกนำมาใช้เพื่อสนับสนุนและเพิ่มเติมขีดความสามารถของโปรแกรมที่ใช้งานอยู่ ให้เกิดประสิทธิภาพสูงยิ่งขึ้น เช่น WinRAR Recuva CPU-Z เป็นต้น
ซอฟต์แวร์ต้นฉบับ	หมายถึง	ชุดข้อความที่ถูกเขียนขึ้น สามารถอ่านและเข้าใจได้โดยใช้ภาษาในการเขียนโปรแกรม ได้แก่ C++, PHP, Python เป็นต้น ในการเขียนโปรแกรมรูปแบบใหม่ Source Code นิยมเก็บไว้ในไฟล์หลายไฟล์แยกจากกัน เพื่อให้ง่ายในการเรียกใช้ส่วนย่อยของคำสั่งนั้น

ซอฟต์แวร์ประสงค์ร้าย	หมายถึง	ซอฟต์ที่มีจุดประสงค์ร้ายต่อระบบเครือข่ายและคอมพิวเตอร์ซึ่งประกอบไปด้วยซอฟต์แวร์ประสงค์ร้าย (Malware) (Virus) เวิร์ม (Worm) โทรจันทร์ฮอร์ส สปายแวร์ (Spyware) แรนซัมแวร์ (Ransomware) และซอฟต์อันตรายอื่น ๆ
มาตรฐาน	หมายถึง	บรรทัดฐานที่บังคับใช้ในการปฏิบัติจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย เช่น การกำหนดรหัสผ่านต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร เป็นต้น
วิธีการปฏิบัติ	หมายถึง	รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
แนวทางปฏิบัติ	หมายถึง	แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
การรักษาความมั่นคงปลอดภัย	หมายถึง	การรักษาความมั่นคงปลอดภัยสำหรับการติดตั้งและการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
ความมั่นคงปลอดภัยสารสนเทศ	หมายถึง	การธำรงไว้ ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)
การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	หมายถึง	การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตหน่วยงานภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบไว้ด้วย
ที่อยู่จดหมายอิเล็กทรอนิกส์	หมายถึง	ชุดอักขระที่ระบุเฉพาะเจาะจงถึงตำแหน่งที่อยู่ของตู้ไปรษณีย์ของผู้ที่ใช้จดหมายอิเล็กทรอนิกส์ ซึ่งจะประกอบด้วยชื่อของบุคคล เช่น Ploy และตามด้วยสัญลักษณ์ @ และชื่อของโดเมน (Domain Name) เช่น ict@enregy.go.th

รหัสผ่าน	หมายถึง	เครื่องมือรักษาความปลอดภัยที่ประกอบด้วยชุดของตัวอักษร ซึ่งใช้ตรวจสอบสิทธิในการเข้าถึงระบบแก่ผู้ใช้งานแต่ละคน เพื่อแสดงรับรองความถูกต้องแท้จริง (Authentication) ของผู้ใช้งาน
ชุดคำสั่งไม่พึงประสงค์	หมายถึง	ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
ช่องโหว่	หมายถึง	ความอ่อนแอในระบบซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้
ความเสี่ยง	หมายถึง	โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ ที่ไม่พึงประสงค์ที่ทำให้ระบบสารสนเทศไม่สามารถทำงานได้ตามวัตถุประสงค์
การเข้ารหัสข้อมูล	หมายถึง	การนำข้อมูลผ่านกระบวนการเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้ต้องมีกระบวนการถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
การบริหารจัดการเปลี่ยนแปลง	หมายถึง	การเปลี่ยนแปลงระบบสารสนเทศ หรือระบบงานทางราชการ ซึ่งการเปลี่ยนแปลงดังกล่าวจะมีผลกระทบต่อฮาร์ดแวร์ ซอฟต์แวร์ระบบ (System Software) โปรแกรมประยุกต์ (Application Software) และระบบเครือข่าย เป็นต้น
เหตุการณ์ด้านความมั่นคงปลอดภัย	หมายถึง	กรณีที่เกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย เช่น การเข้าถึงระบบโดยมิชอบ เพื่อทำการแก้ไข เปลี่ยนแปลง หรือทำลายข้อมูลในระบบ เป็นต้น

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	หมายถึง	สถานการณ์ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม ได้แก่ การโจมตีแบบ DDoS เป็นต้น
ข้อมูลและสารสนเทศที่กำหนดชั้นความลับ	หมายถึง	ข้อมูลและสารสนเทศที่มีความสำคัญ ซึ่งได้กำหนดชั้นความลับตาม ระเบียบ ว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

หมวด ๑
นโยบายความมั่นคงปลอดภัย
(Security Policy)

๑. คำแถลงนโยบาย

สำนักงานปลัดกระทรวงพลังงาน (สป.พน.) จัดทำนโยบายนี้เพื่อเป็นส่วนหนึ่งของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ในการป้องกันภัยคุกคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้สารสนเทศมีความปลอดภัย สามารถรักษาความลับและความถูกต้องของข้อมูล และมีความพร้อมในการให้บริการอยู่ในระดับที่ยอมรับได้ สป.พน. จึงได้กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นแนวทางเสริมสร้างความมั่นคงปลอดภัยสารสนเทศให้กับ สป.พน. หรือหน่วยงานที่มีความเกี่ยวข้องในการปฏิบัติราชการกับ สป.พน. โดยนโยบายนี้มีจุดประสงค์เพื่อการสนับสนุนการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของ สป.พน.

นโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศของ สป.พน. ใช้แนวทางและกระบวนการโดยมีความสอดคล้องตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ มีความมั่นคงปลอดภัย เชื่อถือได้ รวมถึงยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่น ๆ ที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม(ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ซึ่งประกอบด้วย ๑๔ หมวด ตามแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ ในการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจนการคุกคามจากภัยต่าง ๆ ด้วย ที่ครอบคลุมถึงประเด็นสำคัญ ดังนี้

- การรักษาความลับ (Confidentiality) คือ มีการรับรองว่าข้อมูลที่จัดเก็บจะได้รับการคุ้มครองไว้เป็นความลับ ผู้มีสิทธิเท่านั้นที่จะเข้าถึงข้อมูลนั้นได้ และไม่ถูกเปิดเผยสู่บุคคลหรือหน่วยงานอื่นที่ไม่มีสิทธิ
- การรักษาความสมบูรณ์ (Integrity) คือ มีการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา ข้อมูลจะคงอยู่อย่างถูกต้อง และสมบูรณ์ในทุกขั้นตอน
- การพร้อมใช้ (Availability) คือ มีการรับรองว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้
- การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) คือ มีวิธีการสื่อสารที่แสดงข้อความแจ้งผู้ส่งข้อมูลเป็นหลักฐานว่า ได้มีการส่งข้อมูลแล้วและผู้รับได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้น ทั้งผู้รับและผู้ส่งจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

๒. วัตถุประสงค์ของนโยบาย

สป.พน. ได้กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศโดยมีวัตถุประสงค์เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศของ สป.พน. ทำให้การปฏิบัติราชการมีประสิทธิภาพและประสิทธิผล ดังต่อไปนี้

- เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับใน สป.พน.ได้รับทราบ และทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- เพื่อให้มีการดำเนินการที่เหมาะสมและสัมฤทธิผล มีการตรวจสอบ ประเมิน และทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง
- เพื่อสร้างความตระหนักให้ เจ้าหน้าที่ และ หน่วยงานภายนอก ที่ปฏิบัติงานให้กับ สป.พน. ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศ
- เพื่อดำเนินการหรือประสานงานกับหน่วยงานอื่น ๆ ในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงปลอดภัย ที่เป็นประโยชน์ต่อการทำงานหรือการพัฒนาบุคลากรที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

๓. องค์ประกอบของนโยบาย

นโยบายความมั่นคงปลอดภัยสารสนเทศได้กำหนดองค์ประกอบที่สำคัญของการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย โดยครอบคลุมทั้งด้านการควบคุมการเข้าถึง การกำหนดขั้นตอนและกระบวนการที่เหมาะสม ตามหลักมาตรฐานสากล ซึ่งมีองค์ประกอบ ๑๔ หมวด ดังนี้

หมวด ๑ นโยบายความมั่นคงปลอดภัย (Security Policy) นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับการใช้งานระบบสารสนเทศของ สป.พน. เพื่อให้สอดคล้องกับข้อกำหนดทางราชการ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งจัดทำเป็นลายลักษณ์อักษร โดยที่ฝ่ายบริหารเห็นชอบและอนุมัติ และเผยแพร่ให้เจ้าหน้าที่ทุกระดับได้รับรู้ มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สป.พน. ตามระยะเวลาที่กำหนด พร้อมทั้งปรับเปลี่ยนนโยบายตามความเหมาะสม

หมวด ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security) นโยบายนี้มีวัตถุประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์สารสนเทศของ สป.พน. ที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับบุคคลหรือหน่วยงานภายนอก โดยจัดให้มีคณะทำงานและบุคลากรเฉพาะด้านความมั่นคงปลอดภัย มีการประสานงานความรับผิดชอบ ประเมินความเสี่ยง และตรวจสอบการทำงานด้านความมั่นคงปลอดภัย รวมทั้งประสานงานกับหน่วยงานภายนอกและผู้ใช้งานสารสนเทศจากภายนอก โดยมีการระบุและจัดทำข้อกำหนดที่ชัดเจนในการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สป.พน.

หมวด ๓ ความมั่นคงปลอดภัยทางด้านทรัพยากรบุคคล (Human Resource Security) นโยบายนี้มีวัตถุประสงค์เพื่อให้ เจ้าหน้าที่ บุคคลภายนอก และ หน่วยงานภายนอก เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตน ทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และการสิ้นสุดหรือการเปลี่ยนการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

หมวด ๔ การบริหารจัดการทรัพย์สิน (Asset Management) นโยบายนี้มีวัตถุประสงค์เพื่อป้องกันทรัพย์สินของ สป.พน. จากความเสียหายที่อาจเกิดขึ้น และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสม โดยมีการจัดทำบัญชีทรัพย์สิน ระบุผู้เป็นเจ้าของทรัพย์สิน และกำหนดหลักเกณฑ์การใช้งานทรัพย์สินที่เหมาะสม มีการจัดหมวดหมู่ทรัพย์สินตามระดับชั้นความลับ และจัดทำป้ายชื่อ เพื่อการบริหารจัดการทรัพย์สินตามที่ได้จัดหมวดหมู่ไว้

หมวด ๕ การควบคุมการเข้าถึง (Access Control) นโยบายนี้มีวัตถุประสงค์เพื่อกำหนด และจัดทำแนวปฏิบัติตลอดจนกระบวนการในการควบคุมการเข้าใช้งานระบบเครือข่ายและบริการบนเครือข่ายตามความต้องการในการปฏิบัติราชการ โดยการกำหนดการบริหารจัดการและการใช้งานสารสนเทศของผู้ใช้งาน รวมถึงการลงทะเบียนผู้ใช้งาน การบริหารจัดการสิทธิในการใช้ระบบการบริหารจัดการข้อมูลและสารสนเทศที่กำหนดชั้นความลับในการพิสูจน์ตัวตนของผู้ใช้งาน การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานในการปฏิบัติตามวิธีปฏิบัติขององค์กร กำหนดระเบียบปฏิบัติงานเรื่องการเข้าถึงระบบ (Login) อย่างปลอดภัย การกำหนดระบบบริหารจัดการรหัสผ่านการใช้ซอฟต์แวร์อรรถประโยชน์ (Utility Program) และการควบคุมการเข้าถึงซอฟต์แวร์ต้นฉบับ (Source Code)

หมวด ๖ การเข้ารหัสข้อมูล (Cryptography) นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดให้มีการเข้ารหัสอย่างเหมาะสมและมีประสิทธิภาพ เพื่อป้องกันการเปิดเผยความลับของข้อมูล การปลอมแปลงข้อมูล และรักษาไว้ซึ่งความสมบูรณ์ถูกต้องของข้อมูล โดยมีการกำหนดแนวปฏิบัติและมาตรการการเข้ารหัสข้อมูล รวมถึงการบริหารจัดการกุญแจรหัสข้อมูล (Cryptography key)

หมวด ๗ ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) นโยบายนี้มีวัตถุประสงค์เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ป้องกันทรัพย์สินไม่ให้เกิดการสูญหาย ถูกขโมย เกิดความเสียหาย เกิดการก่อกวนหรือแทรกแซง ป้องกันการถูกเปิดเผยโดยไม่ได้รับอนุญาต และป้องกันไม่ให้กิจกรรมการดำเนินงานต่าง ๆ ของ สป.พน. เกิดการติดขัดหรือหยุดชะงัก เช่น การมีระบบกระแสไฟฟ้าสำรองและการมีระบบสื่อสารสำรอง เป็นต้น

หมวด ๘ ความมั่นคงปลอดภัยในการปฏิบัติงาน (Operations Security) นโยบายนี้มีวัตถุประสงค์เพื่อให้การดำเนินงานของอุปกรณ์ที่เกี่ยวข้องเป็นไปอย่างถูกต้องปลอดภัย จึงจัดทำขั้นตอนการปฏิบัติงาน และกำหนดหน้าที่ความรับผิดชอบอย่างชัดเจน สำหรับการป้องกันโปรแกรมที่ไม่ประสงค์ดี โปรแกรมที่ไม่อนุญาต การสำรองข้อมูล การเก็บข้อมูลประวัติการเข้าใช้งานระบบ (Log File) การเฝ้าระวังการควบคุมการติดตั้งซอฟต์แวร์ รวมถึงการบริหารจัดการช่องโหว่

หมวด ๙ ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security) นโยบายนี้ มีวัตถุประสงค์เพื่อสร้างความมั่นคงปลอดภัยข้อมูลและสารสนเทศบนระบบเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ โดยมีการกำหนดการบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย และการถ่ายโอนข้อมูลและสารสนเทศ รวมถึงข้อกำหนดในการรักษาความลับ หรือการไม่เปิดเผยความลับ ซึ่งมีผลบังคับใช้กับเจ้าหน้าที่ขององค์กร รวมถึงบุคคลภายนอก

หมวด ๑๐ การจัดหาพัฒนา และบำรุงรักษาระบบ (Information System Acquisition Development and Maintenance) นโยบายนี้มีวัตถุประสงค์เพื่อให้เจ้าของข้อมูลและสารสนเทศที่ดำเนินการจัดหา จัดจ้าง พัฒนา และบำรุงรักษา ต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่สำคัญขององค์กร โดยพิจารณาทุกขั้นตอนและครอบคลุมถึงระบบที่ใช้ในการพัฒนา ทดสอบ รวมทั้งข้อมูลที่ใช้ในการทดสอบ

หมวด ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships) นโยบายนี้มีวัตถุประสงค์เพื่อป้องกันการเข้าถึงทรัพย์สินขององค์กรจากผู้ให้บริการภายนอก โดยกำหนดแนวทางปฏิบัติการบริหารจัดการ และทำข้อตกลงเป็นลายลักษณ์อักษรกับผู้ให้บริการภายนอกในการเข้าถึงทรัพย์สินขององค์กร

หมวด ๑๒ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information Security Incident Management) นโยบายนี้มีวัตถุประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ สป.พน. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศของ สป.พน.

หมวด ๑๓ ความมั่นคงปลอดภัยด้านการบริหารความต่อเนื่องในการดำเนินงาน (Information Security of Business Continuity Management) นโยบายนี้มีวัตถุประสงค์เพื่อวางแผน จัดทำคู่มือสำหรับนำไปปฏิบัติ บำรุงรักษา ตรวจสอบ ควบคุม และประเมินผลความต่อเนื่องด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ให้มั่นใจว่าระดับความมั่นคงปลอดภัยอยู่ในเกณฑ์ที่ยอมรับได้ในกรณีที่เกิดเหตุการณ์ไม่พึงประสงค์ รวมถึงมีการเตรียมระบบที่สามารถสร้างความต่อเนื่องของระบบเทคโนโลยีสารสนเทศให้พร้อมใช้งานอยู่เสมอ

หมวด ๑๔ การปฏิบัติตามข้อกำหนด (Compliance) นโยบายนี้มีวัตถุประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อการปฏิบัติราชการน้อยที่สุด

นโยบายความมั่นคงปลอดภัยสารสนเทศแต่ละหมวดที่กล่าวมาข้างต้นประกอบด้วย วัตถุประสงค์ในการดำเนินการที่เกี่ยวข้องในหมวดนั้น ๆ มีรายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และวิธีปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อลดความเสียหายต่อการปฏิบัติงาน เป็นหน่วยงานที่ได้รับการยอมรับจากองค์กรต่าง ๆ ในการปฏิบัติราชการได้อย่างมั่นคงปลอดภัยตามมาตรฐานสากล ซึ่งนโยบายความมั่นคงปลอดภัยสารสนเทศนี้ถือเป็นมาตรฐานด้านความมั่นคงปลอดภัย ซึ่งเจ้าหน้าที่ทุกระดับ บุคคลภายนอก และหน่วยงานภายนอกที่เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรต้องรับทราบ มีความเข้าใจ และสามารถปฏิบัติตามแนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศได้อย่างเคร่งครัด

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดการเสียหาย หรือได้รับอันตรายใด ๆ อันเป็นการสร้างความเสียหายแก่องค์กรหรือผู้หนึ่งผู้ใด เนื่องมาจากความบกพร่อง การละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ ผู้บริหารระดับสูงสุดต้องเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น และกำหนดให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ รวมถึงกำหนดให้มีการปฏิบัติที่ชัดเจนและมีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง

หมวด ๒
โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร
(Organization of Information Security)

จุดประสงค์ เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สป.พน. ที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับบุคคลภายนอกหรือหน่วยงานภายนอก โดยจัดให้มีคณะทำงานและบุคลากรเฉพาะด้านความมั่นคงปลอดภัย มีการประสานงานความรับผิดชอบ ประเมินความเสี่ยง และตรวจสอบการทำงานด้านความมั่นคงปลอดภัย รวมทั้งประสานงานกับหน่วยงานภายนอกและผู้ใช้งานสารสนเทศจากภายนอก โดยมีการระบุและจัดทำข้อกำหนดที่ชัดเจนในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สป.พน. โดยประกอบด้วย

- **การกำหนดสิทธิ หน้าที่ และความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ**
- **การควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับหน่วยงานภายนอก**
- **การควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับผู้ปฏิบัติงานชั่วคราว**

การกำหนดสิทธิ หน้าที่ และความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

นโยบายนี้ระบุถึงสิทธิของผู้ใช้งาน หน้าที่ และความรับผิดชอบของบุคคล หน่วยงานที่มีส่วนเกี่ยวข้องในการใช้งาน การดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ สป.พน. เพื่อเป็นการปกป้องทรัพย์สินของ สป.พน. ให้มีความมั่นคงปลอดภัย นโยบายนี้มีผลกับผู้ใช้งานที่มีส่วนเกี่ยวข้องกับ สป.พน. ทั้งหมด

๒. สิทธิ หน้าที่ และความรับผิดชอบ

๒.๑ ผู้บริหารระดับสูง

๒.๑.๑ ปลัดกระทรวงพลังงาน ในฐานะผู้บริหารสูงสุดของกระทรวงพลังงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงพลังงาน

๒.๑.๒ สามารถกำหนดชั้นความลับทุกชั้นความลับ สำหรับข้อมูลและสารสนเทศที่กำหนดชั้นความลับของ สป.พน.

๒.๑.๓ สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับ

๒.๑.๔ สามารถสั่งการ อนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับ

๒.๑.๕ สามารถมอบอำนาจเป็นลายลักษณ์อักษรให้ผู้ใต้บังคับบัญชามีสิทธิในการสั่งการ อนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับ

๒.๑.๖ สามารถแต่งตั้งให้เจ้าหน้าที่ของ สป.พน. ทำหน้าที่เป็นผู้ดูแลระบบสำหรับงานระบบสารสนเทศ

๒.๑.๗ สามารถอนุญาตให้หน่วยงานภายนอกเข้ามาปฏิบัติงานกับระบบสารสนเทศของ สป.พน.

๒.๑.๘ สามารถกำหนดและจำแนกพื้นที่ใช้งานระบบสารสนเทศของ สป.พน.

๒.๑.๙ สามารถกำหนดสิทธิของผู้ใช้งานในการผ่านเข้าออกพื้นที่ใช้งานระบบสารสนเทศของ สป.พน. และต้องกำกับดูแลให้ผู้ที่มีสิทธิผ่านเข้าออกดังกล่าวปฏิบัติตามนโยบาย กฎ ระเบียบ ข้อบังคับ อันเกี่ยวข้องกับระบบสารสนเทศของ สป.พน. อย่างเคร่งครัด

๒.๒ ผู้อำนวยการ

๒.๒.๑ ควบคุมดูแลให้ผู้ใต้บังคับบัญชาปฏิบัติตามแนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

๒.๒.๒ อำนาจในการกำหนดชั้นความลับตามระเบียบว่าด้วยการรักษาความลับของทางราชการของหัวหน้าหน่วยงานของรัฐแต่ในกรณีจำเป็นเร่งด่วนให้ทำได้เป็นการชั่วคราวและให้รีบเสนอผู้มีอำนาจ (ข้อ ๑๖, ๑๗)

๒.๒.๓ เสนอต่อผู้บริหารระดับสูง เพื่อพิจารณาสั่งการให้ข้อมูลและสารสนเทศอันเป็นผลลัพธ์ซึ่งเกิดจากการประมวลผลข้อมูลหรือสารสนเทศที่มาจากสายงานการบังคับบัญชา (เช่น ผลลัพธ์จากการประมวลผลข้อมูลหรือสารสนเทศที่มาจากหลายหน่วยงาน หรือมีการกำหนดชั้นความลับไว้ต่างกัน) ได้รับการกำหนดชั้นความลับตามความเหมาะสม

๒.๒.๔ สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๒.๕ สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับอื่น ๆ ของ สป.พน. เท่าที่ได้รับอนุญาตจากผู้บริหารระดับสูง

๒.๒.๖ สามารถสั่งการ อนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๒.๗ สามารถเสนอเพื่อแต่งตั้งให้ เจ้าหน้าที่ ของ สป.พน. ทำหน้าที่เป็นผู้ดูแลระบบสำหรับงานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา ทั้งนี้ ขึ้นอยู่กับหน้าที่ความรับผิดชอบของหน่วยงานนั้น ๆ

๒.๒.๘ สามารถเสนอต่อผู้บริหารระดับสูงเพื่อขออนุญาตให้หน่วยงานภายนอกเข้าปฏิบัติงานกับระบบสารสนเทศของ สป.พน. ที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๒.๙ สามารถกำหนดและจำแนกพื้นที่ใช้งานระบบสารสนเทศของ สป.พน. ที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๒.๑๐ สามารถกำหนดสิทธิของผู้ใช้งานในการผ่านเข้าออกพื้นที่ใช้งานระบบสารสนเทศของ สป.พน. ที่อยู่ภายใต้สายงานการบังคับบัญชา และมีหน้าที่ต้องกำกับดูแลให้ผู้ที่มีสิทธิผ่านเข้าออกดังกล่าวปฏิบัติตามนโยบาย กฎ ระเบียบ ข้อบังคับ อันเกี่ยวข้องกับระบบสารสนเทศของ สป.พน. อย่างเคร่งครัด

๒.๒.๑๑ มีหน้าที่แจ้งต่อหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้รับทราบและรวบรวมข้อมูลอันเกี่ยวกับ

- การกำหนดหรือเปลี่ยนแปลงสิทธิของผู้ใช้งานที่อยู่ภายใต้สายงานการบังคับบัญชา
- การกำหนดหรือเปลี่ยนแปลงพื้นที่ใช้งานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา

- การกำหนดหรือเปลี่ยนแปลงชั้นความลับของข้อมูล ที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๓ หัวหน้ากลุ่ม

๒.๓.๑ ควบคุมดูแลให้ผู้ใต้บังคับบัญชาปฏิบัติตามแนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

๒.๓.๒ สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับเฉพาะ ชั้นลับ ที่อยู่ภายใต้สายงานการบังคับบัญชา

๒.๓.๓ สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับ เท่าที่ได้รับอนุญาตจากผู้บริหารระดับสูง โดยต้องผ่านความเห็นชอบของ ผู้อำนวยการ ที่เป็นเจ้าของงานระบบสารสนเทศ

๒.๓.๔ สามารถอนุญาตให้บุคคลหรือผู้ใช้งานยืมอุปกรณ์ด้านเทคโนโลยีสารสนเทศในความรับผิดชอบ เช่น Projector, PC เป็นต้น

๒.๔ ผู้ดูแลระบบ

๒.๔.๑ ไม่มีสิทธิเปิดอ่านจดหมายอิเล็กทรอนิกส์หรือการสื่อสารระหว่างกันที่เป็นส่วนตัว (เช่น e-mail, Line, Messenger) ของ ผู้ใช้งาน ยกเว้นในกรณีที่มีคำสั่งศาลให้ดำเนินการตามกฎหมาย

๒.๔.๒ ไม่มีสิทธิเปิดอ่าน หรือใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับ ยกเว้นในกรณีที่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บริหาร สป.พน. ให้มีสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับนั้น

๒.๔.๓ สามารถยุติการทำงานของระบบสารสนเทศ หากพบว่าเป็นภัยต่อความมั่นคงปลอดภัย หรือสร้างภาระให้ระบบสารสนเทศของ สป.พน. โดยไม่จำเป็นต้องมีการแจ้งล่วงหน้า และติดตามสอบสวนหาสาเหตุที่มาของภัยหรือภาระนั้น และทำรายงานให้ผู้อำนวยการกองที่รับผิดชอบระบบทราบ

๒.๔.๔ สามารถยุติการทำงานของระบบสารสนเทศที่เปิดใช้โดยไม่ได้รับอนุญาตจาก สป.พน. โดยไม่ต้องมีการแจ้งล่วงหน้า และติดตามสอบสวนหาสาเหตุที่มาของระบบงานนั้น และทำรายงานให้ผู้อำนวยการทราบ

๒.๔.๕ แจ้งให้ผู้ใช้งานทราบล่วงหน้าถึงวันเวลาที่ต้องปิดระบบเพื่อบำรุงรักษาปรับปรุงหรือเปลี่ยนแปลงระบบ ซึ่งส่งผลให้ต้องหยุดบริการในช่วงเวลาหนึ่ง ยกเว้นในกรณีฉุกเฉิน ผู้ดูแลระบบมีสิทธิปิดระบบทันที และจะต้องพยายามให้ผู้ใช้งานสามารถเก็บบันทึกข้อมูลได้อย่างสมบูรณ์ก่อนที่จะดำเนินการปิดระบบ และทำรายงานให้ผู้อำนวยการกองทราบ

๒.๔.๖ สามารถจำกัดหรือระงับสิทธิของผู้ใช้งานระบบอย่างไม่เหมาะสม และให้รายงานผู้บังบัญชาตามลำดับจนถึงผู้บริหารระดับสูง เพื่อตั้งคณะกรรมการพิจารณาสอบสวนหรือลงโทษตามความเหมาะสม

๒.๔.๗ ต้องดูแลรักษา ตรวจสอบแก้ไข และปรับปรุงระบบสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อให้ระบบสามารถใช้งานได้ดี มีเสถียรภาพ มีความมั่นคงปลอดภัย และมีประสิทธิภาพอยู่เสมอ

๒.๔.๘ ติดตาม กำชับผู้ใช้งาน และปรับปรุงฐานข้อมูลของผู้ใช้งาน ให้มีความถูกต้องเป็นปัจจุบันอยู่เสมอ รวมทั้งต้องลบบัญชีผู้ใช้งานที่หมดสิทธิในการใช้งานระบบออกจากฐานข้อมูล

๒.๔.๙ ต้องติดตามข่าวสารเกี่ยวกับภัยคุกคาม ช่องโหว่ของระบบสารสนเทศ และต้องปรับปรุงดูแลระบบเพื่อลดความเสี่ยงของการถูกบุกรุกอย่างสม่ำเสมอ

๒.๔.๑๐ ต้องขออนุญาตผู้อำนวยการในกรณีที่มีการร่วมมือกับหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการประเมิน ตรวจสอบ

ทดสอบ หาจุดอ่อน ช่องโหว่ อันเกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศ และดำเนินการการแก้ไขอย่างรวดเร็ว

๒.๔.๑๑ ต้องแจ้งหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทันทีและทำรายงานแจ้งผู้บังคับบัญชาตามลำดับชั้น ในกรณีที่ตรวจพบหรือได้รับรายงานจากผู้ใช้งาน หรือสงสัยว่าระบบสารสนเทศที่รับผิดชอบโดยตรง หรือระบบที่เกี่ยวข้องอื่นใดของ สป.พน. ถูกละเมิดทางด้านความมั่นคงปลอดภัย

๒.๕ เจ้าของข้อมูลและสารสนเทศ มีหน้าที่ และความรับผิดชอบ ดังต่อไปนี้

๒.๕.๑ อนุมัติและตรวจทานเพื่อให้แน่ใจว่าสิทธิของผู้ใช้งานถูกต้องเหมาะสม

๒.๕.๒ กำหนดระดับชั้นความลับให้กับข้อมูล

๒.๕.๓ ตรวจทานระดับชั้นความลับของข้อมูลเพื่อให้มั่นใจว่ายังเป็นไปตามความต้องการของการปฏิบัติงาน มีความเหมาะสม และสอดคล้องกับระดับชั้นความลับของข้อมูลนั้น ๆ

๒.๕.๔ ตรวจสอบให้แน่ใจว่าข้อมูลมีการระบุหรือแสดงระดับชั้นความลับตามที่ได้จัดระดับชั้นความลับไว้อย่างถูกต้องและเหมาะสม ไม่ว่าจะอยู่ในรูปแบบหรือสื่อประเภทใดก็ตาม

๒.๕.๕ กำหนดพื้นฐานการรักษาความปลอดภัยในการเข้าถึงข้อมูลของหน่วยงาน จัดทำข้อกำหนดในการสำรองข้อมูล และดำเนินการให้มีการจัดการในเรื่องของการละเมิดความปลอดภัยอย่างเหมาะสม

๒.๖ เจ้าของระบบงาน มีหน้าที่ และความรับผิดชอบ ดังต่อไปนี้

๒.๖.๑ ตรวจสอบให้แน่ใจว่าระบบงานเป็นไปตามความต้องการในปัจจุบันอย่างสม่ำเสมอ

๒.๖.๒ ควบคุมดูแลเพื่อให้มั่นใจว่าข้อมูลมีความปลอดภัยในการควบคุมการเข้าสู่ระบบ

๒.๖.๓ อนุมัติ ตรวจทาน และรับรองสิทธิการเข้าใช้ระบบที่เหมาะกับระดับชั้นความลับของข้อมูล

๒.๖.๔ จัดทำข้อกำหนดในการสำรองข้อมูลและ Source Code ของระบบงาน

๒.๖.๕ ดำเนินการหรือมีการจัดการในเรื่องของการละเมิดความปลอดภัยอย่างเหมาะสม

๒.๖.๖ สามารถมอบหมายหน้าที่และความรับผิดชอบดังกล่าวข้างต้นให้แก่บุคคลอื่นที่เหมาะสม แต่เจ้าของระบบงานยังคงมีหน้าที่และความรับผิดชอบต่อระบบงานดังกล่าวโดยสมบูรณ์

๒.๗ ผู้ใช้งาน มีสิทธิ หน้าที่ และความรับผิดชอบ ดังต่อไปนี้

๒.๗.๑ สามารถเข้าถึงข้อมูล ข่าวสาร ที่มิใช่ข้อมูลและสารสนเทศที่กำหนดชั้นความลับของ สป.พน. ยกเว้นในกรณีที่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บริหาร สป.พน. ให้มีสิทธิในการเข้าถึงหรือควบคุมการใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับนั้น

๒.๗.๒ อุปกรณ์ระบบคอมพิวเตอร์และระบบเครือข่ายของ สป.พน. มีไว้เพื่อใช้ในภารกิจของ สป.พน. เท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บริหาร สป.พน

๒.๗.๓ ต้องช่วยกันรักษาอุปกรณ์ต่าง ๆ ไม่ให้เกิดความเสียหาย หากมีความเสียหายจากอุบัติเหตุหรือภัยต่าง ๆ ผู้ใช้งานต้องรายงานผู้ดูแลระบบและผู้บังคับบัญชาให้รับทราบทันที

๒.๗.๔ การขอใช้งานอุปกรณ์และระบบต่าง ๆ ผู้ใช้งานต้องสามารถแสดงบัตรประจำตัวที่ถูกต้องได้ หากผู้ดูแลระบบร้องขอ

๒.๗.๕ พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ Download ไฟล์ขนาดใหญ่โดยไม่จำเป็น ไม่ส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ในลักษณะจดหมายลูกโซ่ เป็นต้น

๒.๗.๖ เพื่อให้การบริหารระบบเป็นไปอย่างถูกต้อง ผู้ใช้งานต้องให้ข้อมูลประจำตัวที่ถูกต้องสำหรับการเปิดบัญชีผู้ใช้งาน (User ID หรือ Login Account)

๒.๗.๗ ตั้งรหัสผ่าน (Password หรือ Pass phrase) ที่มีความปลอดภัย ตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

๒.๗.๘ ต้องไม่อนุญาตให้ผู้อื่นใช้งานระบบคอมพิวเตอร์ผ่านบัญชีผู้ใช้งานของตนโดยเด็ดขาด มิฉะนั้น ผู้ใช้งานอาจมีความผิดทางวินัยและต้องรับผิดชอบต่อปัญหาที่เกิดขึ้น เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย

๒.๗.๙ ต้องรายงานต่อผู้ดูแลระบบและผู้บังคับบัญชาโดยทันที ในกรณีที่ตรวจพบ หรือสงสัยว่ามีการนำบัญชีผู้ใช้งานของตนหรือของผู้อื่นไปใช้งานโดยไม่ได้รับอนุญาตหรือใช้งานในทางที่มิชอบ และพบเห็นพฤติกรรมการล่วงละเมิดความมั่นคงปลอดภัยทุกอย่างในระบบ

๒.๗.๑๐ ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

๒.๗.๑๑ ไม่ล่วงล้ำเข้าในบริเวณพื้นที่ใช้งานระบบสารสนเทศที่ไม่ได้รับอนุญาต

๒.๗.๑๒ ต้องใช้ระบบในลักษณะที่ถูกต้องตามกฎหมาย ไม่ละเมิดสิทธิและไม่ก่อความเดือดร้อนหรือความเสียหายแก่บุคคลหรือองค์กรอื่น

๒.๗.๑๓ ไม่ติดตั้งหรือเปิดให้บริการระบบเครือข่ายบนเครื่องของ สป.พน. เพื่อทำภารกิจส่วนตัว

๒.๗.๑๔ ต้องคืนทรัพย์สิน สป.พน. อันเกี่ยวกับการปฏิบัติหน้าที่ในทันทีที่พ้นหน้าที่ เช่น อุปกรณ์ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก

๒.๗.๑๕ ต้องทำรายงานแจ้งให้ผู้ดูแลระบบและผู้อำนวยการทราบทันที ในกรณีที่มีการเคลื่อนย้ายหรือถอดถอนอุปกรณ์ระบบสารสนเทศ

๒.๗.๑๖ ต้องปฏิบัติตามมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และวิธีการปฏิบัติ (Procedure) อันเกี่ยวเนื่องกับความมั่นคงปลอดภัยสารสนเทศของ สป.พน.

๒.๗.๑๗ ห้ามผู้ใช้งานติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องของ สป.พน. ก่อนได้รับอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ เพื่อป้องกันปัญหาด้านลิขสิทธิ์และปัญหาอื่น ๆ ที่จะเกิดขึ้นภายหลังการติดตั้ง เช่น การติดตั้ง Access Point ด้วยตนเองแล้วเกิดการเจาะระบบเข้ามาในระบบเครือข่ายของ สป.พน. หรือทำให้เกิดการแพร่กระจายของซอฟต์แวร์ประสงค์ร้าย (Malware) และภัยคุกคามอื่น ๆ เป็นต้น

๒.๗.๑๘ หากพบว่าระบบรักษาความปลอดภัยมีข้อบกพร่อง หรือสงสัยว่ามีผู้ใดกระทำการที่น่าสงสัย ให้แจ้งต่อผู้ดูแลระบบโดยทันที

๒.๗.๑๙ ต้องให้ความร่วมมือกับเจ้าหน้าที่ที่ได้รับมอบหมายให้ทำการสืบสวน สอบสวนเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยของ สป.พน.

๒.๘ หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีหน้าที่ และความรับผิดชอบ ดังต่อไปนี้

๒.๘.๑ พิจารณารายละเอียดการฝ่าฝืนหรือการละเมิดข้อบังคับและนโยบายความมั่นคงปลอดภัยสารสนเทศ ของ สป.พน. ถ้าเป็นการฝ่าฝืนระเบียบขั้นรุนแรงหรือกรณีที่ฝ่าฝืนแล้วก่อให้เกิดความเสียหายแก่ สป.พน. หรือต่อบุคคล จะจัดทำบันทึกรายงานเกี่ยวกับการฝ่าฝืนนโยบายดังกล่าวไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

๒.๘.๒ ในกรณีการละเมิดหรือฝ่าฝืนมีเจตนาไม่ชัดเจน ผู้ละเมิดหรือฝ่าฝืนจะถูกตักเตือนและชี้แจงให้เข้าใจถึงข้อปฏิบัติที่ถูกต้อง หากมีการกระทำการฝ่าฝืนนั้นอีก ให้แต่งตั้งคณะกรรมการพิจารณาและต้องรายงานการกระทำดังกล่าวไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และผู้บังคับบัญชาระดับ

ผู้อำนวยการกองที่เกี่ยวข้องทันที โดยให้มีการสอบสวนและดำเนินการทางวินัยตามความรุนแรงของผลกระทบจากการละเมิดหรือฝ่าฝืนข้อบังคับนั้น ๆ

๒.๘.๓ ป้องกันและแก้ไขปัญหาที่เกิดขึ้นทันที เพื่อให้แน่ใจว่าการละเมิดหรือฝ่าฝืนเหล่านั้นจะไม่ลุกลามเป็นปัญหาใหญ่

๒.๘.๔ การดำเนินการทางกฎหมายใด ๆ ต้องได้รับความช่วยเหลือจากหน่วยงานดูแลรับผิดชอบด้านกฎหมายและตัวแทนของ สป.พน. ในการดำเนินคดีใด ๆ ที่เกี่ยวข้องกับ สป.พน. ต้องเป็นหน้าที่ของเจ้าหน้าที่ระดับผู้บริหารที่ได้รับมอบหมายเท่านั้น

๒.๘.๕ จัดอบรมส่งเสริมให้ผู้ใช้งานตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ

๒.๘.๖ ให้คำแนะนำด้านเทคนิคที่เกี่ยวกับการรักษาความปลอดภัยสารสนเทศ

๒.๘.๗ วางแผนควบคุมระบบความมั่นคงปลอดภัยสารสนเทศและการเตือนภัย รวมถึงวิเคราะห์หาวิธีการแก้ไขจุดอ่อนของระบบสารสนเทศ

๒.๘.๘ สืบสวนเหตุการณ์ต่าง ๆ ที่ไม่เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

๒.๘.๙ ติดต่อและประสานงานเพื่อสร้างความร่วมมือทางด้านความมั่นคงปลอดภัยระหว่างองค์กร

๒.๘.๑๐ รวบรวมรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น ๆ เช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ ศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

๒.๘.๑๑ รวบรวมรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่าง ๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน เช่น กลุ่มที่มีความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ หรือสมาคมต่าง ๆ ในอุตสาหกรรมที่องค์กรมีส่วนร่วม เป็นต้น

๒.๘.๑๒ กำหนดกระบวนการในการอนุมัติการใช้งานระบบสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

๒.๙ หน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายและระบบคอมพิวเตอร์ มีหน้าที่ และความรับผิดชอบ ดังต่อไปนี้

๒.๙.๑ พัฒนา ติดตั้ง ตรวจสอบ ปรับปรุง ซ่อมแซมและบำรุงรักษาอุปกรณ์ บริหารจัดการระบบเกี่ยวกับอุปกรณ์โครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ (IT Infrastructure) ให้กับหน่วยงานของ สป.พน. ทั้งหมด

๒.๙.๒ บริหารจัดการระบบเครือข่ายเชื่อมโยงคอมพิวเตอร์ (Network Administration) ที่ใช้งานภายใน สป.พน. ทุกระบบ และควบคุมการเชื่อมต่อเครือข่ายอินเทอร์เน็ตโดยตรงผ่านช่องทางอื่น รวมทั้งควบคุมการเชื่อมต่อเครือข่ายจากภายนอก เช่น การ Remote เครื่องคอมพิวเตอร์ การใช้งาน VPN เป็นต้น

๒.๙.๓ รับผิดชอบในการจัดหาและควบคุมการใช้งาน Corporate Antivirus จัดเตรียมคู่มือและข้อมูลต่าง ๆ ที่เกี่ยวกับ Corporate Antivirus จัดทำสถิติ กราฟ และผลการใช้งาน รวมไปถึงการอนุญาตหรือจำกัดการใช้งานของผู้ใช้งาน

๒.๙.๔ รับผิดชอบในการบำรุงรักษา ปรับปรุง และตั้งค่าระบบ Corporate Antivirus เพื่อแก้ไขช่องโหว่ และบริหารจัดการลิขสิทธิ์การใช้งานระบบ

๒.๙.๕ รับผิดชอบการจัดทำและปรับปรุงเนื้อหาของ MOEN Website (www.energy.go.th) และ Website ที่เกี่ยวข้องกับความปลอดภัยเทคโนโลยีสารสนเทศ (IT Security) อื่น ๆ ของ สป.พน.

๒.๙.๖ ควบคุมการติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องคอมพิวเตอร์ของ สป.พน.

๒.๙.๗ รับผิดชอบร่วมกับผู้ดูแลระบบในการตรวจสอบซอฟต์แวร์ทั้งหมด เพื่อป้องกันการละเมิดข้อตกลง และหาทางป้องกันซอฟต์แวร์ที่ใช้ในการตรวจประเมินระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิดหรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น ๆ

๒.๙.๘ จัดทำข้อมูลทรัพย์สินระบบสารสนเทศของ สป.พน.รวมถึงลักษณะการตั้งค่าของอุปกรณ์เครือข่าย เพื่อประสิทธิภาพในบริหารระบบสารสนเทศของ สป.พน.

๒.๙.๙ ให้คำแนะนำและเป็นที่ปรึกษาร่วมในการพิจารณารายละเอียดการฝ่าฝืนหรือการละเมิดข้อบังคับ และนโยบายความมั่นคงปลอดภัยสารสนเทศ ของ สป.พน. ร่วมกับหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงร่วมกันแก้ไขปัญหาปัญหาที่เกิดขึ้นดังกล่าว

๒.๙.๑๐ ควบคุมระบบความมั่นคงปลอดภัยสารสนเทศและการเตือนภัย รวมถึงวิเคราะห์หาวิธีการแก้ไขจุดอ่อนของระบบสารสนเทศร่วมกับหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๙.๑๑ กำหนดและควบคุมการสำรองข้อมูลและการกู้คืนระบบสารสนเทศของ สป.พน.

๒.๙.๑๒ ควบคุมการพิสูจน์ตัวตน (Authentication) ก่อนเข้าถึงระบบสารสนเทศของ สป.พน.

๒.๙.๑๓ บริหารจัดการการเช่าเครื่องคอมพิวเตอร์ให้มีปริมาณที่เหมาะสมและเพียงพอต่อการใช้งาน

๒.๑๐ หน่วยงานดูแลรับผิดชอบด้านตรวจสอบภายใน มีหน้าที่ และความรับผิดชอบ ดังต่อไปนี้

๒.๑๐.๑ ตรวจสอบการปฏิบัติงานของผู้ใช้งานให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศของ สป.พน. ที่ดำเนินไปภายใต้มาตรฐานและแนวทางการปฏิบัติที่ได้กำหนดไว้ในนโยบายและร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยสารสนเทศและนโยบายฯ เพื่อป้องกันทรัพย์สินและข้อมูลต่าง ๆ ของ สป.พน.

๒.๑๐.๒ ให้ความช่วยเหลือแก่หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในการชี้ถึงความเสี่ยงและภัยคุกคามต่าง ๆ อันอาจก่อให้เกิดอันตรายต่อความมั่นคงปลอดภัยของ สป.พน.

๒.๑๑ หน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง มีหน้าที่ และความรับผิดชอบในการบริหารและจัดการความเสี่ยงของระบบสารสนเทศ เพื่อปรับปรุงให้องค์กรมีคุณภาพและประสิทธิภาพ รวมถึงลดโอกาสที่จะเกิดความเสียหายได้

๒.๑๒ หน่วยงานดูแลรับผิดชอบด้านกฎหมาย มีหน้าที่ และความรับผิดชอบในการให้ความเห็นหรือให้คำปรึกษาเกี่ยวกับ กฎหมาย พระราชบัญญัติ พระราชกฤษฎีกา ระเบียบ ข้อกำหนด กฎเกณฑ์ข้อบังคับ การฟ้องร้องดำเนินคดี รวมถึงข้อละเมิดทรัพย์สินทางปัญญา ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ สป.พน.

๒.๑๓ หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการ มีหน้าที่ และความรับผิดชอบดังต่อไปนี้

๒.๑๓.๑ ตรวจสอบคุณสมบัติของผู้สมัครข้าราชการ พนักงานราชการ และพนักงานจ้างเหมาบริการ ที่เกี่ยวกับการละเมิดความมั่นคงปลอดภัยสารสนเทศ

๒.๑๓.๒ การให้**เจ้าหน้าที่**ลงนามมิให้เปิดเผยความลับของ สป.พน.

๒.๑๓.๓ รายงานข้อมูลการว่าจ้างงาน การเปลี่ยนแปลงสภาพการว่าจ้างงาน การลาออก การถึงแก่กรรม การโยกย้าย และการพักงานหรือการลงโทษทางวินัย ให้แก่หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยสารสนเทศและนโยบายฯ

๒.๑๒ หน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร มีหน้าที่ และความรับผิดชอบในการจัดการประชุม สัมมนา หรือจัดอบรมให้ความรู้แก่บุคลากรใหม่และผู้ใช้งาน เกี่ยวกับวิธีการปฏิบัติงาน เพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของ สป.พน.

๒.๑๓ หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่ มีหน้าที่ และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ควบคุมการเข้า-ออกอาคารและสำนักงาน จัดเตรียมการป้องกันต่อภัยคุกคามต่าง ๆ ทั้งจากมนุษย์และธรรมชาติ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว และความไม่สงบของบ้านเมือง เป็นต้น

การควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับหน่วยงานภายนอก

๑. วัตถุประสงค์

เพื่อควบคุมหน่วยงานภายนอกที่มีการใช้งานระบบสารสนเทศและทรัพยากรสารสนเทศอื่น ๆ ของ สป.พน. ให้เป็นไปอย่างมั่นคงปลอดภัย นโยบายนี้ใช้กับการดำเนินงานซึ่งไม่สามารถทำขึ้นภายใน สป.พน. เช่น การพัฒนาระบบสารสนเทศ การใช้บริการของที่ปรึกษา การใช้บริการด้านระบบสารสนเทศจากภายนอกเป็นต้น

๒. การระบุสัญญาเพื่อควบคุมการเข้าใช้งานของหน่วยงานภายนอก

๒.๑ หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าถึงข้อมูลของ สป.พน. จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้อำนวยการกองที่เป็นเจ้าของข้อมูลและสารสนเทศ ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าว

๒.๒ ต้องทำการแจ้งเป็นลายลักษณ์อักษรให้หน่วยงานภายนอกทราบถึงความสำคัญที่มีต่อความมั่นคงปลอดภัยสารสนเทศของข้อมูล ซึ่งหน่วยงานภายนอกจะต้องลงนามในเอกสารสัญญาเรื่องการไม่เปิดเผยข้อมูลของ สป.พน. โดยเอกสารดังกล่าวจะถูกจัดเก็บไว้เป็นหลักฐาน ในส่วนของผู้ร่วมสัญญาต้องทำการลงนามในสัญญาเรื่องการปกปิดข้อมูลเป็นความลับ และจัดเก็บเอกสารไว้ในแฟ้มสัญญา

๒.๓ เจ้าของโครงการหรือผู้จัดการโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้เฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาเรื่องการไม่เปิดเผยข้อมูล

๒.๔ คู่สัญญาหรือหน่วยงานภายนอก มีหน้าที่ที่ต้องแจ้งให้กับผู้เป็นเจ้าของหรือผู้รับผิดชอบโครงการทราบทันทีที่พบว่ามีการคุกคามที่มีผลต่อความมั่นคงปลอดภัยในลักษณะใด ๆ ก็ตาม รวมถึงการเข้าถึงข้อมูลโดยผู้ไม่มีสิทธิ หรือการผ่อนปรน หรือละเว้นไม่ปฏิบัติตามวินัยความมั่นคงปลอดภัยสารสนเทศของ สป.พน. นอกจากนั้น **เจ้าหน้าที่** ของ สป.พน. ผู้ซึ่งรับทราบถึงเหตุการณ์ที่คุกคามด้านความปลอดภัยซึ่งเกิดจากคู่สัญญาหรือบุคคลที่สาม ต้องแจ้งให้หน่วยงานที่ดูแลรับผิดชอบเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทราบทันทีตามกระบวนการในนโยบายการรายงานเหตุการณ์ด้านความปลอดภัย

๒.๕ สัญญาการใช้งานระบบสารสนเทศทั้งหมดที่มีการจัดทำขึ้นต้องระบุถึง**สิทธิในการตรวจสอบ** เพื่อให้มั่นใจได้ว่า สป.พน. สามารถเข้าไปประเมินสภาพแวดล้อมของการควบคุมภายในทั้งทางกายภาพ (Physical) และทาง Logical ของคู่สัญญาหรือหน่วยงานภายนอกได้

๓. การให้ความสนับสนุนจาก สป.พน.

หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าถึงข้อมูลของ สป.พน. จะต้องทำการขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการกองที่เป็นเจ้าของข้อมูลและสารสนเทศ ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าว

๔. มาตรฐานการเลือกหน่วยงานภายนอกโดยทั่วไป

๔.๑ ผู้อำนวยการที่รับผิดชอบโครงการ ต้องขอข้อมูลเบื้องต้นของหน่วยงานภายนอก ในรายที่ยังไม่ทราบรายละเอียด ซึ่งอาจจะรวมถึงข้อมูลด้านการเงินที่ใช้อ้างอิงได้

๔.๒ สป.พน. ต้องพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ ขึ้นอยู่กับความสำคัญของระบบที่เข้าไปปฏิบัติงานและข้อมูลที่ให้ไป

๔.๓ สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของ สป.พน. ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานในการประมวลผลข้อมูลนั้น

๕. สัญญาในการไม่เปิดเผยข้อมูล

๕.๑ กรณีที่มีความจำเป็น สป.พน. จะให้สิทธิหน่วยงานภายนอกในการเข้าถึงข้อมูลเช่นเดียวกับผู้ใช้งานภายใน โดยจะจำกัดเพียงการเข้าถึงข้อมูลเท่าที่จำเป็นเพื่อให้งานเสร็จสมบูรณ์

ข้อพิจารณา ให้อยู่ในดุลพินิจของผู้อำนวยการเจ้าของข้อมูลและสารสนเทศนั้น ๆ หรือหน่วยงานที่ดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕.๒ หน่วยงานภายนอก ที่ปรึกษา หรือคู่สัญญาที่ทำงานโดยตรงให้กับ สป.พน. ทุกคน ไม่ว่าจะทำงานอยู่ภายใน สป.พน. หรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของ สป.พน. โดยสัญญาต้องจัดทำให้เสร็จก่อนที่จะให้สิทธิในการเข้าสู่ระบบเครือข่ายและข้อมูลต่าง ๆ ของ สป.พน.

๖. มาตรฐานทั่วไปของหนังสือสัญญาว่าจ้างที่ต้องมีการใช้งานระบบสารสนเทศจากหน่วยงานภายนอก ประกอบไปด้วยข้อความดังต่อไปนี้

๖.๑ สัญญาในการยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยของ สป.พน.

๖.๒ สิทธิสำหรับ สป.พน. ที่จะตรวจสอบสภาพแวดล้อมการทำงานรวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก

๖.๓ เอกสารต่าง ๆ เกี่ยวกับมาตรการการควบคุมที่ใช้ทั้งด้าน Physical และด้าน Logical เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคงปลอดภัย ได้ทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๖.๔ ข้อกำหนดทางด้านกฎหมาย เช่น ความลับส่วนบุคคล (Privacy) และการป้องกันข้อมูล

การควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับผู้ปฏิบัติงานชั่วคราว

๑. วัตถุประสงค์

เพื่อให้ทุกหน่วยงาน กำกับ ดูแล ผู้ปฏิบัติงานชั่วคราว (Temporary Worker) ที่ไม่ใช่ เจ้าหน้าที่ของ สป.พน. และอยู่ในความรับผิดชอบ ให้ใช้ระบบสารสนเทศอย่างเหมาะสม เกิดประโยชน์สูงสุดและมีความปลอดภัย

๒. การขอรับสิทธิของผู้ใช้งาน

๒.๑ หน่วยงานที่มีความประสงค์จะขออนุญาตให้ผู้ปฏิบัติงานชั่วคราวเข้าสู่ระบบสารสนเทศของ สป.พน. ให้ขออนุมัติจากผู้บังคับบัญชาระดับกองขึ้นไปที่มีอำนาจครอบคลุมระบบสารสนเทศที่ผู้ปฏิบัติงานชั่วคราวต้องการจะเข้าถึงทั้งหมด ทั้งนี้ให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่ สป.พน. 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 มีหน้าที่กำกับดูแลพฤติกรรมการใช้ระบบสารสนเทศของ สป.พน. ให้เป็นไปตามความต้องการของหน่วยงาน

๓.๔ หัวหน้าหน่วยงานสามารถยกเลิกสิทธิการใช้ระบบของผู้ปฏิบัติงานชั่วคราวที่มีพฤติกรรมการใช้ระบบสารสนเทศของ สป.พน. ในทางที่ไม่เหมาะสม

๔. การดูแลเมื่อสิ้นสุดการปฏิบัติงานชั่วคราว

๔.๑ ผู้ปฏิบัติงานชั่วคราวที่ได้ทำการสร้างข้อมูลอิเล็กทรอนิกส์ที่ไม่ก่อให้เกิดประโยชน์กับ สป.พน. ไว้บนระบบสารสนเทศของ สป.พน. จะต้องทำการลบข้อมูลทิ้งทั้งหมด โดยผู้ดูแลผู้ปฏิบัติงานชั่วคราวต้องกำกับดูแลการลบข้อมูลอิเล็กทรอนิกส์ดังกล่าว

๔.๒ ผู้ดูแลระบบต้องลบ Username และ Password ของผู้ปฏิบัติงานชั่วคราวทันที เมื่อครบกำหนด การขอใช้งาน

๔.๓ ผู้ดูแลผู้ปฏิบัติงานชั่วคราวต้องแจ้งผู้บังคับบัญชาทันทีที่ผู้ปฏิบัติงานชั่วคราวหมดความจำเป็นหรือเลิกการปฏิบัติงานก่อนกำหนด หรือครบกำหนดการปฏิบัติงานชั่วคราว

๕. การดูแลเรื่องข้อมูลด้านเทคโนโลยีสารสนเทศที่เป็นความลับ

๕.๑ ผู้ปฏิบัติงานชั่วคราวต้องไม่เปิดเผยข้อมูลในระบบสารสนเทศของ สป.พน. ต่อบุคคลอื่นที่ไม่เกี่ยวข้องกับการปฏิบัติงานนั้น ทั้งระหว่างการปฏิบัติงานและภายหลังการปฏิบัติงานเสร็จสิ้นไปแล้ว ยกเว้นกรณีที่จำเป็นตามคำสั่งศาลหรือตามกฎหมาย

๕.๒ สป.พน. สงวนสิทธิ์ที่จะเรียกร้องค่าเสียหาย หากพบว่าผู้ปฏิบัติงานชั่วคราวนำข้อมูลที่เป็นความลับในระบบสารสนเทศของ สป.พน. ไปใช้เพื่อประโยชน์ส่วนตน หรือเพื่อประโยชน์ของบุคคล/นิติบุคคลอื่น ๆ

๖. สิทธิในการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว

การใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว หมายถึง การที่ผู้ปฏิบัติงานชั่วคราวเข้ามาปฏิบัติงานในระบบสารสนเทศของ สป.พน. โดยผ่านเครือข่าย Internet, เครือข่าย Wireless หรือเครือข่ายคอมพิวเตอร์อื่น ๆ ที่อยู่นอกเหนือการควบคุมของ สป.พน. สิทธิในการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราวเป็นสิทธิที่ สป.พน. จะอนุญาตให้เฉพาะกับตัวบุคคลในระหว่างที่บุคคลนั้นสังกัดอยู่กับบริษัท/องค์กรใดเท่านั้น โดยไม่สามารถถ่ายโอนกันได้ระหว่างบุคคล บริษัท/องค์กร หากผู้ที่เคยได้รับสิทธิดังกล่าวไม่ได้สังกัดอยู่กับบริษัท/องค์กรที่เคยได้รับสิทธิแล้ว ให้ถือว่าบุคคลดังกล่าวหมดสิทธิการใช้งาน

๖.๑ ผู้ที่ สป.พน. จะให้สิทธิใช้งาน Remote Access ในการปฏิบัติงานชั่วคราวคือ ผู้ปฏิบัติงานชั่วคราวที่เป็นที่ปรึกษา (Consultant) หรือผู้ปฏิบัติงานตามสัญญาจ้าง (Contractor) เท่านั้น ผู้ปฏิบัติงานชั่วคราวที่เป็นนิสิตนักศึกษาฝึกงานจะไม่ได้รับสิทธิดังกล่าว

๖.๒ ผู้ปฏิบัติงานชั่วคราวจะต้องขออนุญาตผู้อำนวยการกองหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายและระบบคอมพิวเตอร์ล่วงหน้า ก่อนเข้ามาใช้งาน Remote Access เพื่อเข้าสู่ระบบสารสนเทศ ผู้ปฏิบัติงานชั่วคราวจะต้องระบุวัตถุประสงค์ วิธีการ Access และขอบข่ายของการ Access ให้ชัดเจน โดย สป.พน. จะอนุญาตให้เป็นรายครั้ง หรือเป็นช่วงระยะเวลาจำกัด แล้วแต่กรณีและความจำเป็น

๖.๓ สป.พน. สงวนสิทธิ์ที่จะดำเนินคดีตามกฎหมายกับการโยกย้าย เปลี่ยนแปลงโปรแกรมหรือข้อมูลของ สป.พน. อื่นใดนอกเหนือไปจากที่ผู้ปฏิบัติงานชั่วคราวได้รับอนุญาต

๖.๔ สป.พน. สงวนสิทธิ์เรียกร้องค่าเสียหาย หากระบบคอมพิวเตอร์ของ สป.พน. ได้รับความเสียหาย เช่น การติดซอฟต์แวร์ประสงค์ร้าย (Malware) บนคอมพิวเตอร์จากการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว เป็นต้น

๗. ข้อกำหนดสำหรับผู้ปฏิบัติงานชั่วคราวที่เป็นนิสิตนักศึกษาฝึกงาน

ผู้ปฏิบัติงานชั่วคราวที่เป็นนิสิตนักศึกษาฝึกงานต้องส่งมอบ Source Code, Executable Files และลิขสิทธิ์ในผลงานที่ได้พัฒนาขึ้นทั้งหมดในระหว่างการฝึกงานให้กับ สป.พน. เพื่อประโยชน์ในการตรวจสอบด้านความมั่นคงปลอดภัย

หมวด ๓
ความมั่นคงปลอดภัยทางด้านทรัพยากรบุคคล
(Human Resource Security)

จุดประสงค์ เพื่อให้ **เจ้าหน้าที่** ผู้ที่ สป.พน. ทำสัญญาจ้างและหน่วยงานภายนอก เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตน ทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และการสิ้นสุดหรือการเปลี่ยนการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ที่ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่ โดยมีนโยบาย ดังนี้

- **ความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล**

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล (Human Resource Security)

๑. วัตถุประสงค์

เพื่อให้มีมาตรฐานในการควบคุมความปลอดภัยส่วนบุคคล โดยกำหนดเป็นมาตรฐานเกี่ยวกับผู้บริหาร เจ้าหน้าที่ ของ สป.พน. เริ่มตั้งแต่กระบวนการสรรหา เจ้าหน้าที่ ใหม่ เพื่อให้มั่นใจว่ามีการพิจารณาคุณสมบัติอย่างเพียงพอก่อนที่จะมีการว่าจ้าง ตลอดจนเมื่อเริ่มปฏิบัติงานต้องมีการกำหนดสิทธิในการเข้าสู่อาคารสถานที่และระบบงานที่สำคัญ เพื่อปฏิบัติงานตามหน้าที่และสิทธินั้น และจะต้องมีการยกเลิกเมื่อสิ้นสุดการว่าจ้างหรือมีการโยกย้ายการปฏิบัติงานของ เจ้าหน้าที่ ดังกล่าว

๒. มาตรฐานการสร้างความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากร

๒.๑ การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Including Security in Job Responsibilities)

ผู้อำนวยการ ต้องกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศในคุณสมบัติของบุคลากรด้านเทคโนโลยีสารสนเทศในกำกับ ดังนี้

๒.๑.๑ ต้องรับผิดชอบและสามารถปกปิดรหัสผ่าน ไว้มิให้รั่วไหลได้

๒.๑.๒ สามารถป้องกันเครื่องคอมพิวเตอร์จากการติดหรือแพร่ระบาดของซอฟต์แวร์ประสงค์ร้าย (Malware) ได้

๒.๑.๓ มีความรู้ในการทำให้ระบบสารสนเทศมีความแข็งแกร่ง (Hardening)

๒.๑.๔ มีความรับผิดชอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอื่น ๆ ตามหน้าที่ของงานที่ได้รับมอบหมาย

๒.๒ การตรวจสอบคุณสมบัติของผู้สมัคร

๒.๒.๑ หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการ ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคน ก่อนที่จะบรรจุเป็น เจ้าหน้าที่ หรือลูกจ้างของ สป.พน. โดยจะต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบสารสนเทศของหน่วยงานใดมาก่อน

๒.๒.๒ หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการ จะต้องจัดเตรียมข้อมูลที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศของ สป.พน. เพื่อให้ เจ้าหน้าที่ ที่เข้ามาใหม่ได้ศึกษาและรับทราบ

๒.๒.๓ **เจ้าหน้าที่** ใหม่ทุกคนจะต้องลงนามรับทราบและยอมรับสัญญาในนโยบายความมั่นคงปลอดภัยสารสนเทศในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ความรับผิดชอบตามนโยบายเหล่านั้น

๒.๓ การกำหนดเงื่อนไขการจ้างงาน

๒.๓.๑ หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลต้องกำหนดเงื่อนไขการจ้างงานที่รวมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของ สป.พน.

๒.๓.๒ เพื่อให้การบริหารจัดการ Login หรือ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการ ต้องแจ้งให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยสารสนเทศและนโยบายฯ ทราบทันทีเมื่อมี

๒.๓.๒.๑ การบรรจุเจ้าหน้าที่

๒.๓.๒.๒ การเปลี่ยนแปลงสภาพเจ้าหน้าที่

๒.๓.๒.๓ การลาออก หรือการสิ้นสุดการเป็น เจ้าหน้าที่ หรือการถึงแก่กรรม

๒.๓.๒.๔ การโยกย้ายหน่วยงาน

๒.๓.๒.๕ การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

๒.๓.๓ ผู้อำนวยการของทุกหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ ต้องกำหนดเปลี่ยนแปลง หรือยกเลิกสิทธิของผู้ใช้งานที่เกี่ยวกับ Login หรือ User ID เพื่อให้สอดคล้องกับการเปลี่ยนแปลงสถานะของการว่าจ้างนั้นทันที โดยต้องเก็บข้อมูลให้สามารถตรวจสอบประวัติการเปลี่ยนแปลงสิทธิในระบบสารสนเทศที่เกิดขึ้นเหล่านั้นได้

๒.๓.๔ เมื่อสิ้นสุดการเป็นเจ้าหน้าที่หรือเปลี่ยนลักษณะการปฏิบัติราชการ ผู้ใช้งานจะต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของ สป.พน. เช่น อุปกรณ์ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออกฯลฯ ให้แก่ สป.พน. ในทันทีที่พ้นหน้าที่ เป็นต้น

๒.๔ การลงนามมิให้เปิดเผยความลับของ สป.พน.

หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลและสวัสดิการ ต้องจัดให้มีการลงนามในสัญญาระหว่าง เจ้าหน้าที่ และ สป.พน. ว่าจะไม่เปิดเผยความลับของ สป.พน. โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้าง เจ้าหน้าที่ นั้น ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า ๑ ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

๓. การอบรมผู้ใช้งาน

เพื่อให้ผู้ใช้งานได้รับทราบและตระหนักถึงภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้สามารถป้องกันภัยที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศได้อย่างมีประสิทธิภาพ

๓.๑ การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน

๓.๑.๑ หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ร่วมกับหน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร ต้องจัดการประชุม สัมมนา หรืออบรมให้ความรู้แก่ผู้ใช้งาน เกี่ยวกับวิธีปฏิบัติงานเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศและเครือข่ายของ สป.พน. โดยหลักสูตรการอบรมขึ้นอยู่กับหน้าที่ความรับผิดชอบของผู้ใช้งาน

๓.๑.๒ หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยสารสนเทศและนโยบายฯ มีหน้าที่ในการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยสารสนเทศ ของ สป.พน. ด้วย

๓.๑.๓ เจ้าหน้าที่ ใหม่ของ สป.พน.. ทุกท่าน ต้องได้รับการอบรมเกี่ยวกับนโยบายความมั่นคงปลอดภัยสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้องกับ สป.พน. โดยเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของ เจ้าหน้าที่ ด้วย

๓.๒ กระบวนการทางกฎหมายและวินัย

สป.พน. จัดให้มี มาตรการดำเนินการกับผู้ฝ่าฝืนหรือละเมิดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีข้อปฏิบัติ ดังนี้

๓.๒.๑ การฝ่าฝืนระเบียบโดยเล็กน้อยจากความไม่ตั้งใจหรือบังเอิญ เช่น การเลือกรหัสผ่านที่ไม่เหมาะสม การสร้าง process ที่เกินกำลังระบบ การใช้เนื้อที่ดิสก์เกินโควต้าโดยไม่ปฏิบัติตาม คำเตือน การสั่งใช้งานโปรแกรมที่ใช้ทรัพยากรจำนวนมากจนเกิดผลกระทบต่อการทำงานของระบบ เป็นต้น ผู้ดูแลระบบจะแจ้งเตือนโดยวาจา หรือจดหมายอิเล็กทรอนิกส์ หรือเป็นลายลักษณ์อักษร แต่หากเป็นการกระทำผิดซ้ำซ้อน ผู้ดูแลระบบอาจระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศไว้ก่อนจนกว่าจะมีการตักเตือนอย่างเป็นลายลักษณ์อักษรโดยผู้บังคับบัญชา และมีการปรับปรุงแล้ว

๓.๒.๒ การฝ่าฝืนระเบียบขั้นรุนแรง เกิดจากการละเมิดกฎโดยเจตนาหรือจงใจสร้างความเสียหายให้แก่ระบบ โดยไม่มีสิทธิและไม่ได้รับอนุญาต

๓.๒.๒.๑ การจงใจสร้างความเสียหายแก่โปรแกรมหรือข้อมูลหรืออุปกรณ์ฮาร์ดแวร์ระบบ

๓.๒.๒.๒ การขโมยหรือพยายามขโมยทรัพย์สินหรือสิ่งที่ไม่มีสิทธิในการครอบครองมาไว้ในครอบครอง ซึ่งก่อให้เกิดความเสียหายแก่ผู้อื่น เช่น การลักลอบใช้งานอุปกรณ์ ระบบสื่อสาร หรือคอมพิวเตอร์ เป็นต้น

๓.๒.๓ การเข้าถึงระบบโดยมิชอบหรือโดยไม่มีอำนาจ (Unauthorized access) แบ่งเป็นการเข้าถึงทั้งในระดับกายภาพ การเข้าถึงระบบสารสนเทศหรือข้อมูล และการเข้าถึงโดยผ่านเครือข่ายสาธารณะ เช่น การลักลอบดักฟังหรือดักเก็บข้อมูลที่มีชั้นความลับ ทั้งในส่วนของการติดตั้งซอฟท์แวร์และฮาร์ดแวร์ที่สามารถดักจับข้อมูล การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) การทดลอง Crack Password การทดลองถอดรหัส การตรวจสอบ Network Traffic โดยไม่ได้รับอนุญาตหรือมีเหตุอันสมควร เป็นต้น

๓.๒.๔ ประพฤติมิชอบในกิจกรรมใด ๆ ที่เกี่ยวข้องกับ สป.พน. เช่น การคดโกง คัดลอกผลงาน หรือให้ข้อมูลที่ผิดแก่ทาง สป.พน. โดยเจตนา

๓.๒.๕ การสร้างเว็บเพจส่วนตัวที่แสดงออกในลักษณะที่ขัดต่อกฎหมาย กฎ ระเบียบ และศีลธรรม

๓.๒.๖ การก่อความวุ่นวายที่ขัดต่อกฎ ระเบียบของ สป.พน. หรือสร้างความเดือดร้อนรบกวนการทำงานของผู้ใช้งานอื่น ๆ ในระบบเครือข่าย

๓.๒.๗ กรณีที่ฝ่าฝืนหรือละเมิดข้อกำหนดในระเบียบนี้ และก่อให้เกิดความเสียหายแก่ สป.พน. หรือบุคคลหนึ่งบุคคลใด สป.พน. จะพิจารณาดำเนินการทางวินัยและกฎหมายแก่ผู้ใช้งานหรือหน่วยงานภายนอกนั้นตามความเหมาะสม ดังต่อไปนี้

๓.๒.๗.๑ ผู้ดูแลระบบจะพิจารณาระงับการใช้งาน และจะแจ้งชื่อผู้ใช้งานที่ทำผิดระเบียบไปยังหน่วยงานต้นสังกัดให้รับทราบ หรือแจ้งผู้บริหาร สป.พน. รับทราบและพิจารณาตั้งกรรมการสอบสวนข้อเท็จจริง เพื่อพิจารณาจากความรุนแรงหรือความเสียหายที่เกิดขึ้นเป็นรายกรณีไป และ สป.พน. อาจพิจารณาดำเนินการทางวินัยหรือทางกฎหมายแก่ผู้นั้นตามความเหมาะสม

๓.๒.๗.๒ ลงโทษทางวินัยต่อผู้ละเมิดตามความเหมาะสม เพื่อมิให้เกิดการละเมิดซ้ำ และในกรณีที่ผู้ละเมิดเป็นหน่วยงานภายนอก ให้ดำเนินการตามกฎหมายต่อไป

๓.๒.๗.๓ หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อ สป.พน. อย่างร้ายแรง หรือเข้าข่ายความผิดตามกฎหมาย ให้ดำเนินการตามกฎหมายต่อไป

๓.๒.๗.๔ หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อระบบสารสนเทศและต้องเสียค่าใช้จ่ายในการกู้คืน สป.พน. สามารถเรียกร้องค่าเสียหายในส่วนนี้ เพื่อเป็นค่าใช้จ่ายในการกู้คืน

ข้อยกเว้น : กิจกรรมที่เกี่ยวกับการทดสอบระบบสารสนเทศ เพื่อตรวจสอบหรือส่งเสริมความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่าย เช่น การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) การทดลองสุ่มถอดรหัสผ่าน (Crack Password) การตรวจสอบ Network Traffic เป็นต้น หากปฏิบัติโดยหน่วยงานหรือบุคคลที่ได้รับอนุญาต หรือโดยหน่วยงานหรือบุคคลได้รับมอบหมายจาก สป.พน. แล้ว จะไม่ถือว่าเป็นการฝ่าฝืนระเบียบนี้

หมวด ๔
การบริหารจัดการทรัพย์สิน
(Asset Management)

จุดประสงค์ เพื่อป้องกันทรัพย์สินของ สป.พน. จากความเสียหายที่อาจเกิดขึ้นได้ และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสม โดยมีการจัดทำบัญชีทรัพย์สินระบุผู้เป็นเจ้าของทรัพย์สิน และกำหนดหลักเกณฑ์การใช้งานทรัพย์สินที่เหมาะสม มีการจัดหมวดหมู่ทรัพย์สินตามระดับชั้นความลับ และจัดทำป้ายชื่อ เพื่อการบริหารจัดการทรัพย์สินตามที่ได้จัดหมวดหมู่ไว้ โดยมีนโยบาย ดังนี้

การจัดหมวดหมู่และการควบคุมทรัพย์สิน (Asset Classification and Control)

๑. วัตถุประสงค์

เพื่อเป็นการกำหนดมาตรฐานในการจัดหมวดหมู่และการควบคุมทรัพย์สินของ สป.พน. เพื่อป้องกันทรัพย์สินจากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจเกิดขึ้นได้

๒. การจัดหมวดหมู่และการควบคุมทรัพย์สิน

๒.๑ การจัดทำบัญชีทรัพย์สิน ผู้อำนวยการแต่ละหน่วยงาน ต้องทำบัญชีทรัพย์สินของหน่วยงานและแบ่งประเภทให้ชัดเจน ซึ่งรวมถึงบัญชีครุภัณฑ์คอมพิวเตอร์และบัญชีข้อมูลที่เก็บไว้ในสื่อต่าง ๆ ทั้งหมด เพื่อใช้ในการกำหนดมูลค่าทรัพย์สิน ระดับความสำคัญและวิธีการป้องกัน ที่เหมาะสม รวมทั้งต้องระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) ตามที่กำหนดไว้ในบัญชีทรัพย์สิน ซึ่งมีแนวทางปฏิบัติ ดังนี้

๒.๑.๑ ทรัพย์สินของ สป.พน. ที่เป็นครุภัณฑ์อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย และซอฟต์แวร์ที่มีค่าลิขสิทธิ์ ต้องมีการขึ้นบัญชีไว้ในระบบ ของ สป.พน. ตามหลักเกณฑ์หรือสัญญาที่ได้มีการกำหนดไว้สำหรับระบบดังกล่าว

๒.๑.๒ ทรัพย์สินของ สป.พน. ที่เป็นซอฟต์แวร์ที่ใช้เพื่อการให้บริการของ สป.พน. ซึ่งไม่มีค่าลิขสิทธิ์ หากหน่วยงานใดมีการใช้งาน ให้หน่วยงานนั้นทำทะเบียนการใช้งานไว้ที่หน่วยงาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและทรัพย์สินของ สป.พน. เพื่อประโยชน์ในการค้นหาติดตามและสำรวจช่องโหว่ที่อาจมีผลกระทบต่อความมั่นคงปลอดภัยในระบบสารสนเทศ

๒.๑.๓ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ซอฟต์แวร์ ต้องกำหนดให้มีหน่วยงานเป็นผู้รับผิดชอบ และหน่วยงานที่เช่า จะต้องจัดทำบัญชีรายการของอุปกรณ์ ซอฟต์แวร์ หรือระบบงานคอมพิวเตอร์ที่เช่ามาใช้งาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและทรัพย์สินของ สป.พน.

๒.๑.๔ สื่อบันทึกหรือบรรจุข้อมูล ทั้งกรณีที่เป็นทรัพย์สินของ สป.พน. หากหน่วยงานใดมีการใช้สื่อเพื่อบันทึกข้อมูลที่มีการกำหนดชั้นความลับ ชั้นลับที่สุด หรือ ชั้นลับมาก หรือ ชั้นลับ หน่วยงานนั้นจะต้องมีการทำบัญชีควบคุมการใช้งานเพื่อระบุผู้รับผิดชอบและป้องกันไม่ให้รั่วไหล

๒.๒ การตรวจสอบบัญชีทรัพย์สิน ผู้อำนวยการแต่ละหน่วยงาน ต้องจัดให้มีการตรวจสอบบัญชีทรัพย์สินตามระยะเวลาที่กำหนดไว้ ได้แก่ เดือนละครั้ง (สำหรับระบบสำคัญ) หรือปีละครั้ง (สำหรับระบบการใช้งานทั่วไป)

๒.๓ การจัดหมวดหมู่ข้อมูลและสารสนเทศ)

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

๒.๓.๒ เอกสารหรือสิ่งตีพิมพ์ ที่พิมพ์หรือทำซ้ำขึ้นมาจากข้อมูลดิจิทัลหรือสารสนเทศดิจิทัล ซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับข้อมูลดิจิทัลหรือสารสนเทศดิจิทัลนั้น ยกเว้นว่ามีการจัดลำดับชั้นความลับใหม่โดยหน่วยงานผู้ผลิตเอกสารหรือสิ่งพิมพ์นั้น

๒.๓.๓ ผู้อำนวยการแต่ละหน่วยงาน ต้องทำการจัดหมวดหมู่ กำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันสารสนเทศของ สป.พน. ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดย สป.พน. จัดให้มีกระบวนการในการจัดหมวดหมู่ของข้อมูลและทรัพย์สิน ได้แก่ ชั้นลับที่สุด ชั้นลับมากและชั้นลับ การกำหนดแนวทางการแบ่งชั้นความลับของข้อมูล ต้องอยู่ในการควบคุมดูแลและรักษาความปลอดภัยที่เหมาะสมไม่ว่าจะอยู่ในรูปแบบใดก็ตาม

๒.๓.๔ ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การเก็บรักษา จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้ เจ้าหน้าที่ ของ สป.พน. ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

๒.๓.๕ การใช้งานและการเข้าถึงเอกสารสำคัญ บุคคลที่ได้รับการระบุชื่อให้มีสิทธิ์เข้าถึงเอกสารชั้นความลับให้เข้าถึงเอกสารในเวลาราชการ โดยเข้าถึง คือ ๐๘.๓๐ – ๑๖.๓๐ น. หรือนอกเวลาราชการตามสิทธิ์ที่ได้รับมอบหมาย และเข้าถึงเอกสาร ณ สป.พน. เท่านั้น

๒.๔ การจัดทำป้ายชื่อ ข้อมูล และสารสนเทศ

๒.๔.๑ ผู้อำนวยการแต่ละหน่วยงาน ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับข้อมูลและสารสนเทศ โดยแยกตามหมวดหมู่ที่กำหนดไว้ มีการส่งมอบและจัดเก็บ ตามขั้นตอนกระบวนการต่าง ๆ ซึ่งประกอบไปด้วย การถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสาร และการทำลาย มีแนวทางปฏิบัติ ดังนี้

๒.๔.๑.๑ ข้อมูลที่อยู่ ชั้นลับที่สุด ทั้งฉบับจริงและสำเนาต้องมีการระบุถึงระดับความปลอดภัยของข้อมูลในเอกสารตรงบริเวณส่วนหัวและ/หรือส่วนท้ายของเอกสารทุกหน้า

๒.๔.๑.๒ การนำส่งเอกสารข้อมูล ชั้นลับที่สุด ต้องใส่ซองเอกสารลับเฉพาะที่ไม่สามารถเห็นถึงเนื้อหาของเอกสารที่บรรจุภายในและปิดผนึก ลงชื่อของผู้รับอย่างชัดเจน

๒.๔.๑.๓ ข้อมูลที่อยู่ ชั้นลับที่สุด ต้องมีการจัดเก็บในลิ้นชักหรือตู้ที่มีการล็อก หรือห้องที่มีการออกแบบพิเศษสำหรับการเก็บรักษาเอกสารเหล่านี้โดยเฉพาะ 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 ซองซ้อนเช่นเดียวกัน โดยซองด้านในระบุถึงชื่อและประเภทของข้อมูลอย่างชัดเจน ส่วนซองด้านนอกจะระบุถึงชื่อและที่อยู่ของผู้รับเท่านั้น

๒.๔.๑.๘ ข้อมูล ชั้นลับมาก ต้องส่งให้ถึงมือผู้รับที่ระบุเท่านั้นและต้องมีลายเซ็นของผู้รับระบุว่าได้รับเอกสารแล้ว

๒.๔.๑.๙ การทำสำเนาเอกสารข้อมูลที่อยู่ ชั้นลับมาก ต้องได้รับการอนุมัติจากผู้อำนวยการ เท่านั้น

๒.๔.๑.๑๐ ข้อมูลที่อยู่ ชั้นลับมาก ต้องถูกจัดพิมพ์จากเครื่องพิมพ์ที่เชื่อมโยงกับระบบเครือข่ายที่สามารถควบคุมการใช้ได้เพื่อป้องกันการอ่าน เปลี่ยนแปลง หรือ ลบข้อมูลได้จากผู้ที่ไม่ได้รับอนุญาต

๒.๔.๑.๑๑ เอกสารข้อมูล ชั้นลับที่สุด ชั้นลับมาก และชั้นลับที่ไม่ได้นำมาใช้แล้วต้องถูกรวบรวม ขีดฆ่า และทำเครื่องหมายทำลายได้ และนำเอกสารไปทำลายเพื่อไม่ให้สามารถอ่านหรือนำมาใช้ได้อีกโดยการฉีกหรือเผาทำลาย

หมวด ๕
การควบคุมการเข้าถึง
(Access Control)

จุดประสงค์ เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร โดยประกอบด้วย

- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ**
- **การบริหารจัดการรหัสผ่าน**
- **การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร**

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๑. วัตถุประสงค์

นโยบายนี้ ระบุถึงข้อกำหนดเพื่อควบคุมสำหรับการเข้าถึงระบบสารสนเทศของ สป.พน. เพื่อให้มีความมั่นคงปลอดภัยและป้องกันไม่ให้ผู้ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้

๒. กระบวนการความมั่นคงปลอดภัยสารสนเทศของการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๒.๑ สถานที่ตั้งของระบบสารสนเทศที่สำคัญ ต้องมีการควบคุมการเข้าออกที่รัดกุมและให้เฉพาะบุคคลที่ได้รับอนุญาตและมีความจำเป็นเท่านั้นสามารถเข้าใช้งานได้ เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์บางอย่างของสำนักงานที่ไม่มีเจ้าหน้าที่ ดูแล

๒.๒ ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบและข้อมูลให้เหมาะสมกับการใช้บริการและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิอย่างสม่ำเสมอ

๒.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงบริการได้

๒.๔ ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของ สป.พน. และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลที่สำคัญ ทั้งนี้ ผู้ที่สามารถใช้ซอฟต์แวร์หรือฮาร์ดแวร์ในการตรวจตราและเฝ้าระวังในระบบเครือข่ายหรือระบบงานใด ๆ ต้องเป็นผู้ที่ได้รับอนุญาตจากหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยสารสนเทศและนโยบายฯ อย่างถูกต้องเท่านั้น

๒.๕ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ หากมีปัญหาเกิดขึ้น

๒.๖ ในการขออนุญาตเข้าสู่ระบบงานต่าง ๆ จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ กำหนดให้มีการลงนามอนุมัติและเก็บเอกสารดังกล่าวไว้เป็นหลักฐาน

๒.๗ เจ้าของข้อมูลและสารสนเทศและเจ้าของระบบงานนั้น ๆ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๒.๘ ในกรณีที่บุคลากรต้องการที่จะใช้ข้อมูลหรือระบบสารสนเทศที่ไม่เคยมีสิทธิในการใช้งานมาก่อน บุคลากรผู้นั้นจะต้องได้รับอนุญาตจากผู้บังคับบัญชาและเจ้าของข้อมูลหรือระบบสารสนเทศก่อน

๒.๙ ต้องปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

แนวทางการปฏิบัติ : การตั้งค่าของระบบที่ผ่านเข้าสู่ข้อมูล ให้ผู้ดูแลระบบเป็นผู้กำหนดตั้งค่าของระบบตามระดับชั้นความลับที่เหมาะสม

๓. การบริหารจัดการการเข้าถึงระบบของผู้ใช้งาน

๓.๑ การลงทะเบียนผู้ใช้งาน

ผู้อำนวยการกองแต่ละหน่วยงานและหัวหน้าหน่วยงานดูแลรับผิดชอบการบริหารงานบุคคลและสวัสดิการ ต้องร่วมกันจัดทำระเบียบปฏิบัติในการลงทะเบียนผู้ใช้งานใหม่ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ นอกจากนี้ ต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้งานทันที ในกรณีที่มีการลาออกหรือเปลี่ยนตำแหน่งงานภายใน สป.พน

๓.๒. การบริหารจัดการสิทธิการใช้งานระบบ

๓.๒.๑ ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน เช่น การกำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศตามความจำเป็นขั้นต่ำเท่านั้น

๓.๒.๒ ผู้ใช้งานต้องได้รับการอนุมัติสิทธิให้เสร็จสมบูรณ์ก่อน จึงสามารถเข้าใช้งานระบบได้

๓.๓ การบริหารจัดการรหัสผ่านของผู้ใช้งาน

เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ ผู้ใช้งานต้องปฏิบัติตามนโยบายการบริหารจัดการรหัสผ่าน

๓.๔ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

ผู้ดูแลระบบ เจ้าของข้อมูลและสารสนเทศและเจ้าของระบบงาน ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่เหมาะสม โดยต้องมีการสอบทานความเหมาะสมของสิทธิของผู้ใช้งานในการเข้าใช้ข้อมูลอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔. การควบคุมการเข้าถึงเครือข่าย

เพื่อป้องกันการเข้าถึงหรือควบคุมการใช้งานสารสนเทศจากผู้ที่ไม่ได้รับอนุญาต ต้องพิจารณาดังต่อไปนี้

๔.๑ ในกรณีที่อนุญาตให้ Protocol บางประเภทสามารถเข้าถึงระบบเครือข่ายของ สป.พน. จะต้องมีมาตรการการป้องกันล่วงหน้าและขั้นตอนการปฏิบัติงานโดยเฉพาะ

๔.๒ แม้ว่าจะมีการติดตั้ง Router และ Firewall อย่างปลอดภัยแล้วก็ตาม การแก้ไขในภายหลังอาจก่อให้เกิดความเสี่ยงต่อระบบงานได้ เพื่อลดความเสี่ยงต่าง ๆ ทุกครั้งที่มีการเปลี่ยนแปลง Router และ Firewall จะต้องปฏิบัติตามนโยบายการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ

๔.๓ ต้องไม่กำหนดให้ทำ Packet Forwarding หรือ Re-routing สำหรับ Server ที่มีการติดตั้ง Protocol ที่สามารถทำได้ เช่น กำหนดให้ FTP ไม่สามารถทำ IP Forwarding หรือ Passive FTP mode ได้

๔.๔ หมายเลขเครือข่ายภายใน (Internal Network Address) ของ สป.พน. ต้องมีการป้องกัน มิให้ส่วนงานที่เชื่อมต่อจากภายนอกสามารถมองเห็นได้ เพื่อป้องกันไม่ให้ Hackers หรือหน่วยงานภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบงานเครือข่ายและส่วนประกอบของคอมพิวเตอร์ของ สป.พน. ได้

๔.๕ สำหรับข้อมูลที่ผ่านเข้าและส่งออกจากระบบเครือข่าย สป.พน. ต้องส่งข้อมูลผ่าน Firewall เพื่อป้องกันการเชื่อมต่อจากผู้ที่ไม่ได้รับอนุญาต โดยกำหนดให้ผู้ดูแลระบบเครือข่ายเป็นผู้อนุมัติการเชื่อมต่อระบบเครือข่ายจากภายนอกของ สป.พน.

๔.๖ การเข้าสู่ระบบเครือข่ายของ สป.พน. ผ่านอินเทอร์เน็ต จะต้องมีการพิสูจน์ตัวตนและได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านระบบสารสนเทศก่อน

๔.๗ ระบบเครือข่ายทั้งหมดของ สป.พน. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก สป.พน. ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับซอฟต์แวร์ประสงค์ร้าย (Malware) ด้วย

๔.๘ ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายัง สป.พน. และต้องกำหนดให้การเชื่อมต่อนี้เข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เท่านั้น โดยกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของ สป.พน. ทั้งด้าน Physical และ Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่าย สป.พน. ได้โดยอิสระ

๔.๙ ผู้ดูแลระบบต้องจัดแบ่งระหว่างเครือข่ายภายในและเครือข่ายภายนอก (Segregation in Networks) โดยพิจารณาจากบริการเครือข่ายของกลุ่มผู้ใช้งานทั้งสองฝ่าย

๔.๑๐ ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อบนเครือข่ายมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว เพื่อจำกัดสิทธิในการใช้งานระบบสารสนเทศของ สป.พน.

๕. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก สป.พน.

ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก สป.พน. สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของ สป.พน. ได้ ดังนี้

๕.๑ ผู้ใช้งานทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบก่อน

๕.๒ การเข้าสู่ระบบของ สป.พน. ต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย ๑ วิธี เช่น การตรวจสอบการเข้าสู่ระบบโดยใช้ชื่อผู้ใช้และรหัสผ่าน เป็นต้น

๕.๓ ต้องแจ้งเป็นลายลักษณ์อักษรให้กับบุคคลที่ใช้บริการด้านสารสนเทศตามสัญญาถึงความสำคัญที่มีต่อการรักษาความปลอดภัยของข้อมูลสารสนเทศ ซึ่งแต่ละบุคคลต้องลงนามในเอกสารสัญญาเรื่องการไม่เปิดเผยข้อมูลของ สป.พน. และจัดเก็บเอกสารไว้ในแฟ้มสัญญา

๕.๔ การเข้าสู่ระบบของ สป.พน. จากอินเทอร์เน็ตหรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องตรวจสอบผู้ใช้งานจากสิ่งที่รู้อยู่ ได้แก่ ชื่อผู้ใช้ รหัสผ่าน และเพื่อเพิ่มความปลอดภัยจะต้องมีการเข้ารหัส (Cryptographic) การเข้าสู่ระบบจากระยะไกลร่วมกันกับการควบคุม

๖. ความมั่นคงปลอดภัยสำหรับการให้บริการเครือข่าย

ผู้อำนวยการกองแต่ละหน่วยงานและผู้ดูแลระบบ ต้องจัดทำข้อกำหนดหรือสัญญาด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่าง สป.พน. กับเจ้าหน้าที่ ซึ่งมีแนวทางปฏิบัติดังนี้

๖.๑ ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิของผู้ใช้งานเพื่อควบคุม เจ้าหน้าที่ ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๖.๒ ผู้ดูแลระบบต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๖.๓ ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ เจ้าหน้าที่ สามารถใช้เส้นทางอื่น ๆ ได้

๖.๔ ระบบเครือข่ายทั้งหมดของ สป.พน. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก สป.พน. ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับซอฟต์แวร์ประสงค์ร้าย (Malware) ด้วย

๖.๕ ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายัง สป.พน. และต้องกำหนดให้การเชื่อมต่อนี้เข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เท่านั้น โดยต้องกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของ สป.พน. ทั้งทาง Physical และ Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่าย สป.พน. ได้โดยอิสระ

๗. การควบคุมการเข้าถึงระบบปฏิบัติการ

๗.๑ ผู้ดูแลระบบต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ โดยมีแนวทางปฏิบัติ ดังนี้

๗.๑.๑ แสดงข้อความเตือนว่าคอมพิวเตอร์ใช้งานโดยผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

๗.๑.๒ ตรวจสอบความถูกต้องของข้อมูลนำเข้าเฉพาะเมื่อการนำเข้าเสร็จสิ้นสมบูรณ์แล้ว ถ้ามีความผิดพลาด ระบบไม่แสดงว่าข้อมูลนำเข้าส่วนไหนไม่ถูกต้อง

๗.๑.๓ จำกัดจำนวนครั้งของการพยายามเข้าใช้ระบบ เช่น ระบบยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง เป็นต้น และพิจารณาเพิ่มเติมสำหรับประเด็นต่อไปนี้

- บันทึกการพยายามทั้งที่สำเร็จและไม่สำเร็จ
- หลังจาก Log On ผิดพลาด บังคับระยะเวลาทิ้งช่วงก่อนที่จะยอมให้ทำต่อไป
- ตัดการเชื่อมโยงเครือข่าย
- ส่งข้อความเตือนไปยังหน้าจอของระบบ ถ้าความพยายามในการ Log On เกินจำนวนครั้งมากที่สุดที่ยอมรับได้
- กำหนดรหัสผ่านที่มีคุณภาพ

๗.๑.๖ จำกัดจำนวนครั้งสูงสุดและต่ำสุด ถ้าเกินกว่านั้นระบบต้องหยุดการให้ Log On

๗.๑.๗ แสดงข้อมูลต่อไปนี้หลังจากที่ Log On สำเร็จ

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

๗.๒ ผู้ดูแลระบบต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ โดยมีแนวทางปฏิบัติดังนี้

๗.๒.๑ บังคับใช้สำหรับผู้ใช้งานทุกประเภท

๗.๒.๒ User ID ของผู้ใช้งานต้องสามารถตรวจสอบร่องรอยกิจกรรมของผู้ใช้งานแต่ละคนได้ในภายหลัง

๗.๒.๓ กิจกรรมงานประจำของผู้ดูแลระบบต้องไม่ดำเนินการโดยผู้ใช้งานที่ได้สิทธิพิเศษ

๗.๒.๔ กรณีที่จำเป็นต้องมีการใช้งาน User ID ร่วมสำหรับกลุ่มของผู้ใช้งานหรือในเฉพาะบางงาน ในกรณีดังกล่าวต้องมีการจัดทำเอกสารอนุมัติรับรองจากผู้บริหารหรือผู้ที่ได้รับมอบหมาย

๗.๒.๕ ต้องกำหนดตัวควบคุมอื่นเพิ่มเติม เพื่อให้รับผิดชอบต่อข้อมูลในกรณีใช้ User ID ร่วมกัน

๗.๒.๖ การใช้ User ID ร่วมดังกล่าว ถูกใช้เฉพาะกรณีที่การใช้งานนั้นไม่จำเป็นต้องบันทึกประวัติการใช้งาน (ได้แก่ การดูอย่างเดียว เป็นต้น) หรือในกรณีที่มีการควบคุมอื่นควบคู่ไปด้วย เช่น อนุญาตให้เข้าใช้เพียงครั้งเดียว

๗.๒.๗ กรณีที่จำเป็นต้องตรวจยืนยันตัวตนอย่างเข้มงวด อาจใช้วิธีอื่นแทนการใช้รหัสผ่านในการตรวจยืนยันตัวตนได้ เช่นวิธีการใช้การเข้ารหัสเพื่อรักษาความลับ สมาร์ทการ์ด โทเค่น หรือวิธีการทางไบโอเมตริก

๗.๓ ผู้ดูแลระบบต้องจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพตามนโยบายการบริหารจัดการรหัสผ่าน

๗.๔ ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว มีแนวทางปฏิบัติดังนี้

๗.๔.๑ การใช้ยูทิลิตี้ต้องมีการระบุตัวตน ตรวจสอบยืนยัน และการควบคุมสิทธิของผู้ใช้งาน

๗.๔.๒ แยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมประยุกต์

๗.๔.๓ จำกัดการใช้งานของระบบยูทิลิตี้ให้เฉพาะสำหรับผู้ใช้งานที่จำเป็น

๗.๔.๔ การให้สิทธิการใช้ยูทิลิตี้แบบเฉพาะกิจ

๗.๔.๕ ต้องจำกัดสิทธิการใช้งานระบบยูทิลิตี้

๗.๔.๖ บันทึกประวัติการใช้งานของระบบยูทิลิตี้

๗.๔.๗ นิยามและจัดทำเอกสารระดับการให้สิทธิการเข้าถึงระบบยูทิลิตี้

๗.๔.๘ การยกเลิกระบบยูทิลิตี้ที่ไม่ได้ใช้งานหรือไม่จำเป็น

๗.๔.๙ ไม่ให้สิทธิการใช้ยูทิลิตี้กับผู้ใช้งานที่มีสิทธิเข้าถึงระบบโปรแกรมประยุกต์

๗.๕ ผู้ดูแลระบบต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้งานเมื่อไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้ มีแนวทางปฏิบัติดังนี้

๗.๕.๑ มีกลไกในการเคลียร์ Session เมื่อไม่ได้ใช้งานเป็นระยะเวลา ๑ ชั่วโมง (Time-out)

๗.๕.๒ Time-out ต้องกำหนดให้เหมาะสมกับความเสี่ยงนั้น ประเภทข้อมูลที่เกี่ยวข้องและระบบซอฟต์แวร์นั้น ๆ

๗.๖ ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง โดยมีแนวทางปฏิบัติดังนี้

๗.๖.๑ ตัดการเชื่อมต่อเมื่อใช้งานได้ระยะหนึ่ง ซึ่งได้กำหนดไว้ล่วงหน้า

๗.๖.๒ จำกัดการเชื่อมต่อเครือข่ายให้เฉพาะภายในระยะเวลาทำการ

๗.๖.๓ ให้ตรวจสอบยืนยันตัวตนใหม่ทุกช่วงเวลาที่กำหนด

๘. การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ

๘.๑ ผู้ดูแลระบบต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอปพลิเคชันตามนโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ โดยต้องแยกตามประเภทของผู้ใช้งาน การจำกัดสิทธิของผู้ใช้งานโดยพิจารณาอยู่บนพื้นฐานความจำเป็นของระบบซอฟต์แวร์แต่ละระบบ โดยมีแนวทางปฏิบัติ ดังนี้

๘.๑.๑ เตรียมหน้าจอหรือเมนูสำหรับควบคุมการเข้าถึงระบบ

๘.๑.๒ ควบคุมสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน

๘.๑.๓ ควบคุมสิทธิการเข้าถึงข้อมูลของระบบซอฟต์แวร์อื่น

๘.๑.๔ สร้างความแน่ใจให้ได้ว่าข้อมูลที่สำคัญจะถูกแสดงในหน้าจอที่ปลอดภัยและเหมาะสม

๘.๒ เจ้าของระบบงานต้องแยกระบบสารสนเทศที่มีความสำคัญสูง และระบบซึ่งไวต่อการรบกวนไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ มีแนวทางปฏิบัติดังนี้

๘.๒.๑ ความสำคัญ (Sensitivity) ของระบบโปรแกรมประยุกต์ ต้องมีการระบุอย่างชัดเจนและจัดทำเป็นเอกสารโดยเจ้าของระบบ และกำหนดสิทธิการเข้าถึงระบบ

๘.๒.๒ เมื่อจำเป็นต้องใช้ระบบร่วมกันกับระบบอื่นหรือผู้ใช้งานอื่น จะต้องมีการระบุความเสี่ยงและมีการยอมรับโดยเจ้าของระบบนั้น

๘.๓ ให้ผู้ใช้งานและบุคลากรฝ่ายสนับสนุนภายในหน่วยงาน เข้าใช้สารสนเทศและฟังก์ชัน (Function) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชั่นเท่าที่จำเป็นโดยต้องได้รับอนุญาตจากผู้ดูแลระบบก่อน โดยมีมาตรการควบคุมผู้ใช้ภายนอก ดังนี้

๘.๓.๑ ในกรณีการจ้างเหมาดำเนินการพัฒนาระบบและบำรุงรักษาระบบให้ผู้ใช้ภายนอกเข้าใช้งานสารสนเทศและฟังก์ชันต่าง ๆ เท่าที่จำเป็น โดยต้องได้รับอนุญาตก่อน

๘.๓.๒ ในกรณีการจ้างเหมาดำเนินการพัฒนาระบบและบำรุงรักษาระบบให้ผู้ใช้ภายนอกต้องควบคุมและจำกัดการนำข้อมูลออกจากระบบงาน

การบริหารจัดการรหัสผ่าน

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการใช้รหัสผ่าน

๒. การบริหารจัดการรหัสผ่าน

๒.๑ รหัสผ่านเป็นวิธีพื้นฐานในการระบุตัวตน ดังนั้น จึงต้องมีการควบคุมที่เข้มงวดเพื่อให้มั่นใจว่าผู้ที่เข้ามาใช้ระบบนั้นคือบุคคลที่มีสิทธิเข้าสู่ระบบข้อมูลของ สป.พน. จริง

๒.๒ ผู้ใช้งานระบบต้องลงนามยินยอมในสัญญาเรื่องการเก็บรักษารหัสผ่านไว้เป็นความลับ ซึ่งข้อความดังกล่าวรวมอยู่ในเงื่อนไขการจ้างงาน

๒.๓ สำหรับผู้ใช้งานรายใหม่จะได้รับรหัสผ่านเริ่มแรกในการผ่านเข้าระบบและเมื่อมีการเข้าสู่ระบบในครั้งแรก ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที และต้องเปลี่ยนรหัสผ่านตามระยะเวลา ได้แก่ อย่างน้อยทุก ๓ เดือน

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 ได้แก่ มีการแนะนำว่ารหัสผ่านที่ผู้ใช้งานกำหนดนั้นสามารถคาดเดาได้ง่าย หรือคาดเดาได้ยาก เป็นต้น

๒.๙ บันทึกประวัติการเปลี่ยนรหัสผ่านเพื่อป้องกันการใช้ซ้ำ

๒.๑๐ ต้องไม่แสดงรหัสผ่านที่พิมพ์ลงไปหรือซ่อนไม่ให้มองเห็นหรือเข้าใจได้

๓. การใช้งานรหัสผ่าน

๓.๑ เก็บรหัสผ่านไว้เป็นความลับ

๓.๒ ต้องไม่เก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ในรูปแบบที่สามารถอ่านได้ หรือไม่เก็บรักษารหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถเห็นหรือเข้าถึงได้ง่าย ได้แก่ บนเครื่องคอมพิวเตอร์ บนโต๊ะทำงาน เป็นต้น และต้องเก็บข้อมูลรหัสผ่านไว้ต่างหากจากข้อมูลอื่น

๓.๓ ไม่พิมพ์รหัสผ่านในขณะที่มีผู้อื่นเห็นการพิมพ์ดังกล่าว

๓.๔ ไม่ทำการใด ๆ เพื่อให้ตนเองทราบถึงบัญชีผู้ใช้งานหรือรหัสผ่านของผู้อื่น

๓.๕ เปลี่ยนรหัสผ่านส่วนของตนเองในครั้งแรกของการใช้งานผ่านระบบ ไม่ว่าระบบจะบังคับให้มีการเปลี่ยนรหัสผ่านหรือไม่ก็ตาม และไม่ตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิม

๓.๖ หากมีเหตุที่น่าเชื่อถือได้ ผู้ใช้งานรายงานเหตุการณ์ที่สงสัยว่ามีการเปิดเผยรหัสผ่านไปยังผู้ดูแลระบบ และให้ดำเนินการเปลี่ยนรหัสผ่านทันที

๓.๗ ถ้าพบว่า รหัสผ่านของตนถูกล็อกโดยไม่ทราบสาเหตุ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบ

๓.๘ ในกรณีที่ได้รับความช่วยเหลือในการแก้ไขปัญหาและต้องการให้ใส่รหัสผ่าน ผู้ใช้งานต้องไม่ให้รหัสผ่านแก่ผู้ช่วยเหลือ และต้องใส่รหัสผ่านด้วยตนเอง

๔. การกำหนดรหัสผ่าน

๔.๑ การกำหนดรหัสผ่านต้องไม่ใช้คำศัพท์ที่มาจากพจนานุกรม ชื่อหนัง ชื่อสถานที่หรือชื่อสิ่งลึกลับ และต้องไม่ใช้ข้อมูลที่เกี่ยวข้องกับ สป.พน. หรือเป็นข้อมูลส่วนตัวของผู้ใช้งานซึ่งง่ายต่อการคาดเดา (เช่น รหัสเจ้าหน้าที่, ที่อยู่, ชื่อบุคคลในครอบครัว เป็นต้น)

๔.๒ ต้องไม่กำหนดรหัสผ่านที่ประกอบด้วยตัวอักษรหรือตัวเลขที่เรียงซ้ำกันเกินกว่า ๓ ตัว หรือเรียงกันตามลำดับ เช่น aaaabbbb, 44444444, abcdefg

๔.๓ รหัสผ่านที่ดีมีลักษณะดังนี้

๔.๓.๑ มีความยาวอย่างน้อย ๘ ตัวอักษรหรือตามที่ผู้ดูแลระบบกำหนด

๔.๓.๒ มีส่วนประกอบของอักษร อักขระพิเศษ หรือตัวเลขประสมกันตามลักษณะ ดังนี้

๔.๓.๒.๑. ตัวอักษรใหญ่ เช่น A, B, C, ...

๔.๓.๒.๒. ตัวอักษรเล็ก เช่น a, b, c, ...

๔.๓.๒.๓. ตัวเลข เช่น 0, 1, 2, ...

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

๕. การเปลี่ยนรหัสผ่าน

๕.๑ รหัสผ่านเข้าสู่ระบบ (เช่น root, NT Admin เป็นต้น) ต้องเปลี่ยนอย่างน้อยทุก ๓ เดือน

๕.๒ รหัสผ่านของระบบที่ให้บริการจะต้องเป็นส่วนหนึ่งของการจัดการฐานข้อมูลรหัสผ่านส่วนกลาง

๕.๓ รหัสผ่านของผู้ใช้งานต้องเปลี่ยนอย่างน้อยทุก ๓ เดือน

๖. การยกเลิกรหัสผ่าน

รหัสผ่านของผู้ใช้งานที่ลาออก สิ้นสุดการจ้างงานหรือย้าย ต้องทำการยกเลิกสิทธิของผู้ใช้งานในระบบทันทีและลบชื่อผู้ใช้งานนั้นออกจากระบบทันที

การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอก

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

๒. อุปกรณ์สื่อสารประเภทพกพา

เพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น Notebook และ Laptop เป็นต้น) ต้องพิจารณาดังต่อไปนี้

๒.๑ ในกรณีที่มีการใช้งานเครื่องคอมพิวเตอร์แบบพกพาที่เป็นทรัพย์สินของ สป.พน. จะต้องปฏิบัติตามในการใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook Computer Policy) อย่างเคร่งครัด

๒.๒ อุปกรณ์สื่อสารประเภทพกพาที่ได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายและระบบคอมพิวเตอร์แล้วเท่านั้นที่จะสามารถเข้าถึงข้อมูลสารสนเทศของ สป.พน. ได้

๒.๓ อุปกรณ์สื่อสารประเภทพกพาจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อยโดยการใส่รหัสผ่านตามการบริหารจัดการรหัสผ่าน (Password Management Policy)

๒.๔ ไม่เก็บข้อมูลสำคัญของ สป.พน. ไว้บนอุปกรณ์สื่อสารประเภทพกพา แต่ถ้าไม่สามารถจัดเก็บบนเครื่องคอมพิวเตอร์ส่วนบุคคลของ สป.พน. ที่ใช้งานอยู่ได้ ข้อมูลที่จัดเก็บบนอุปกรณ์สื่อสารประเภทพกพา จะต้องมีการเข้ารหัสข้อมูลตามแนวทางการเข้ารหัสของ สป.พน.

๒.๕ ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

๒.๖ ผู้ใช้งานอุปกรณ์สื่อสารประเภทพกพา ต้องระวังการแอบดูข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต

๒.๗ ข้อมูลสำคัญของ สป.พน. จะต้องไม่ถูกส่งผ่านเครือข่ายไร้สายไปยังหรือจากอุปกรณ์สื่อสารประเภทพกพา ถ้าจะมีการส่งผ่านอย่างน้อยจะต้องเป็นวิธีการส่งข้อมูลผ่านเครือข่ายไร้สายที่ได้รับการอนุมัติแล้วตามแนวทางการเข้ารหัสของ สป.พน.

๒.๘ ข้อมูลที่มีชั้นความลับซึ่งถูกจัดเก็บไว้บนอุปกรณ์สื่อสารประเภทพกพาหรือถูกส่งผ่านเครือข่ายไร้สายที่ต้องส่งออกไปนอก สป.พน. ต้องผ่านการอนุมัติจากเจ้าของข้อมูลและสารสนเทศและเข้ารหัสข้อมูลก่อนเท่านั้น และไม่เคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูลและสารสนเทศ เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและสารสนเทศ และจะต้องกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว

๒.๙ ระบบคอมพิวเตอร์อื่นที่ต้องการเชื่อมต่อกับระบบของ สป.พน. จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายและระบบคอมพิวเตอร์

๒.๑๐ ต้องมีการรักษาความปลอดภัยทางกายภาพร่วมด้วย เช่น จะต้องปิดห้องทำงานเมื่อไม่มีบุคคลที่ได้รับอนุญาตอยู่โต๊ะทำงานและชั้นเก็บเอกสารต่าง ๆ จะต้องล็อกอย่างดี เป็นต้น

๒.๑๑ กรณีที่อุปกรณ์สื่อสารประเภทพกพาเป็นสมบัติของ สป.พน. การคืนเครื่องหรือส่งซ่อมให้ผู้ใช้งานทำสำเนาข้อมูลจากอุปกรณ์สื่อสารประเภทพกพาเก็บไว้ทั้งหมด และลบข้อมูลทั้งหมดที่มีอยู่บนอุปกรณ์สื่อสารประเภทพกพา ก่อนส่งให้หน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายและระบบคอมพิวเตอร์

๒.๑๒ อุปกรณ์สื่อสารประเภทพกพา ได้แก่ เครื่องคอมพิวเตอร์แบบพกพา (Notebook) ต้องอัปเดตระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ตามแนวปฏิบัติการใช้งานระบบป้องกันซอฟต์แวร์ประสงค์ร้าย (Malware) สำหรับเครื่องคอมพิวเตอร์ของ สป.พน.

๒.๑๓ หากผู้ใช้งานพ้นสภาพการเป็น เจ้าหน้าที่ ของ สป.พน. สิทธิของผู้ใช้งานในการเข้าถึงและใช้ข้อมูลสารสนเทศซึ่งเป็นความลับของผู้ใช้งานเป็นอันสิ้นสุดลงทันที

๒.๑๔ สป.พน. อาจดำเนินการทางวินัย แพ่ง หรืออาญา กับผู้ที่ละเมิดการเข้าถึง ใช้งาน หรือเผยแพร่ข้อมูลสารสนเทศที่เป็นความลับโดยที่ผู้นั้นไม่มีสิทธิอันชอบ

๓. การปฏิบัติงานจากภายนอกสำนักงาน

๓.๑ ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอก สป.พน. หน่วยงานที่รับผิดชอบต้องปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ สำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิที่ได้รับ และตรวจสอบการใช้งานอย่างสม่ำเสมอ

๓.๒ การเชื่อมต่อ Remote Access จะต้องมีการดำเนินการที่ได้รับการอนุมัติและเชื่อมต่อผ่านระบบ Virtual Private Network (VPN) ของ สป.พน. เท่านั้น

หมวด ๖
การเข้ารหัสข้อมูล
(Cryptography)

จุดประสงค์ เพื่อกำหนดให้มีการเข้ารหัสอย่างเหมาะสมและมีประสิทธิภาพ เพื่อป้องกันการเปิดเผยความลับของข้อมูล การปลอมแปลงข้อมูล และรักษาไว้ซึ่งความสมบูรณ์ถูกต้องของข้อมูล โดยมีการกำหนดแนวปฏิบัติและมาตรการการเข้ารหัสข้อมูล รวมถึงการบริหารจัดการกุญแจรหัสข้อมูล (Cryptography key) โดยมีแนวปฏิบัติ ดังนี้

- **แนวปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูล**

แนวปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูล

๑. วัตถุประสงค์

แนวปฏิบัตินี้กำหนดขึ้นเพื่อกำหนดแนวทางการเข้ารหัสข้อมูลและสารสนเทศให้มีความถูกต้องและมีประสิทธิภาพ เพื่อให้ได้มาซึ่งการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน ของข้อมูลและสารสนเทศขององค์กร

๒. มาตรการการเข้ารหัสข้อมูล

๒.๑ ผู้ดูแลระบบ ต้องกำหนดให้มีการเข้ารหัสข้อมูลตามมาตรฐานสากล ได้แก่ มาตรฐานขั้นตอนวิธี RSA, 3DES, AES, IDEA เป็นต้น และต้องดำเนินการเข้ารหัสให้สอดคล้องกับระดับชั้นความลับของข้อมูลและสารสนเทศ

๒.๒ ผู้ดูแลระบบ ต้องกำหนดมาตรฐานในการเข้ารหัสบริการด้านสารสนเทศ (Service) ได้แก่ บริการไปรษณีย์อิเล็กทรอนิกส์ (Pretty Good Privacy: PGP) บริการเว็บไซต์ (HTTP over SSL หรือ TLS) เป็นต้น

๒.๓ ผู้ดูแลระบบ ต้องทบทวนมาตรฐานขั้นตอนวิธีและกุญแจรหัสไม่น้อยกว่าปีละ ๑ ครั้ง เพื่อให้องค์กรสามารถป้องกันภัยคุกคามรูปแบบใหม่ที่อาจเกิดขึ้น

๓. การบริหารจัดการกุญแจรหัส

๓.๑ ผู้ดูแลระบบ ต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยในการบริหารจัดการกุญแจรหัส (Key Management) ในกระบวนการสร้าง การเปลี่ยน การจัดส่ง และการลบ โดยคำนึงถึงระดับชั้นความลับขององค์กร และระเบียบปฏิบัติการรักษาความลับทางราชการ

๓.๒ ผู้ดูแลระบบ ต้องเพิกถอนกุญแจรหัสส่วนตัว (Private Key) และกุญแจรหัสสาธารณะ (Public Key) ของผู้ใช้งานที่ถูกยกเลิกสิทธิพร้อมบันทึกเหตุผลของการเพิกถอน วันที่ เวลา ที่กุญแจรหัสถูกเพิกถอนตามแนวปฏิบัติการบริหารจัดการการเข้าถึงระบบของผู้ใช้งาน

๓.๓ ผู้ใช้งาน ต้องจัดเก็บกุญแจรหัสส่วนตัว (Private Key) ไว้เป็นความลับจากบุคคลที่ไม่ได้รับอนุญาตให้นำไปใช้งาน

๓.๔ การเปลี่ยนแปลงใด ๆ ของการบริหารจัดการกุญแจรหัสต้องปฏิบัติตามแนวปฏิบัติการบริหารจัดการการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ

หมวด ๗
ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security)

จุดประสงค์ เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ป้องกันทรัพย์สินสารสนเทศของ สป.พน. ไม่ให้เกิดการสูญหาย ถูกขโมย เกิดความเสียหาย เกิดการก่อกวนหรือแทรกแซง ป้องกันการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินของ สป.พน. และป้องกันไม่ให้กิจกรรมการดำเนินงานต่าง ๆ ของ สป.พน. เกิดการติดขัดหรือหยุดชะงัก เช่น การมีระบบกระแสไฟฟ้าสำรอง ระบบสื่อสารสำรอง เป็นต้น โดยมีนโยบาย ดังนี้

- **แนวปฏิบัติด้านความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม**
- **การควบคุมการเข้าออกศูนย์ข้อมูล (Data Center) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)**

แนวปฏิบัติด้านความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑. วัตถุประสงค์

เพื่อเป็นมาตรฐานในความมั่นคงปลอดภัยสารสนเทศทางกายภาพที่เกี่ยวกับสถานที่ ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นทรัพย์สินของ สป.พน. โดยนโยบายนี้มีผลบังคับใช้กับผู้ใช้งานและหน่วยงาน สป.พน. ซึ่งมีส่วนเกี่ยวข้องกับการใช้ระบบสารสนเทศของ สป.พน.

๒. มาตรฐานในการกำหนดบริเวณที่ต้องมีความมั่นคงปลอดภัยสารสนเทศ

๒.๑ ทุกหน่วยงาน ตั้งแต่ระดับกองขึ้นไป จะต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวัง ควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ และประกาศให้รับทราบทั่วกัน (ระบุให้ชัดเจนว่ามีพื้นที่ใช้งานระบบสารสนเทศกี่ประเภทและประเภทใดบ้าง)

๒.๒ ทุกหน่วยงานต้องกำหนดการติดตั้งอุปกรณ์ในพื้นที่ใช้งานระบบสารสนเทศให้สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูลและสารสนเทศที่มีอยู่ในระบบ

๒.๓ หน่วยงานที่รับผิดชอบอุปกรณ์ที่สำคัญของระบบสารสนเทศ ต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย ได้แก่ กล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถป้องกันภัยคุกคามจากผู้บุกรุก เป็นต้น ในพื้นที่ใช้งานระบบสารสนเทศของ สป.พน. ได้แก่ ห้อง Server/Data Center ห้อง Network Control ห้อง Network Center และห้องเก็บข้อมูลสำรอง เพื่อให้เป็นไปตามมาตรฐานสากลที่กำหนดไว้

๓. การควบคุมการเข้าออก

หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่ร่วมกับผู้อำนวยการกองที่เป็นเจ้าของระบบงานกำหนดมาตรการการควบคุมการเข้าออกในบริเวณพื้นที่ใช้งานระบบสารสนเทศ โดยให้ผ่านเข้าออกได้เฉพาะผู้ใช้งานที่มีสิทธิเท่านั้น ซึ่งมีแนวทางปฏิบัติ ดังนี้

๓.๑ ระบุตัวผู้ใช้งานและช่วงเวลาที่มีสิทธิผ่านเข้าออกในแต่ละพื้นที่อย่างชัดเจน

๓.๒ ผู้ใช้งานจะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนดเท่านั้น

๓.๓ หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตหรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้จะต้องแสดงบัตรประจำตัวที่ สป.พน. ออกให้ หรือบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่)

๔. ความมั่นคงปลอดภัยสารสนเทศสำหรับสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ

๔.๑ ผู้อำนวยการแต่ละหน่วยงาน ต้องจัดให้มีมาตรการความมั่นคงปลอดภัยสารสนเทศให้กับสำนักงาน ห้องทำงานและเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก สำนักงานจะต้อง **ไม่มีป้าย** หรือ **สัญลักษณ์** ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณดังกล่าว ประตูและหน้าต่างของสำนักงานต้องใส่กุญแจเมื่อไม่มีคนอยู่ เครื่องโทรสารหรือเครื่องถ่ายเอกสารต้องแยกออกมาจากบริเวณดังกล่าว เป็นต้น โดยมีแนวทางปฏิบัติ ได้แก่ กั้นพื้นที่อย่างรอบด้าน (เช่น ติดตั้งผนัง ติดตั้งเหล็กดัด ล็อกประตูที่ใช้ดอกกุญแจ หรือมีระบบ Access Control และปรับปรุงให้มีความเหมาะสมทางสภาวะแวดล้อม (เช่น ติดตั้งระบบปรับอากาศ การควบคุมความชื้น เป็นต้น)

๔.๒ การปฏิบัติงานในพื้นที่ควบคุม

๔.๒.๑ ผู้อำนวยการแต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม เช่น การไม่อนุญาตให้ถ่ายภาพหรือวิดีโอในบริเวณนั้น เป็นต้น

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

๔.๓ การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่ ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยหน่วยงานภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินของ สป.พน. โดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ต้องจัดเป็นบริเวณแยกออกมาต่างหาก

๔.๔ ความมั่นคงปลอดภัยของอุปกรณ์

๔.๔.๑ ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

๔.๔.๒ ผู้อำนวยการที่เป็นเจ้าของระบบงาน ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงปีละ ๑ ครั้ง หรือระบบที่สำคัญมากอาจจะกำหนดให้มีการบำรุงรักษาทุกสิ้นเดือน เป็นต้น

๔.๔.๓ ผู้อำนวยการแต่ละหน่วยงาน ต้องกำหนดให้มีการป้องกันทรัพย์สินและอุปกรณ์ของ สป.พน. ได้แก่ Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน โดยต้องปฏิบัติตามระเบียบในการใช้งานการยืม-คืน

๔.๔.๔ ผู้อำนวยการแต่ละหน่วยงาน ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ (Secure Disposal of Reuse of Equipment) ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น ทั้งนี้เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว ซึ่งมีแนวทางปฏิบัติ ดังนี้

ระดับชั้นความลับ	สื่อที่อ่านเขียนด้วยแสง (Optical Media)	สื่ออิเล็กทรอนิคส์ (Electronic Media)
๑ (ลับ)	สามารถทิ้งได้	สามารถทิ้งได้
๒ (ลับมาก)	ลบล้างข้อมูล หรือทำลายสื่อโดยอุปกรณ์ทำลายสื่อเฉพาะ	ลบล้างข้อมูล หรือทำลายสื่อโดยอุปกรณ์ทำลายสื่อเฉพาะ
๓ (ลับที่สุด)	ลบล้างข้อมูล และทำลายสื่อโดยอุปกรณ์ทำลายสื่อเฉพาะ	ลบล้างข้อมูล และทำลายสื่อโดยอุปกรณ์ทำลายสื่อเฉพาะ

๔.๕ ระบบกระแสไฟฟ้าสำรอง (Power Supplies) และระบบป้องกันภัย

ผู้อำนวยการแต่ละหน่วยงาน ต้องกำหนดให้มีระบบกระแสไฟฟ้าสำรอง สำหรับระบบที่สำคัญ โดยมีแนวทางปฏิบัติ ดังนี้

๔.๕.๑ ต้องมีระบบไฟฟ้าสำรองอัตโนมัติ เพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง และต้องมีการตรวจสอบระบบไฟฟ้าสำรองและบำรุงรักษาอย่างน้อยปีละ ๒ ครั้ง

๔.๕.๒ ต้องจัดให้มีระบบเตือนภัย/ป้องกันภัย เช่น ระบบดับเพลิง ระบบเตือนอัคคีภัย

๔.๕.๓ ต้องมีการวางแผน และซักซ้อมการปฏิบัติรับมือกับภัย เช่น อัคคีภัย อย่างน้อยปีละ ๑ ครั้ง

๔.๕.๔ ไม่กระทำการใด ๆ ให้เกิดมีประกายไฟหรือเปลวไฟ

๔.๕.๕ ระบบที่สำคัญของ สป.พน. จะต้องมีการปฏิบัติตามนโยบายแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ เพื่อป้องกันผลกระทบที่จะเกิดขึ้นกับการปฏิบัติราชการ

๔.๖ การเดินสายไฟฟ้าหลัก (Main Power Cable) และสายเคเบิลหลัก (Backbone Cable) หน่วยงานที่รับผิดชอบ จะต้องคำนึงถึงการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน เช่น ผ่านเข้ามาทางใต้ดิน ผ่านช่องพิเศษที่จัดไว้หรือเป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย ซึ่งมีแนวทางปฏิบัติ เป็นต้น เช่น บริเวณที่มีการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน และมีการติดตั้งตู้พักสาย ต้องล็อกไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่หรือบุคคลที่มีสิทธิเท่านั้น เป็นต้น

๔.๗ การควบคุมทั่วไป

๔.๗.๑ เจ้าหน้าที่ ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศที่เป็น ชั้นลับที่สุด หรือ ชั้นลับมาก ไว้ในที่สามารถพบเห็นได้ง่าย (Clear Desk) โดยจัดเก็บไว้ในที่ที่ปลอดภัย นอกจากนี้ ตู้จ่ายเอกสารหรือจดหมายและเครื่องโทรสารจะต้องได้รับการดูแลให้ปลอดภัยด้วย

๔.๗.๒ การเคลื่อนย้ายทรัพย์สินของ สป.พน. ผู้ดูแลระบบแต่ละหน่วยงาน ต้องทำเป็นบันทึกและขออนุญาตจากผู้อำนวยการกองอย่างถูกต้องในการเคลื่อนย้าย ซึ่งมีแนวทางปฏิบัติ ดังนี้

๔.๗.๒.๑ ผู้ที่รับผิดชอบในการย้ายสถานที่ทำงาน ต้องตรวจสอบความเรียบร้อยครั้งสุดท้ายทันทีหลังจากที่ทำการย้ายของเสร็จสิ้น รวมทั้งตรวจสอบพื้นที่และทรัพย์สินด้วย การย้ายสถานที่ทำงาน เป็นช่วงเวลาที่ต้องระวังเรื่องการรักษาความปลอดภัยที่อาจมีการมองข้ามได้ โดยเฉพาะช่วงเวลาที่ต้องเร่งจัดการย้ายให้เสร็จสิ้น จึงต้องให้ความระมัดระวัง เพราะอาจมีการผ่อนปรนมาตรการรักษาความปลอดภัยต่อข้อมูลที่มีความสำคัญหรือต่อระบบเครือข่ายของ สป.พน. ได้

๔.๗.๒.๒ ข้อมูลที่มีความสำคัญมาก รวมถึงข้อมูลในคอมพิวเตอร์แบบพกพา (Notebook) ต้องมีการเคลื่อนย้าย/ถ่ายโอนโดยผู้เป็นเจ้าของข้อมูลและสารสนเทศเท่านั้น ไม่เคลื่อนย้าย/ถ่ายโอนโดยบุคคลที่ไม่ใช่

เจ้าของข้อมูลและสารสนเทศ เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและสารสนเทศ

๔.๗.๒.๓ ผู้ใช้งานจะต้องแน่ใจว่าข้อมูลสำคัญใด ๆ ต้องมีการเข้ารหัสเมื่อถูกจัดเก็บอยู่ในฮาร์ดดิสก์

๔.๗.๒.๔ ผู้ที่มีส่วนร่วมในการเคลื่อนย้ายสถานที่ทำงานจะต้องมีการตรวจตราสถานที่ย้ายทรัพย์สินออก เพื่อให้มั่นใจได้ว่าไม่มีข้อมูลใดหลงเหลืออยู่ มีการกำหนดความรับผิดชอบในการดูแลให้ครอบคลุมส่วนที่เก็บเอกสาร (เช่น ตู้เก็บแฟ้มเอกสาร ห้องเก็บรักษาแฟ้มข้อมูล ห้องนิรภัย เป็นต้น)

๔.๗.๒.๕ ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลงหรือเคลื่อนย้าย เพื่อใช้เป็นข้อมูลในการควบคุมทรัพย์สินของ สป.พน.

การควบคุมการเข้าออกศูนย์ข้อมูลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ภายใน ศทส. เข้าถึง ล่วงรู้ แก้ไขเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ของ สป.พน. โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ เช่น เจ้าหน้าที่ ศทส. เจ้าหน้าที่ สป.พน. ผู้ติดต่อจากหน่วยงานภายนอก ที่มีความจำเป็นต้องเข้าออก ศทส. เป็นต้น

๒. กระบวนการควบคุมการเข้าออกศูนย์ข้อมูล ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)

๒.๑ ผู้ดูแลระบบศูนย์ข้อมูล ศทส. มีแนวทางปฏิบัติ ดังนี้

๒.๑.๑ จัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

๒.๑.๒ ทำการกำหนดสิทธิบุคคลในการเข้าออกศูนย์ข้อมูล ศทส. โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน ศทส. ได้แก่ เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

๒.๑.๓ สิทธิในการเข้าออกศูนย์ข้อมูล ศทส. ของ เจ้าหน้าที่ แต่ละคน ต้องได้รับการอนุมัติจากผู้มีอำนาจ โดยผ่านกระบวนการลงทะเบียนเป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายใน ศทส.

๒.๑.๔ เจ้าหน้าที่ และบุคคลภายนอก ทุกคนต้องลงทะเบียน เพื่อใช้ในการเข้าออกศูนย์ข้อมูล ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๑.๕ ต้องจัดทำระบบเก็บบันทึกการเข้าออกศูนย์ข้อมูล ศทส. โดยบันทึกดังกล่าว ต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก และต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

๒.๑.๖ ไม่อนุญาตให้ผู้ที่ไม่เกี่ยวข้องหรือผู้ที่ไม่ได้รับอนุญาตจาก ศทส. เข้าภายในศูนย์ข้อมูล ศทส.

๒.๑.๗ การเข้าถึงศูนย์ข้อมูล ศทส.ต้องมีการลงบันทึกตามแบบฟอร์มของ ศทส. ทั้งเข้าและออก พร้อมทั้งระบุเหตุผลในการเข้าใช้ห้องระบบปฏิบัติการคอมพิวเตอร์ และมีเจ้าหน้าที่ ศทส. ลงนามรับรองทุกครั้ง

๒.๑.๘ ตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้าออกศูนย์ข้อมูล ศทส. เป็นประจำทุกเดือน

๒.๑.๙ ต้องทำการทบทวนสิทธิของเจ้าหน้าที่ ศทส. ให้มีความถูกต้องอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๒.๒ เจ้าหน้าที่ และ**ผู้ติดต่อจากหน่วยงานภายนอก** มีแนวทางปฏิบัติ ดังนี้

๒.๒.๑ ลงทะเบียน เพื่อใช้ในการเข้าออกศูนย์ข้อมูล ศทส. ในสมุดบันทึก

๒.๒.๒ ในกรณีที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายใน ศูนย์ข้อมูล ศทส. ต้องแจ้งเจ้าหน้าที่ ศทส. และลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกของ ศทส. ให้ถูกต้องชัดเจน

๒.๒.๓ ต้องติดบัตรประจำตัวหรือบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจน ตลอดเวลาที่อยู่ในศูนย์ข้อมูล ศทส.

๒.๒.๔ สิทธิการเข้าออกศูนย์ข้อมูล ศทส. จะขึ้นอยู่กับเหตุผลความจำเป็นในการ ขอเข้าใช้พื้นที่ และสามารถเข้าได้เฉพาะพื้นที่ที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้าออกของ ศทส. เท่านั้น

๒.๒.๕ สามารถนำผู้ติดตามเข้ามาช่วยงานได้ไม่เกินครั้งละ ๒ คน ถ้าต้องการมากกว่านี้ต้องแจ้งเข้ามาเป็นลายลักษณ์อักษรล่วงหน้าก่อน ๒ วัน

หมวด ๘
ความมั่นคงปลอดภัยในการปฏิบัติงาน
(Operations Security)

จุดประสงค์ เพื่อให้การดำเนินงานของอุปกรณ์ที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องปลอดภัย โดยมีแนวปฏิบัติดังนี้

- **แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล**
- **แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา**
- **การใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่**
- **แนวปฏิบัติการควบคุมซอฟต์แวร์ปฏิบัติงาน**
- **แนวปฏิบัติการใช้งานระบบป้องกันซอฟต์แวร์ประสงค์ร้าย (Malware) สำหรับเครื่องคอมพิวเตอร์**
- **แนวปฏิบัติการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์**
- **แนวปฏิบัติการจัดการสื่อที่ใช้ในการบันทึกข้อมูล**
- **แนวปฏิบัติการเฝ้าระวังและบันทึกเหตุการณ์**

แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๑. วัตถุประสงค์

เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลที่เป็นทรัพย์สินขององค์กร และส่วนตัวที่ได้รับอนุญาตจากองค์กร เพื่อป้องกันข้อมูลและสารสนเทศที่สำคัญขององค์กร พร้อมทั้งช่วยให้ผู้ใช้งานทราบถึงบทบาทหน้าที่และความรับผิดชอบในการปฏิบัติงาน

๒. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล มีแนวทางปฏิบัติ ดังนี้

๒.๑ เครื่องคอมพิวเตอร์ที่ สป.พน. อนุญาตให้ผู้ใช้งานใช้งาน เป็นทรัพย์สินของ สป.พน. ดังนั้นผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ เพื่อใช้ในงานราชการ ของ สป.พน.

๒.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของ สป.พน. ต้องเป็นโปรแกรมที่ สป.พน. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย และอนุญาตให้ใช้งาน ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของ สป.พน.

๒.๔ ผู้ใช้งาน ต้องไม่ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ที่มีการทำงานกระทบต่อระบบส่วนกลาง

๒.๕ การตั้งชื่อเครื่องคอมพิวเตอร์ส่วนบุคคลจะต้องตั้งชื่อและกำหนดโดย ศทส. เท่านั้น

๒.๖ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อม จะต้องดำเนินการโดย ศทส. เท่านั้น

๒.๗ ก่อนใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อตรวจหาซอฟต์แวร์ประสงค์ร้าย (Malware) โดยโปรแกรมป้องกัน เช่น Flash Drive, SD Card, External Hard Drive เป็นต้น

๒.๘ ต้องเก็บข้อมูลสำคัญของ สป.พน. ไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานใช้งานอยู่

๒.๙ ไม่สร้างเส้นทางลัด (Shortcut) บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ สป.พน.

๒.๑๐ ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลและรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยปฏิบัติ ดังนี้

๒.๑๐.๑ ไม่รับประทานอาหารหรือนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณพื้นที่ติดตั้งเครื่องคอมพิวเตอร์

๒.๑๐.๒ ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์ หรือ Disk Drive

๓. การควบคุมการเข้าถึงระบบปฏิบัติการ มีแนวทางปฏิบัติ ดังนี้

๓.๑ ผู้ใช้งาน ต้องกำหนดชื่อผู้ใช้งาน (Login) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๓.๒ ผู้ใช้งาน ต้องตั้งเวลาประมาณ ๑๐ นาที หลังจากไม่มีการใช้งานอุปกรณ์คอมพิวเตอร์ ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

๓.๓ ผู้ใช้งาน ต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน และรหัสผ่านเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๓.๔ ในระหว่างเวลาพักกลางวัน และหลังเลิกงาน ผู้ใช้งาน ต้อง Log out ออกจากเครื่องคอมพิวเตอร์หรือทำการล็อกหน้าจอ

๔. การใช้รหัสผ่าน (Password) มีแนวทางปฏิบัติ ดังนี้ ผู้ใช้งาน ต้องกำหนดรหัสผ่าน ให้เป็นไปตามนโยบายการบริหารจัดการรหัสผ่าน

๕. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ มีแนวทางปฏิบัติ ดังนี้

๕.๑ ผู้ใช้งาน ต้องทำการปรับปรุง (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๕.๒ ผู้ใช้งาน ต้องตรวจสอบซอฟต์แวร์ประสงค์ร้าย (Malware) จากสื่อต่าง ๆ เช่น External Disk เป็นต้น ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๕.๓ ผู้ใช้งาน ตรวจสอบก่อนใช้งานไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากระบบเครือข่ายอินเทอร์เน็ตด้วยโปรแกรมป้องกันซอฟต์แวร์ประสงค์ร้าย (Malware)

๕.๔ ผู้ใช้งาน ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใด ๆ ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๖. การสำรองข้อมูลและการกู้คืนข้อมูล

ข้อมูลเป็นสิ่งที่มีความสำคัญต่อการดำเนินงาน จึงต้องมีการสำรองข้อมูลและการกู้คืนข้อมูลอย่างสม่ำเสมอ โดยมีแนวทางปฏิบัติ ดังนี้

๖.๑ ผู้ใช้งาน ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ส่วนบุคคลไว้บน สื่อบันทึกอื่น ๆ เช่น CD, External Hard disk เป็นต้น

๖.๒ ผู้ใช้งาน มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๖.๓ ผู้ใช้งาน ที่ต้องการเคลื่อนย้ายสื่อสำรองข้อมูลออกนอกสถานที่จะต้องมีการป้องกันการเข้าถึงข้อมูลอย่างมั่นคงปลอดภัย

๖.๔ สื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนข้อมูลสม่ำเสมอ

๖.๕ สื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๗. การนำครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกจาก สป.พน. มีแนวทางปฏิบัติ ดังนี้

๗.๑ ผู้ใช้งาน ที่จะนำครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกจาก สป.พน. จะต้องกรอกรายละเอียดตามแบบฟอร์มการนำทรัพย์สินออกนอกอาคารสถานที่ ให้ถูกต้องและครบถ้วนเท่านั้น ถึงจะอนุญาตให้นำออกครุภัณฑ์คอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงได้

๗.๒ ผู้ใช้งาน ที่นำครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกจาก สป.พน. จะต้องลงข้อมูลที่จำเป็นให้ครบถ้วนในแบบฟอร์มการนำทรัพย์สินออกนอกอาคารสถานที่และต้องได้รับอนุญาตจากผู้มีอำนาจพร้อมทั้งแนบสำเนาบัตรประจำตัวยืนยันตัวเองทุกครั้ง

๗.๓ ผู้ใช้งาน ต้องเก็บสำเนาแบบฟอร์มการนำทรัพย์สินออกนอกอาคารสถานที่ไว้ เพื่อเป็นหลักฐาน

๘. การบำรุงรักษาครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง มีแนวทางปฏิบัติ ดังนี้

๘.๑ ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงจะต้องขึ้นทะเบียนครุภัณฑ์เพื่อความสะดวกในการตรวจสอบและการบำรุงรักษา

๘.๒ ศทส. จะให้บริการเฉพาะครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง ที่ขึ้นทะเบียนครุภัณฑ์แล้วหรืออยู่ระหว่างการส่งมอบแล้วเท่านั้น

๘.๓ หากครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงเกิดการชำรุดเสียหาย ไม่สามารถใช้งานได้ทั้งด้านซอฟต์แวร์หรือฮาร์ดแวร์ ผู้ใช้งาน มีหน้าที่จะต้องแจ้งให้ ศทส. รับทราบเพื่อดำเนินการแก้ไขต่อไป

๘.๔ หากครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอยู่ในสัญญาหรือระยะเวลาการรับประกันเกิดการชำรุดเสียหาย ศทส. มีหน้าที่ติดต่อคู่สัญญาหรือผู้แทนจำหน่าย เพื่อดำเนินการตรวจซ่อมตามที่ระบุในสัญญา

๘.๕ หากครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอยู่นอกเหนือหรือพ้นระยะเวลาการรับประกัน ศทส. มีหน้าที่ตรวจสอบในเบื้องต้นและประสานกับกองเจ้าของครุภัณฑ์ในการดำเนินการซ่อมแซมต่อไป

แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพา และการนำไปปฏิบัติงานภายนอก สป.พน. เพื่อเป็นการป้องกันข้อมูล และอุปกรณ์ของ สป.พน. ให้เกิดความปลอดภัย ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ต้องหลีกเลี่ยง ในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

๒. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา มีแนวทางปฏิบัติ ดังนี้

๒.๑ เครื่องคอมพิวเตอร์แบบพกพาที่ สป.พน. อนุญาตให้ผู้ใช้งานใช้งานเป็นทรัพย์สินของ สป.พน. ดังนั้น ผู้ใช้งานต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างระมัดระวัง และใช้ในการทำงานของ สป.พน.

๒.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของ สป.พน. ต้องเป็นโปรแกรมที่ สปพน. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพา หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) แบบพกพาจะต้องกำหนดและตั้งชื่อโดย ศทส.

๒.๔ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดย ศทส.

๒.๕ ผู้ใช้งาน ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัย และมีประสิทธิภาพ

๒.๖ ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๒.๗ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ

๒.๘ ไม่ใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยน

๒.๙ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องเพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๒.๑๐ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD เครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๒.๑๑ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๒.๑๒ การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๒.๑๓ ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์ (Hard Disk) กำลังทำงาน

๒.๑๔ ต้องไม่ใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ

๒.๑๕ การใช้งานและการเก็บเครื่องคอมพิวเตอร์แบบพกพา ควรอยู่ในสภาพแวดล้อมที่มีอุณหภูมิที่ไม่สูงกว่า ๓๕ องศาเซลเซียส

๒.๑๖ ไม่วางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๒.๑๗ ไม่ติดตั้ง หรือวางเครื่องคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน ได้แก่ ในยานพาหนะที่กำลังเคลื่อนที่

๒.๑๘ การเช็ดทำความสะอาดหน้าจอภาพ ต้องเช็ดอย่างเบามือที่สุด และเช็ดไปในทิศทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วน

๓. ความปลอดภัยทางด้านกายภาพ มีแนวทางปฏิบัติ ดังนี้

๓.๑ ผู้ใช้งาน มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในสถานที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๓.๒ ผู้ใช้งาน ต้องไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระแทก

๓.๓ ผู้ใช้งาน ต้องไม่ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Components) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ และการใช้รหัสผ่าน (Password) มีแนวทางปฏิบัติดังนี้

๔.๑ ผู้ใช้งาน ต้องกำหนดชื่อผู้ใช้งาน (Login) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๔.๒ ผู้ใช้งาน ต้องกำหนดรหัสผ่าน ให้เป็นไปตามแนวทางการบริหารจัดการรหัสผ่าน

๔.๓ ผู้ใช้งาน ต้องตั้งเวลาประมาณ ๑๐ นาที หลังจากไม่มีการใช้งานอุปกรณ์คอมพิวเตอร์ ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

๔.๔ ผู้ใช้งาน ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๕. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ มีแนวทางปฏิบัติ ดังนี้

๕.๑ ผู้ใช้งาน ต้องทำการปรับปรุง (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๕.๒ ผู้ใช้งาน ต้องไม่ทำการปิดหรือยกเลิกระบบการป้องกันซอฟต์แวร์ประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

๕.๓ หาก ผู้ใช้งาน พบหรือสงสัย ว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ **ผู้ใช้งาน** ต้องไม่เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของซอฟต์แวร์ประสงค์ร้าย (Malware) ไปยังเครื่องคอมพิวเตอร์อื่น ๆ ได้

๖. การสำรองข้อมูลและการกู้คืนข้อมูล มีแนวทางปฏิบัติ ดังนี้

๖.๑ ผู้ใช้งาน ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา

๖.๒ ผู้ใช้งาน ต้องเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อเกิดการรั่วไหลข้อมูล

๖.๓ ผู้ใช้งาน ที่ต้องการเคลื่อนย้ายสื่อสำรองข้อมูลออกนอกสถานที่จะต้องมีการป้องกันการเข้าถึงข้อมูลอย่างมั่นคงปลอดภัย

๖.๔ สื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนข้อมูลสม่ำเสมอ

๖.๕ สื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๗. การบำรุงรักษาครุภัณฑ์คอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพา มีแนวทางปฏิบัติ ดังนี้

๗.๑ เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาจะต้องขึ้นทะเบียนครุภัณฑ์เพื่อความสะดวกในการตรวจสอบและการบำรุงรักษา

๗.๒ ศทส. จะให้บริการเฉพาะเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพา ที่ขึ้นทะเบียนครุภัณฑ์แล้วหรืออยู่ระหว่างการส่งมอบแล้วเท่านั้น

๗.๓ หากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาเกิดการชำรุดเสียหาย ไม่สามารถใช้งานได้ทั้งด้านซอฟต์แวร์หรือฮาร์ดแวร์ ผู้ใช้งาน มีหน้าที่จะต้องแจ้งให้ ศทส. รับทราบเพื่อดำเนินการแก้ไขต่อไป

๗.๔ หากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาอยู่ในสัญญาหรือระยะเวลาการรับประกันเกิดการชำรุดเสียหาย ศทส. มีหน้าที่ติดต่อคู่สัญญาหรือผู้แทนจำหน่าย เพื่อดำเนินการตรวจซ่อมตามที่ระบุในสัญญา

๗.๕ หากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาอยู่นอกเหนือหรือพ้นระยะเวลาการรับประกัน ศทส. มีหน้าที่ตรวจสอบในเบื้องต้นหรือประสานกับฝ่ายพัสดุในการดำเนินการซ่อมแซมต่อไป

การใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ เช่น คอมพิวเตอร์แท็ปเล็ต เป็นต้น และการควบคุมดูแลการนำอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ไปปฏิบัติงานภายนอก สป.พน. เพื่อเป็นการป้องกันข้อมูล และอุปกรณ์ของ สป.พน. ให้มีความมั่นคงปลอดภัย ผู้ใช้งาน จึงต้องรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ต้องหลีกเลี่ยง ในการใช้อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๒. การใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ มีแนวทางปฏิบัติ ดังนี้

๒.๑ อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ที่ สป.พน. อนุญาตให้ ผู้ใช้งาน ใช้งานเป็นทรัพย์สินของ สป.พน. ดังนั้นผู้ใช้งานจึงต้องใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่อย่างระมัดระวัง และเพื่องานราชการของ สป.พน.

๒.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ของ สป.พน. ต้องเป็นโปรแกรมที่ สป.พน. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย และอนุญาตให้ใช้งาน ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๓ การเคลื่อนย้ายหรือส่งอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ตรวจซ่อมจะต้องดำเนินการโดย ศทส.

๒.๔ ผู้ใช้งาน ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัย และมีประสิทธิภาพ

๒.๕ ผู้ใช้งาน ต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ และรักษาสภาพของอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ให้มีสภาพเดิม

๒.๖ ผู้ใช้งาน ต้องไม่ใส่อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยน

๒.๗ การใช้อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่เป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ผู้ใช้งาน ต้องปิดเครื่องเพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๒.๘ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๒.๙ ผู้ใช้งาน ต้องไม่ใช้ หรือวางอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ใกล้สิ่งที่เป็นของเหลวความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

๒.๑๐ การใช้งานและการเก็บอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ ต้องอยู่ในสภาพแวดล้อมที่มีอุณหภูมิที่ไม่สูงกว่า ๓๕ องศาเซลเซียส

๒.๑๑ ไม่วางอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ ได้แก่ แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๒.๑๒ การเช็ดทำความสะอาดหน้าจอภาพ ต้องเช็ดอย่างเบามือที่สุด และควรเช็ดไปในทิศทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วน

๓. ความปลอดภัยทางด้านกายภาพ มีแนวทางปฏิบัติ ดังนี้

๓.๑ ผู้ใช้งาน มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย และไม่วางเครื่องทิ้งไว้ในสถานที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๓.๒ ผู้ใช้งาน ไม่เก็บหรือใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระแทก

๓.๓ ผู้ใช้งาน ต้องไม่ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Components) ที่ติดตั้งอยู่ภายใน รวมถึงอุปกรณ์สำรองไฟฟ้า

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ และการใช้รหัสผ่าน (Password) มีแนวทางปฏิบัติดังนี้

๔.๑ ผู้ใช้งาน ต้องกำหนดชื่อผู้ใช้งาน (Login) และรหัสผ่าน (Password) ในการใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่

๔.๒ ผู้ใช้งาน ต้องกำหนดรหัสผ่าน ให้มีความยาวอย่างน้อย ๘ ตัวอักษรและมีส่วนประกอบของอักษร อักขระพิเศษและหรือตัวเลขประสมกัน

๔.๓ ผู้ใช้งาน ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ เชื่อมต่อกับระบบเครือข่ายของ สป.พน.

๕. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ มีแนวทางปฏิบัติ ดังนี้

๕.๑ ผู้ใช้งาน ต้องทำการปรับปรุง (Update) ระบบปฏิบัติการ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๕.๒ หาก ผู้ใช้งาน พบหรือสงสัย ว่าอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่มีการติดชุดคำสั่งไม่พึงประสงค์ **ผู้ใช้งาน** ต้องไม่เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของซอฟต์แวร์ประสงค์ร้าย (Malware) ไปยังเครื่องคอมพิวเตอร์อื่น ๆ ได้

๖. การสำรองข้อมูลและการกู้คืนข้อมูล มีแนวทางปฏิบัติ ดังนี้

๖.๑ ผู้ใช้งาน ต้องทำการสำรองข้อมูลจากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

๖.๒ ผู้ใช้งาน ต้องเก็บรักษาสื่อสำรองข้อมูลไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อเกิดการรั่วไหลข้อมูล

๖.๓ ผู้ใช้งาน ที่ต้องการเคลื่อนย้ายสื่อสำรองข้อมูลออกนอกสถานที่จะต้องมีการป้องกันการเข้าถึงข้อมูลอย่างมั่นคงปลอดภัย

๗. การบำรุงรักษาอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ มีแนวทางปฏิบัติ ดังนี้

๗.๑ อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่จะต้องขึ้นทะเบียนครุภัณฑ์เพื่อความสะดวกในการตรวจสอบและการบำรุงรักษา

๗.๒ ศทส. จะให้บริการเฉพาะอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ ที่ขึ้นทะเบียนครุภัณฑ์แล้วหรืออยู่ระหว่างการส่งมอบแล้วเท่านั้น

๗.๓ หากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่เกิดการชำรุดเสียหาย ไม่สามารถใช้งานได้ทั้งด้านซอฟต์แวร์หรือฮาร์ดแวร์ ผู้ใช้งาน มีหน้าที่จะต้องแจ้งให้ ศทส. รับทราบเพื่อดำเนินการแก้ไขต่อไป

๗.๔ หากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่อยู่ในสัญญาหรือระยะเวลาการรับประกันเกิดการชำรุดเสียหาย ศทส. มีหน้าที่ติดต่อคู่สัญญาหรือผู้แทนจำหน่าย เพื่อดำเนินการตรวจซ่อมตามที่ระบุในสัญญา

๗.๕ หากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่อยู่นอกเหนือหรือพ้นระยะเวลาการรับประกัน ศทส. มีหน้าที่ตรวจสอบเบื้องต้นและประสานกับกองเจ้าของครุภัณฑ์ ในการดำเนินการซ่อมแซมต่อไป

แนวปฏิบัติการควบคุมซอฟต์แวร์ปฏิบัติงาน

๑. วัตถุประสงค์

เพื่อใช้เป็นมาตรฐานในการควบคุมการติดตั้งซอฟต์แวร์ที่ใช้ในการปฏิบัติงาน ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายรวมถึงซอฟต์แวร์ที่ สป.พน. อนุญาตให้ใช้งาน

๒. การควบคุมการติดตั้งซอฟต์แวร์

๒.๑ ผู้อำนวยการ หรือผู้ที่ได้รับมอบหมายต้องกำหนดรายการซอฟต์แวร์ขั้นพื้นฐาน (Software Baseline) ในการติดตั้งลงบนเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสารแบบเคลื่อนที่ และต้องวางแผนการบริหารจัดการรุ่นของซอฟต์แวร์ (Software Version) เพื่อป้องกันช่องโหว่ของซอฟต์แวร์ (Software Patch)

๓. การควบคุมซอฟต์แวร์ลิขสิทธิ์

๓.๑ ซอฟต์แวร์ลิขสิทธิ์ของ สป.พน. อนุญาตให้ใช้ เพื่อการปฏิบัติงานขององค์กรเท่านั้น ห้ามเผยแพร่ โดยคัดลอกส่วนใดส่วนหนึ่งหรือทั้งหมดให้กับบุคคลภายนอกที่ไม่ได้รับอนุญาตโดยเด็ดขาด

๓.๒ ซอฟต์แวร์ลิขสิทธิ์ของ สป.พน. อนุญาตให้ใช้เฉพาะ ผู้ใช้งาน หรือบุคคลที่ สป.พน. อนุญาตให้ใช้งานเท่านั้น หากละเมิดเงื่อนไขการใช้งานซอฟต์แวร์ลิขสิทธิ์ของ สป.พน. ไม่ว่ากรณีใด ๆ ผู้ละเมิด ต้องรับผิดชอบต่อการละเมิดกฎหมายและทรัพย์สินทางปัญญาที่เกิดขึ้น

๓.๓ การควบคุมการใช้งานซอฟต์แวร์ลิขสิทธิ์ของ สป.พน. ต้องปฏิบัติตามแนวปฏิบัติด้านการปฏิบัติตามข้อกำหนดของสัญญาและกฎหมาย

แนวปฏิบัติการใช้งานระบบป้องกันซอฟต์แวร์ประสงค์ร้ายสำหรับเครื่องคอมพิวเตอร์

๑. วัตถุประสงค์

เพื่อใช้เป็นแนวทางป้องกันและลดความเสี่ยงของภัยคุกคามจากซอฟต์แวร์ประสงค์ร้าย (Malware) และมีผลต่อการบุกรุก การรบกวน หรือการทำลายระบบเทคโนโลยีสารสนเทศที่สำคัญของ สป.พน.

๒. แนวปฏิบัติการใช้งานระบบป้องกันซอฟต์แวร์ประสงค์ร้าย (Anti-Malware)

เพื่อลดความเสี่ยงและปัญหาการเข้ามาของซอฟต์แวร์ประสงค์ร้าย (Malware) ในเครื่องคอมพิวเตอร์ ของ สป.พน. รวมทั้งให้มีหลักการปฏิบัติที่สอดคล้องกัน ต้องปฏิบัติ ดังต่อไปนี้

๒.๑ ให้ระบบป้องกันซอฟต์แวร์ประสงค์ร้ายที่หน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายและระบบคอมพิวเตอร์ติดตั้ง เป็นระบบหลักสำหรับเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายและคอมพิวเตอร์ของ สป.พน.

๒.๒ ให้หน่วยงานภายในซึ่งเชื่อมต่อกับระบบเครือข่ายและคอมพิวเตอร์ของ สป.พน. ติดตั้งใช้งานระบบป้องกันซอฟต์แวร์ประสงค์ร้าย ดังกล่าวอย่างทั่วถึงทั้งในส่วนกลางและส่วนภูมิภาค โดยมีหลักพิจารณาให้ความสำคัญ (High Priority) กับกลุ่มต่อไปนี้เป็นอย่างน้อย

๒.๒.๑ อุปกรณ์คอมพิวเตอร์ที่ต้องติดต่อใช้งานกับระบบงานสำคัญ และหรือระบบสารสนเทศที่มีข้อมูลความลับของ สป.พน. เช่น DPIS, GDX, CRM เป็นต้น

๒.๒.๒ อุปกรณ์คอมพิวเตอร์ที่ใช้ทำงานกับข้อมูลสำคัญ หรือข้อมูลอันเป็นความลับของ สป.พน. เช่น การจัดทำข้อกำหนด การทำร่างสัญญาทางกฎหมาย การทำงานด้านบัญชี/การเงิน การประมูล/เปิดซอง เป็นต้น

๒.๒.๓ อุปกรณ์คอมพิวเตอร์หรือ Craft Terminal ที่ใช้ควบคุมระบบงานสำคัญ (System Management) ของ สป.พน.

๒.๒.๔ อุปกรณ์คอมพิวเตอร์ของหัวหน้ากลุ่มขึ้นไปรวมถึงอุปกรณ์คอมพิวเตอร์ของเลขานุการ/หน้าห้องผู้ใช้งาน

๒.๒.๕ อุปกรณ์คอมพิวเตอร์ที่ใช้พัฒนาซอฟท์แวร์ หรือใช้ทำงาน System Administration หรือ Network Administration

๒.๒.๖ อุปกรณ์คอมพิวเตอร์ของผู้ใช้งานที่ต้องทำหน้าที่ติดต่อกับหน่วยงานภายนอก หรือที่ต้องเชื่อมต่อกับระบบเครือข่ายและคอมพิวเตอร์ เพื่อประโยชน์ทางราชการหรือภาพลักษณ์ของ สป.พน.

๒.๓ กำหนดให้หน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายและระบบคอมพิวเตอร์ร่วมกับหน่วยงานที่เกี่ยวข้องเป็นผู้ประสานงานและดำเนินการที่เกี่ยวข้อง

๒.๓.๑ จัดทำคู่มือการติดตั้งใช้งานภาษาไทยที่เข้าใจง่าย คู่มือการแก้ปัญหาเบื้องต้นฯลฯ

๒.๓.๒ ประชาสัมพันธ์เพื่อก่อให้เกิดความตระหนักในความสำคัญของการป้องกันซอฟต์แวร์ประสงค์ร้าย

๒.๓.๓ จัดอบรมให้กับผู้แทนของหน่วยงานต่าง ๆ เพื่อช่วยแบ่งเบาภาระการแก้ไขปัญหา

๒.๓.๔ รับผิดชอบในการบำรุงรักษา ปรับปรุง ตั้งค่าระบบป้องกันซอฟต์แวร์ประสงค์ร้ายเพื่อแก้ไขช่องโหว่ และบริหารจัดการลิขสิทธิ์การใช้งานระบบ

๒.๓.๕ หน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายและระบบคอมพิวเตอร์จัดทำสถิติ กราฟและผลการใช้งาน แล้วส่งไปยังหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อรวบรวมข้อมูล

๒.๔ หน่วยงานที่ดูแลรับผิดชอบด้านระบบเครือข่ายและคอมพิวเตอร์ จะต้องปฏิบัติตามนโยบายเกี่ยวกับการใช้งานระบบป้องกันซอฟต์แวร์ประสงค์ร้ายที่ใช้งานภายในระบบเครือข่ายและคอมพิวเตอร์ของ สป.พน. ดังนี้

๒.๔.๑ หากเป็นระบบป้องกันซอฟต์แวร์ประสงค์ร้ายที่ไม่มีลิขสิทธิ์ถูกต้อง สป.พน. จะไม่อนุญาตให้ใช้งาน ทั้งนี้ ให้หน่วยงานใช้ระบบป้องกันซอฟต์แวร์ประสงค์ร้ายของหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายและระบบคอมพิวเตอร์เป็นหลัก

๒.๔.๒ หากระบบป้องกันซอฟต์แวร์ประสงค์ร้ายเดิมหมดสัญญาบำรุงรักษาแล้ว ต้องพิจารณายกเลิกการใช้งานระบบป้องกันซอฟต์แวร์ประสงค์ร้ายที่ไม่มีการบำรุงรักษาดังกล่าว และหันมาใช้งานระบบของหน่วยงานที่ดูแลรับผิดชอบด้านระบบเครือข่ายและคอมพิวเตอร์ (หากไม่มีปัญหาทางเทคนิคอื่นใด) เนื่องจากระบบที่ไม่สามารถปรับปรุงฐานข้อมูลซอฟต์แวร์ประสงค์ร้ายได้แล้วจะหมดประสิทธิภาพภายในระยะเวลาอันรวดเร็ว

๒.๕ หากมีหน่วยงานใดที่ต้องการใช้งานระบบป้องกันซอฟต์แวร์ประสงค์ร้าย แต่ไม่สามารถใช้รุ่นหรือ Version ที่หน่วยงานที่ดูแลรับผิดชอบด้านระบบเครือข่ายและคอมพิวเตอร์มีอยู่ได้ ให้หน่วยงานเสนอการตั้งงบประมาณผ่านหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และต้องมีความเห็นชอบของหน่วยงานที่ดูแลรับผิดชอบด้านระบบเครือข่ายและคอมพิวเตอร์ประกอบ

๒.๖ กรณีระบบป้องกันซอฟต์แวร์ประสงค์ร้าย สำหรับระบบงาน Server (เช่น Windows Server, Unix, Linux เป็นต้น) หรือสำหรับอุปกรณ์อื่นที่ไม่ใช่ PC และ Notebook (เช่น Appliance, Network Equipment เป็นต้น) หากหน่วยงานใดมีความจำเป็นต้องใช้งานภายใน (ไม่ใช่เพื่อการให้บริการ) ให้ส่งเรื่องให้หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศพิจารณาเป็นรายกรณีไป

แนวปฏิบัติการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานทราบถึงบทบาทหน้าที่และความรับผิดชอบการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย และลดความเสี่ยงต่อการถูกดักจับข้อมูลที่สำคัญของ สป.พน.

๒. การใช้งานอินเทอร์เน็ต

๒.๑ ผู้ใช้งาน ควรใช้อินเทอร์เน็ตเฉพาะงานในราชการเท่านั้น

๒.๒ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ สป.พน. จัดสรรไว้เท่านั้น ได้แก่ Proxy, Firewall, IPS-IDS เป็นต้น ผู้ใช้งาน ต้องไม่ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น **ยกเว้น** มีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นลายลักษณ์อักษร

๒.๓ เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์พกพา และอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ ก่อนทำการเชื่อมต่อเครือข่ายอินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web Browser) จะต้องมีการติดตั้งระบบป้องกันซอฟต์แวร์ประสงค์ร้าย (Anti-Malware) และทำการปรับปรุงระบบปฏิบัติการและเว็บเบราเซอร์ให้มีความทันสมัย

๒.๔ ในการรับ/ส่งข้อมูลคอมพิวเตอร์ผ่านทางระบบเครือข่ายอินเทอร์เน็ตจะต้องมีการตรวจสอบซอฟต์แวร์ประสงค์ร้าย (Malware scanning) โดยระบบป้องกันซอฟต์แวร์ประสงค์ร้าย ก่อนการรับ/ส่งข้อมูลทุกครั้ง

๒.๕ ผู้ใช้งาน ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ สป.พน. เพื่อหาประโยชน์ส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือ เว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๒.๖ ผู้ใช้งาน จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ สป.พน.

๒.๗ ผู้ใช้งาน ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ สป.พน.

๒.๘ ผู้ใช้งาน ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ สป.พน.ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบเครือข่ายอินเทอร์เน็ต

๒.๙ ผู้ใช้งาน ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านระบบเครือข่ายอินเทอร์เน็ต

๒.๑๐ ผู้ใช้งาน ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๒.๑๑ ผู้ใช้งาน มีหน้าที่ที่จะตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนระบบเครือข่ายอินเทอร์เน็ต ก่อนนำข้อมูลไปใช้

๒.๑๒ ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบเครือข่ายอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จาก ผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๒.๑๔ ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ สป.พน. การทำลายความสัมพันธ์กับเจ้าหน้าที่และหน่วยงานอื่น ๆ

๒.๑๕ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๒.๑๖ ไม่ติดตั้งและใช้งานโปรแกรมประเภทตรวจสอบ หรือ รบกวนการทำงานของระบบเครือข่ายคอมพิวเตอร์ ได้แก่ โปรแกรมดาวน์โหลดแบบ torrent หรือ โปรแกรมตรวจสอบ/ตรวจจับข้อมูลในระบบเครือข่าย ก่อนได้รับอนุญาตจากผู้มีอำนาจ และ ศทส. เป็นลายลักษณ์อักษร

๓. การใช้งานจดหมายอิเล็กทรอนิกส์

๓.๑ ผู้ใช้งาน ควรใช้จดหมายอิเล็กทรอนิกส์เฉพาะงานในราชการ

๓.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ สป.พน. ให้เหมาะสมกับการเข้าใช้ บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น อการลาออก เกษียณอายุราชการ เป็นต้น

๓.๓ ผู้ดูแลระบบ ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่ และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของ สป.พน.

๓.๔ ผู้ใช้งาน ที่ต้องการใช้งานจดหมายอิเล็กทรอนิกส์ต้องติดต่อ ศทส. เพื่อกรอกรายละเอียดในแบบฟอร์มขอเข้าใช้งานระบบ

๓.๕ สำหรับผู้ใช้งานรายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๓.๖ ควรมีการกำหนดรหัสผ่านจดหมายอิเล็กทรอนิกส์ ให้เป็นไปตามแนวทางการบริหารจัดการรหัสผ่าน เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของ x หรือ • ในการพิมพ์แต่ละตัวอักษร

๓.๗ ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน ๓ ครั้ง

๓.๘ ผู้ดูแลระบบ ต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ มีการนำผู้ใช้งานออกจากระบบเมื่อผู้ใช้งานไม่ได้ใช้งานระบบนานเกิน ๑๕ นาที และเมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

๓.๙ ผู้ใช้งาน ต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๓.๑๐ ผู้ใช้งาน ต้องมีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอและเคร่งครัด โดยต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน

๓.๑๑ ผู้ใช้งาน ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อ สป.พน. ละเมิดสิทธิ ละเมิดศีลธรรม สร้างความรำคาญต่อผู้อื่น และไม่แสวงหาผลประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของ สป.พน.

๓.๑๒ ผู้ใช้งาน ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-Mail Address) ของผู้อื่น เพื่ออ่าน รับ/ส่ง ข้อความ

๓.๑๓ ผู้ใช้งาน ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ สป.พน. เพื่อปฏิบัติภารกิจของ สป.พน. เท่านั้น

๓.๑๔ ผู้ใช้งาน จะต้องปฏิบัติตามคำชี้แจงหรือข้อเสนอแนะของ ศทส. อย่างเคร่งครัด ในกรณีที่มีการปรับปรุงหรือตรวจซ่อมเครื่องคอมพิวเตอร์ให้บริการจดหมายอิเล็กทรอนิกส์

๓.๑๖ ผู้ใช้งาน หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการ Log off ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๓.๑๗ ผู้ใช้งาน ต้องไม่ส่งไฟล์ที่มีขนาดใหญ่เกิน ๒๕ เมกกะไบท์

๓.๑๘ ผู้ใช้งาน ต้องไม่เปิดเอกสารแนบที่น่าสงสัย หากมีความจำเป็นที่จะต้องเปิดเอกสารแนบจะต้องมีการตรวจสอบเอกสารแนบโดยใช้โปรแกรมป้องกันซอฟต์แวร์ประสงค์ร้าย

๓.๑๙ ผู้ใช้งาน ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๓.๒๐ ผู้ใช้งาน ต้องใช้ข้อความที่สุภาพ เหมาะสม และถูกกาลเทศะในการรับ/ส่งจดหมายอิเล็กทรอนิกส์

๓.๒๑ ผู้ใช้งาน ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

แนวปฏิบัติการจัดการสื่อที่ใช้ในการบันทึกข้อมูล

๑. วัตถุประสงค์

เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต

๒. การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนที่ย้ายได้

เพื่อควบคุมและป้องกันสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ มีแนวทางการปฏิบัติดังนี้

๒.๑ ข้อมูลที่มีชั้นความลับ ต้องกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว

๒.๒ ในกรณีที่สื่อบันทึกข้อมูลไม่มีการนำมาใช้งานแล้ว หากมีการนำออกไปยังภายนอก จะต้องมั่นใจว่าข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก

๒.๓ ในกรณีที่จำเป็นต้องนำสื่อบันทึกข้อมูลออกไปยังภายนอก จะต้องได้รับการอนุมัติจากหน่วยงานที่รับผิดชอบสื่อบันทึกข้อมูลดังกล่าว และต้องบันทึกการโยกย้าย เพื่อใช้ในการตรวจสอบ

๒.๔ สื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต

๒.๕ ในการจัดเก็บสื่อบันทึกข้อมูลที่สำคัญ ต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล เช่น มีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน กำหนดบุคลากรที่มีสิทธิในการใช้งาน เป็นต้น

๒.๖ ถ้าข้อมูลที่ต้องการจัดเก็บมีอายุการจัดเก็บยาวนานกว่าอายุการใช้งานของสื่อบันทึกข้อมูล ต้องมีการสำรองข้อมูลเก็บไว้ที่สื่อบันทึกข้อมูลอื่นที่มีความปลอดภัย เพื่อป้องกันการสูญหายของข้อมูล

๒.๗ ต้องจัดทำทะเบียนบันทึกข้อมูลของสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เพื่อลดโอกาสการสูญหายของข้อมูล

๒.๘ ตัวอ่านสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ จะต้องใช้เพื่อเหตุผลทางราชการเท่านั้น การมอบอำนาจในระดับต่าง ๆ ต้องมีการทำเอกสารเป็นลายลักษณ์อักษรอย่างชัดเจน

๓. การกำจัดสื่อบันทึกข้อมูล

การทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีก ต้องเป็นไปอย่างมั่นคงและปลอดภัย เพื่อลดความเสี่ยงของการรั่วไหลข้อมูลของ สป.พน. ไปยังผู้อื่นที่ไม่ได้รับอนุญาต ซึ่งมีแนวทางปฏิบัติดังนี้

๓.๑ สื่อที่บันทึกข้อมูลที่มีความสำคัญมาก จะต้องมีการทำลายด้วยวิธีการที่ปลอดภัย ได้แก่ การเผา แยกชิ้นส่วนเป็นชิ้นเล็ก ๆ หรือลบข้อมูลด้วยโปรแกรมอื่น ๆ ที่มีใช้ใน สป.พน.

๓.๒ กระบวนการต่าง ๆ ต้องระบุวิธีการกำจัดสื่อบันทึกข้อมูลอย่างชัดเจน เพื่อความปลอดภัยของข้อมูล โดยปฏิบัติตามแนวทางความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

๓.๓ เพื่อความสะดวก ต้องรวบรวมสื่อทั้งหมดที่ไม่ต้องการแล้วกำจัดพร้อมกันด้วยวิธีการที่ปลอดภัย

๓.๔ ในกรณีที่เลือกใช้บริการกำจัดสื่อและเอกสาร รวมทั้งอุปกรณ์ต่าง ๆ จากหน่วยงานภายนอก จะต้องเลือกหน่วยงานภายนอกที่มีมาตรฐานและมีประสบการณ์

๓.๕ ในการกำจัดสื่อบันทึกข้อมูล จะต้องมีการบันทึก เพื่อใช้ในการตรวจสอบ

หมายเหตุ : ข้อมูลที่ไม่มีความสำคัญเมื่อมีการรวบรวมเป็นจำนวนมาก ๆ ผู้ที่ต้องการอาจจะสามารถนำข้อมูลที่ถูกรวบรวมไว้ไปใช้ได้ ดังนั้นในการรวบรวมเพื่อกำจัด ต้องคำนึงถึงข้อมูลที่มีการรวบรวมไว้ด้วย

๔. ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์ มีแนวทางปฏิบัติดังนี้

๔.๑ ติดป้ายชื่อของสื่อบันทึกข้อมูลทั้งหมด เพื่อระบุประเภท

๔.๒ จำกัดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศของผู้ที่ไม่ได้รับอนุญาต

๔.๓ ทำบันทึกข้อมูลเกี่ยวกับผู้ที่มีสิทธิได้รับข้อมูล

๔.๔ ข้อมูลที่ป้อนเข้าสู่ระบบและในระหว่างการประมวลผลต้องมีความครบถ้วน และต้องตรวจสอบผลลัพธ์ที่ออกมาด้วย

๔.๕ ต้องมีการปกป้องข้อมูลที่อยู่ในระหว่างการแสดงผลลัพธ์ออกมาตามระดับความสำคัญ

๔.๖ เก็บรักษาสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต

๔.๗ กระจายข้อมูลให้ผู้ที่มีสิทธิได้รับข้อมูลเท่านั้น

๔.๘ ลบเครื่องหมายของสำเนาสื่อบันทึกข้อมูลทั้งหมด เพื่อไม่ให้เป็นที่สังเกตของผู้ที่มีสิทธิได้รับข้อมูล

๔.๙ ทบทวนการกระจายข้อมูลและรายชื่อของผู้ที่มีสิทธิได้รับข้อมูลอย่างต่อเนื่อง

๕. การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ

มาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต มีแนวทางปฏิบัติดังนี้

๕.๑ มีการจัดเก็บเอกสารระบบอย่างมั่นคงปลอดภัย

๕.๒ เอกสารระบบที่จัดเก็บไว้ในเครือข่ายสาธารณะ หรือมีการใช้งานผ่านเครือข่ายสาธารณะจะต้องมีระบบการป้องกันที่เหมาะสม

๕.๓ เอกสารระบบสำหรับผู้ดูแลระบบที่มีการแชร์ผ่านเครือข่ายสาธารณะไม่ควรมีการระบุ Username และ Password เพราะอาจทำให้ผู้ไม่มีสิทธิสามารถนำข้อมูลดังกล่าวไปใช้ในการเข้าถึงระบบได้

แนวปฏิบัติด้านการเฝ้าระวังและบันทึกเหตุการณ์

๑. วัตถุประสงค์

เพื่อใช้เป็นมาตรฐานสำหรับการเฝ้าระวังและบันทึกเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศของ สป.พน. ในการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ โดยการรวบรวมหลักฐานการเข้าใช้งานระบบสารสนเทศของ สป.พน. ที่คำนึงถึงความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability) และการปฏิบัติตาม พ.ร.บ. ว่าด้วยการทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐

๒. การบันทึกเหตุการณ์ข้อมูลจราจรทางคอมพิวเตอร์

ให้บันทึกกิจกรรมการใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการของระบบ และเหตุการณ์ด้านความมั่นคงปลอดภัยให้เป็นไปตาม พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๓. การตรวจสอบการใช้งานระบบ

เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ โดยต้องมีการประเมินความเสี่ยงและปฏิบัติตามที่กฎหมายกำหนด มีแนวทางปฏิบัติดังนี้

๓.๑ การระบุตัวตนในการเข้าถึง ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้

๓.๑.๑ User ID

๓.๑.๒ วัน เวลา และรายละเอียดที่สำคัญ

๓.๑.๓ ชนิดของเหตุการณ์

๓.๑.๔ การเข้าถึงไฟล์

๓.๑.๕ โปรแกรมหรือยูทิลิตี้ที่ใช้

๓.๒ การดำเนินการเกี่ยวกับสิทธิของผู้ใช้งาน

๓.๒.๑ การใช้บัญชีผู้ใช้งานแบบสิทธิพิเศษ ของ Administrator ,Root หรือ Supervisor

๓.๒.๒ การเริ่มต้นและหยุดของระบบ

๓.๒.๓ อุปกรณ์ที่นำมาเชื่อมต่อ

๓.๓ การพยายามเข้าถึงของผู้ที่ไม่มีสิทธิ

๓.๓.๑ การล้มเหลวหรือยกเลิกของผู้ใช้งาน

๓.๓.๒ การล้มเหลวหรือยกเลิกการกระทำที่เกี่ยวกับข้อมูลหรือทรัพยากรอื่น ๆ

๓.๓.๓ การฝ่าฝืนนโยบายการเข้าถึงและการแจ้งเตือนของ Network Gateway และ Firewall

๓.๓.๔ การแจ้งเตือนของ IDS

๓.๔ การเปลี่ยนแปลงหรือพยายามที่จะเปลี่ยนแปลงการตั้งค่าและการควบคุมของระบบรักษาความปลอดภัย

๔. การป้องกันข้อมูลบันทึกเหตุการณ์

เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต จึงต้องพิจารณาเรื่องดังต่อไปนี้

๔.๑ การเปลี่ยนแปลงชนิดของข้อความที่ถูกบันทึก

๔.๒ Log ที่ถูกแก้ไขหรือถูกลบ

๔.๓ ความจุของพื้นที่ในการจัดเก็บ Log ที่ไม่เพียงพอ ทำให้ไม่สามารถจัดเก็บ Log ได้

๔.๔ ระยะเวลาในการจัดเก็บและการ Backup Log

๕. บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ

Log ที่จะบันทึกประกอบด้วย

๕.๑ เวลาที่เกิดเหตุการณ์ ทั้งที่สำเร็จและล้มเหลว

๕.๒ ข้อมูลที่เกี่ยวกับเหตุการณ์ (ไฟล์ที่เกี่ยวข้อง) หรือการล้มเหลว (ความผิดพลาดที่เกิดขึ้นและการแก้ไขต่าง ๆ)

๕.๓ บัญชีผู้ใช้งานและผู้ดูแลระบบหรือผู้ปฏิบัติการที่เกี่ยวข้อง

๕.๔ กระบวนการทำงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ

๖. การบันทึกเหตุการณ์ข้อผิดพลาด

การบันทึกเหตุการณ์ข้อผิดพลาดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไข ดังนี้

๖.๑ ตรวจสอบข้อผิดพลาด และดำเนินการแก้ไขข้อผิดพลาดตามข้อมูลที่มีแจ้งไว้ใน Log ข้อผิดพลาด

๗. การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน

การตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงาน โดยการตั้งเวลาด้วย Network Time Protocol หรือ NTP ไปยังเซิร์ฟเวอร์ที่ให้บริการข้อมูลเวลาอย่างน้อยที่เป็น Stratum 1 ให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ของ สป.พน. ถูกบุกรุก โดยสามารถอ้างอิงผู้ให้บริการ ดังต่อไปนี้

๗.๑ ภายใน สป.พน.

การตั้งเวลาของเครื่อง Server และเครื่องคอมพิวเตอร์ทุกเครื่องใน สป.พน. โดยการตั้งเวลาด้วย Network Time Protocol (NTP) ไปยัง Server ที่ให้บริการข้อมูลเวลา

๗.๑ ภายในประเทศไทย

๗.๒.๑ สถาบันมาตรวิทยาแห่งชาติ เครื่อง time1.nimt.or.th หรือ ๒๐๓.๑๘๕.๖๙.๖๐

๗.๒.๒ กรมอุทกศาสตร์ กองทัพเรือ เครื่องเซิร์ฟเวอร์ time.navy.mi.th หรือ 118.175.67.83

๗.๒.๓ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทยหรือ ThaiCERT เครื่องเซิร์ฟเวอร์ clock.thaicert.org หรือ 203.155.129.186 หรือ 203.185.129.187

๗.๒ ในต่างประเทศ ได้แก่ National Institute of Standards and Technology ประเทศสหรัฐอเมริกา เครื่องเซิร์ฟเวอร์ time.nist.gov หรือ 192.43.244.18

หมวด ๙
ความมั่นคงปลอดภัยในการสื่อสารข้อมูล
(Communications Security)

จุดประสงค์ เพื่อสร้างความมั่นคงปลอดภัยข้อมูลและสารสนเทศบนระบบเครือข่าย และอุปกรณ์คอมพิวเตอร์ โดยมีการกำหนดการบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย และการถ่ายโอนข้อมูลและสารสนเทศ รวมถึงข้อกำหนดในการรักษาความลับ หรือการไม่เปิดเผยความลับซึ่งมีผลบังคับใช้กับเจ้าหน้าที่ขององค์กร รวมถึงบุคคลภายนอก โดยมีแนวปฏิบัติดังนี้

- **แนวปฏิบัติด้านการบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย**
- **แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย**
- **แนวปฏิบัติด้านการแลกเปลี่ยนสารสนเทศ**
- **แนวปฏิบัติสำหรับสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ**

แนวปฏิบัติด้านการบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย

๑. วัตถุประสงค์

เพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างถูกต้องและปลอดภัย จึงจำเป็นต้องมีการบริหารจัดการเครือข่ายของ สป.พน. ให้มีความมั่นคงปลอดภัยด้านความถูกต้อง การเก็บรักษาเป็นความลับและความพร้อมในการใช้งาน นโยบายดังกล่าวนี้มีผลบังคับใช้กับ เจ้าหน้าที่ ของ สป.พน. และหน่วยงานภายนอกที่ขออนุญาตใช้งานระบบสารสนเทศของ สป.พน.

๒. มาตรฐานทั่วไป

๒.๑ การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน

๒.๑.๑ ผู้อำนวยการที่เป็นเจ้าของระบบงาน ต้องจัดทำคู่มือและขั้นตอนการปฏิบัติงานของระบบงานนั้น ๆ โดยมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่าย

๒.๑.๒ ในกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ หน่วยงานที่ดูแลระบบสารสนเทศนั้นต้องทำการบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ

๒.๑.๓ ผู้อำนวยการที่เป็นเจ้าของระบบงาน ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบสารสนเทศและเครือข่ายที่หน่วยงานนั้น ๆ รับผิดชอบ

๒.๑.๔ ผู้อำนวยการที่เป็นเจ้าของระบบงาน ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้ละเมิด

๒.๑.๕ ผู้อำนวยการที่เป็นเจ้าของระบบงาน ต้องแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบสารสนเทศออกจากเครื่องที่ทำงานจริงหรือเครื่องให้บริการ

๒.๑.๖ ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอก สป.พน. หน่วยงานที่รับผิดชอบต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ สำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิของผู้ใช้งานที่ได้รับ และตรวจสอบการใช้งานอย่างสม่ำเสมอ

๒.๒ การบริหารจัดการการเปลี่ยนแปลงในการให้บริการต่อหน่วยงานภายนอก

ต้องปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงหรือพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับความมั่นคงปลอดภัยสารสนเทศ การใช้

ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก โดยต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้ที่ได้รับมอบหมายก่อนจึงจะสามารถดำเนินการได้ รวมทั้งปรับปรุงเอกสารที่เกี่ยวข้องให้ทันสมัย เมื่อมีการเปลี่ยนแปลงสารสนเทศ

๒.๓ การบริหารจัดการเครือข่าย

๒.๓.๑ ผู้ดูแลระบบ ต้องบริหารจัดการความมั่นคงปลอดภัยในเครือข่าย ซึ่งมีแนวทางปฏิบัติดังนี้

๒.๓.๑.๑ **ระบบเครือข่ายภายใน** อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่ายเพื่อการทำงานภายใน สป.พน. ได้แก่ Router, Switch และ HUB มีข้อปฏิบัติดังนี้

- อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมโยงเครือข่าย ต้องปิด Service Port ที่ไม่จำเป็น และในการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่า Default Community, Default Username และ Default Password
- การเชื่อมโยงเครือข่ายเพื่อใช้งานระบบต่าง ๆ จะสามารถกระทำได้ก็ต่อเมื่อได้รับอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านระบบเครือข่ายและคอมพิวเตอร์ การเชื่อมโยงเครือข่ายเองโดยพลการ หากทำให้เกิดความเสียหายกับระบบเครือข่ายจะต้องถูกลงโทษตามที่กำหนดไว้
- ผู้ดูแลระบบจะต้องมีแผนดำเนินการบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์ เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ
- ผู้ดูแลระบบมีหน้าที่ในการติดตั้งอุปกรณ์ซอฟต์แวร์ระบบ การเข้ารหัสข้อมูลอัตโนมัติหรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ
- ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

๒.๓.๑.๒ **อุปกรณ์ Server** อุปกรณ์ Server ที่ติดตั้งเพื่อการทำงานภายใน สป.พน. มีข้อปฏิบัติดังนี้

- ผู้ดูแลระบบต้องไม่ใช้ Default Username/Default Password
- ต้องทำ Hardening และบันทึกการทำ Configuration Set up ของอุปกรณ์ Server และจัดทำเป็นเอกสารทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง
- ให้เปิด Service Port ที่จำเป็นเท่านั้น ส่วน Port ที่ไม่ใช้งานให้ปิดทั้งหมดและต้องมีการบันทึกการติดตั้ง Service Patch ทุกครั้ง
- ต้องไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ
- เมื่อจบการใช้งานที่ Console ต้อง Logoff User นั้นโดยทันที
- ผู้ดูแลระบบจะต้องสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยเดือนละครั้ง และทดสอบการสำรองข้อมูลอย่างน้อยปีละ ๒ ครั้ง โดยต้องสอดคล้องกับความสำคัญของระบบ

๒.๓.๑.๓ **อุปกรณ์ PC Terminal** มีข้อปฏิบัติดังนี้

- ให้เปิด Service Port ที่จำเป็นเท่านั้นส่วน port ที่ไม่ใช้งานให้ทำการปิดให้หมดและต้องมีการบันทึกการติดตั้ง Service Patch ทุกครั้ง

- ต้องติดตั้ง Protocol เฉพาะที่ทำงานร่วมกับ Server เท่านั้น
- การ Remote Terminal Console เมื่อไม่ใช้งานแล้วจะต้อง Log off ทุกครั้ง

๒.๓.๒ การป้องกันการใช้งานเครือข่าย

๒.๓.๒.๑ ห้ามนำอุปกรณ์เครือข่ายมาติดตั้งกับระบบเครือข่ายของ สป.พน. โดยไม่รับอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านระบบเครือข่ายและคอมพิวเตอร์

๒.๓.๒.๒ ห้ามผู้ใช้งานเครือข่ายกระทำการใด ๆ ที่รบกวนระบบเครือข่าย ได้แก่ การเปิดใช้งาน Service DHCP เพื่อเชื่อมต่อเข้ากับระบบเครือข่ายของ สป.พน. เอง

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของ สป.พน. โดยการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สายของ สป.พน.

๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย มีแนวทางปฏิบัติ ดังนี้

๒.๑ ผู้ใช้งาน ต้องไม่นำอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless Access Point) มาติดตั้งใช้งานเองโดยไม่ได้รับความเห็นชอบจาก ศทส.

๒.๒ ผู้ใช้งาน ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ สป.พน. จะต้องทำการลงทะเบียนกับ **ผู้ดูแลระบบ** ของ ศทส. และต้องได้รับการพิจารณาอนุญาตจาก ผอ.ศทส.

๒.๓ ผู้ใช้งาน จะต้องปฏิบัติตามคำแนะนำการใช้งานของ ศทส. เพื่อการรักษาความมั่นคงปลอดภัยโดยเคร่งครัด

๒.๔ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

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

๒.๖ ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณไร้สายมาใช้งาน

๒.๗ ผู้ดูแลระบบ ต้องเปลี่ยนค่า Login ID และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ Login ID และรหัสผ่านที่มีความปลอดภัยเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๒.๘ ผู้ดูแลระบบ ต้องมีการติดตั้งอุปกรณ์ป้องกันการเข้าถึงเครือข่าย (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายใน

๒.๙ ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

แนวปฏิบัติด้านการแลกเปลี่ยนสารสนเทศ

๑. วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการแลกเปลี่ยนกันภายใน สป.พน. และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

๒. ขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ

เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร ทั้ง องค์กรและหน่วยงานภายนอก โดยผ่านทางช่องทางการสื่อสารทุกชนิด ต้องพิจารณาดังต่อไปนี้

๒.๑ การป้องกันจากการถูกดักจับ คัดลอก แก้ไข ส่งผิดเส้นทาง และการทำลายข้อมูล

๒.๒ การตรวจจับและป้องกัน Source Code ที่ไม่พึงประสงค์ ซึ่งอาจถูกส่งผ่านการสื่อสารทางอิเล็กทรอนิกส์

๒.๓ การป้องกันการส่งข้อมูลที่สำคัญด้วยวิธีการแนบเอกสาร (Attachment File)

๒.๔ แนวทางปฏิบัติต้องสอดคล้องกับแนวทางความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

๒.๕ ผู้ใช้งานต้องรับผิดชอบในบทบาทหน้าที่ ไม่ฝ่าฝืนนโยบายหรือกฎระเบียบของ สป.พน. เช่น การหมิ่นประมาท การข่มขู่หรือก่อกวนความสงบ การปลอมตัว การส่งต่อจดหมายลูกโซ่ การจัดซื้อจัดจ้างนอกเหนือการอนุมัติ เป็นต้น

๒.๖ เทคนิคการเข้ารหัส เพื่อปกป้องความลับ และความถูกต้องของสารสนเทศ

๒.๗ แนวทางในการเก็บรักษาและทำลายจดหมายทางราชการต้องเป็นไปตามที่กฎหมายกำหนด

๒.๘ ไม่ทิ้งเอกสารสำคัญไว้ที่เครื่องถ่ายเอกสาร เครื่องพิมพ์หรือเครื่องโทรสาร ซึ่งผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้

๒.๙ ควบคุมและยับยั้งการส่งต่อข้อมูลของอุปกรณ์สื่อสาร เช่น การส่งต่อจดหมายอิเล็กทรอนิกส์อัตโนมัติไปนอก สป.พน. เป็นต้น

๒.๑๐ ไม่ทิ้งข้อความสำคัญบนเครื่องตอบรับ ซึ่งอาจจะถูกตอบกลับโดยผู้ที่ไม่ได้รับอนุญาต หรือถูกเก็บบนระบบของสาธารณะ หรือถูกเก็บอย่างไม่ถูกต้องเนื่องจากการโทรที่ผิดพลาด

๒.๑๑ เตือนผู้ใช้งานเกี่ยวกับปัญหาในการใช้เครื่องโทรสาร

๒.๑๑.๑ การเข้าถึงของผู้ที่ไม่ได้รับอนุญาต เพื่อดึงข้อมูลภายในเครื่องที่จัดเก็บไว้

๒.๑๑.๒ การตั้งโปรแกรมในการส่งไปยังเลขหมายปลายทางโดยตั้งใจและไม่ตั้งใจ

๒.๑๑.๓ การส่งเอกสารหรือข้อความผิดเลขหมายโดยการโทรที่ผิดพลาดหรือบันทึกเลขหมายผิด

๒.๑๑.๔ เครื่องโทรสารและเครื่องถ่ายเอกสารรุ่นใหม่จะมีหน่วยความจำในการเก็บเอกสารบางหน้าหรือการส่งที่ผิดพลาด ซึ่งจะถูกพิมพ์ออกมาเมื่อเครื่องทำงานได้ตามปกติ

๓. ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange Agreements)

ในการแลกเปลี่ยนสารสนเทศ ต้องคำนึงถึงความปลอดภัยในการแลกเปลี่ยนดังต่อไปนี้

๓.๑ การบริหารจัดการในการควบคุมและแจ้งให้ทราบเกี่ยวกับการสื่อสาร การส่งและการรับ

๓.๒ การแจ้งให้ผู้ส่งรับทราบเกี่ยวกับการสื่อสาร การส่งและการรับ

๓.๓ กระบวนการที่สามารถติดตามและปฏิเสธความรับผิดชอบไม่ได้

๓.๔ มาตรฐานทางเทคนิคขั้นต่ำในการบรรจุและส่งออก

๓.๕ สัญญาข้อตกลง

๓.๖ มาตรฐานในการระบุตัวผู้ส่งเอกสาร

๓.๗ ความรับผิดชอบและภาระหน้าที่เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ ได้แก่ การสูญหายของข้อมูล

๓.๘ ใช้ระบบป้ายชื่อตามข้อตกลงสำหรับข้อมูลที่มีความสำคัญ เพื่อเข้าใจได้ทันทีในความหมายของป้ายชื่อและเป็นการปกป้องสารสนเทศอย่างเหมาะสม

๓.๙ ความเป็นเจ้าของและความรับผิดชอบสำหรับการปกป้องข้อมูล ลิขสิทธิ์ การปฏิบัติตามใบอนุญาตการใช้งานซอฟท์แวร์ และค่าตอบแทนต่าง ๆ

๓.๑๐ มาตรฐานทางเทคนิคในการบันทึกและอ่านข้อมูลสารสนเทศและซอฟต์แวร์

แนวปฏิบัติสำหรับสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ

การป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ ครอบคลุมถึงซอฟท์แวร์ ข้อมูลและสารสนเทศอื่น ๆ ที่ต้องการความถูกต้องในระดับสูงที่จะถูกเผยแพร่ออกสู่สาธารณะ จะต้องมีการป้องกันที่ดี ได้แก่ ลายมือชื่ออิเล็กทรอนิกส์ การเข้าถึงจากเครือข่ายสาธารณะ จะต้องตรวจสอบความผิดพลาดต่าง ๆ และได้รับการอนุมัติก่อน ต้องมีการควบคุมดังต่อไปนี้

- สารสนเทศนั้นต้องเป็นไปตามกฎหมายที่เกี่ยวข้องกับการปกป้องข้อมูล
- สารสนเทศที่นำเข้าและประมวลผลโดยระบบจะต้องสมบูรณ์และถูกต้องตามสภาวะการณ์
- สารสนเทศสำคัญจะต้องถูกปกป้องในระหว่างที่มีการรวบรวม ประมวลผลและจัดเก็บ การป้องกันการโจมตีจากหน้าเว็บไซต์ เพื่อไม่ให้มีการเข้าถึงเครือข่ายของ สป.พน.

หมวด ๑๐
การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
(Information System Acquisition, Development and Maintenance)

จุดประสงค์ เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ ป้องกันความผิดพลาด การสูญหายและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาตหรือการใช้งานสารสนเทศผิดวัตถุประสงค์ รักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยวิธีการเข้ารหัสข้อมูล สร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์ สารสนเทศ และไฟล์ต่าง ๆ ของระบบที่ให้บริการ ลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ โดยประกอบด้วย

- **แนวปฏิบัติในการพัฒนาระบบสารสนเทศ**
- **แนวปฏิบัติในการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ**

แนวปฏิบัติในการพัฒนาระบบสารสนเทศ

๑. วัตถุประสงค์

เพื่อลดความเสี่ยงต่อการเสียหายหรือการเปลี่ยนแปลงแก้ไขข้อมูลและระบบสารสนเทศ ที่มีความสำคัญต่อการปฏิบัติราชการของ สป.พน.

๒. ความมั่นคงปลอดภัยสารสนเทศในการพัฒนาระบบสารสนเทศ

๒.๑ หน่วยงานที่ดูแลระบบสารสนเทศ จะต้องทำการวิเคราะห์ระบบสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้

- มาตรการปฏิบัติก่อนเกิดความเสียหาย โดยการสำรองข้อมูล ระบบเครือข่ายสำรอง
- มาตรการปฏิบัติหลังเกิดความเสียหาย เช่น แผนการกู้คืน ระยะเวลาในการกู้คืน เป็นต้น

๒.๒ การพัฒนาระบบสารสนเทศต้องมีการควบคุม เพื่อให้เกิดความถูกต้องและเหมาะสมของข้อมูลที่นำเข้าและผลลัพธ์ที่ได้จากระบบ จึงจำเป็นที่จะต้องมีระบบการตรวจทานความถูกต้องของข้อมูลที่ดีเพื่อลดความเสี่ยงของการนำข้อมูลเข้าและการประมวลผลข้อมูล

๒.๓ การตรวจสอบข้อมูลนำเข้า

ในกรณีที่เจ้าของข้อมูลและสารสนเทศต้องการนำข้อมูลเข้าไปยังระบบสารสนเทศ ก่อนที่จะนำเข้า ต้องตรวจสอบข้อมูลว่าเป็นข้อมูลที่ถูกต้อง ครบถ้วนและไม่ก่อให้เกิดความเสียหายต่อระบบ

๒.๔ การควบคุมข้อมูลที่อยู่ในระหว่างการประมวลผล

ในกรณีที่เจ้าของข้อมูลและสารสนเทศมีการนำข้อมูลเข้าไปยังระบบสารสนเทศ ในระหว่างการประมวลผล จะต้องกำหนดกลไกสำหรับการตรวจสอบว่า ข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ โดยมีสาเหตุจากความผิดพลาดในการประมวลผล หรือการกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง

๒.๕ การตรวจสอบความถูกต้องของข้อความ

เจ้าของข้อมูลและสารสนเทศต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอปพลิเคชัน (เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง) รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต

๒.๖ การตรวจสอบข้อมูลผลลัพธ์ (Output Data Validation) ก่อนนำข้อมูลออกจากระบบต้องปฏิบัติดังนี้

- มีการอนุญาตจากเจ้าของข้อมูลและสารสนเทศให้นำข้อมูลออกจากระบบได้
- มีการตรวจสอบข้อมูลว่ามีความถูกต้อง
- มีกระบวนการบันทึกโดยเข้ารหัสข้อมูล สามารถพิสูจน์และรับรองข้อมูล ในกรณีที่เป็นข้อมูลในชั้นความลับ

๓. มาตรการการเข้ารหัสข้อมูล

๓.๑ เจ้าของข้อมูลและสารสนเทศต้องกำหนดให้มีการเข้ารหัสหรือใช้ข้อมูลตามมาตรฐานสากล เช่น ขั้นตอนวิธี RSA, DES, 3DES เป็นต้น และต้องมีการกำหนดชั้นความลับของข้อมูลและสารสนเทศ เพื่อให้ทราบถึงสถานะและการดำเนินการในการเข้ารหัสข้อมูลสารสนเทศที่ใช้

๓.๒ ขั้นตอนวิธี (Algorithm) ที่เรียกใช้ต้องรองรับโปรแกรมประยุกต์ที่นำไปใช้งานได้ เช่น PGP (Pretty Good Privacy), SSL (Secure Socket Layer), TLS (Transport Layer Security) เป็นต้น

๓.๓ ความยาวของคีย์ในการเข้ารหัสต้องไม่น้อยกว่า 56 บิต สำหรับการเข้ารหัสแบบสมมาตร (Symmetric) และแบบอสมมาตร (Asymmetric) ต้องมีความยาวไม่น้อยกว่าตามที่ตกลงกันไว้

๓.๔ เจ้าของข้อมูลและสารสนเทศต้องมีการทบทวนมาตรฐานของคีย์ที่เข้ารหัสในทุก ๆ ปี เพื่อให้สอดคล้องกับความปลอดภัย และประสิทธิภาพของเครื่องที่ดำเนินงาน

๓.๕ กรณีที่ไม่ทราบหรือต้องการข้อมูลเกี่ยวกับการเข้ารหัสเพิ่มเติม ให้ติดต่อมาที่หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

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

๔. ความมั่นคงปลอดภัยสารสนเทศของแฟ้มข้อมูลระบบ

๔.๑ หลักการควบคุมการติดตั้งซอฟต์แวร์ (Control of Operational Software) ผู้อำนวยการกองต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดีว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

๔.๒ หลักการป้องกันข้อมูลจริงที่ใช้ในการทดสอบระบบ (Protect of System Test Data) ข้อมูลจริงที่จะนำใช้ทดสอบระบบ ต้องได้รับอนุญาตจากผู้อำนวยการกองที่รับผิดชอบในการรักษาข้อมูลนั้น ๆ 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

๕. กระบวนความมั่นคงปลอดภัยสารสนเทศในการพัฒนาระบบ

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

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

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

แนวปฏิบัติในการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ

๑. วัตถุประสงค์

เพื่อไม่ให้มีผลกระทบต่อโปรแกรมประยุกต์ (Application Software) โปรแกรมระบบ (System Software) ระบบเครือข่าย (Network System) หรือการเปลี่ยนแปลงอื่น ๆ ที่เกิดจากการเปลี่ยนแปลงระบบงาน ได้แก่ การพัฒนาระบบ การทดสอบระบบ จะต้องอยู่ภายใต้การควบคุมที่เหมาะสมและเพียงพอ โดยวิธีการดังกล่าวจะช่วยให้ระบบสารสนเทศนั้น ๆ สามารถทำงานเข้ากันได้ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์

การเปลี่ยนแปลงแก้ไข ต้องมีคำขอการเปลี่ยนแปลงอย่างเป็นทางการ ซึ่งมีการอนุมัติโดยผู้บริหารที่มีอำนาจอนุมัติการเปลี่ยนแปลงระบบงานนั้น ๆ

๒. ความต้องการในการขอให้มีการเปลี่ยนแปลง

๒.๑ ผู้ร้องขอ ต้องดำเนินการตามกระบวนการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริงหรือใช้งานอยู่แล้วโดยทำหนังสือแจ้งไปยังหน่วยงานเจ้าของข้อมูลและสารสนเทศ หน่วยงานเจ้าของระบบงาน และหรือหน่วยงานที่เกี่ยวข้องทุกส่วนให้รับทราบก่อนทำการแก้ไขซอฟต์แวร์นั้น และต้องมีการอนุมัติโดยผู้มีอำนาจในการลงนามในแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form by User) ซึ่งโดยทั่วไปแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบจะต้องมีข้อมูลที่จำเป็นดังนี้

- คำขอให้แก้ไขต้องมาจากผู้มีสิทธิ
- เหตุผลการปฏิบัติราชการที่ต้องมีการเปลี่ยนแปลง
- ลักษณะของข้อบกพร่องที่ทำให้ต้องมีการเปลี่ยนแปลง (ถ้ามี)
- ทรัพยากรที่จำเป็นต้องใช้ในการเปลี่ยนแปลงระบบงาน
- รายละเอียดการทดสอบ (Test Script)
- กระบวนการนำระบบเดิมที่ใช้งานได้กลับมาใช้ใหม่ ในกรณีที่ระบบใหม่มีปัญหา
- ต้องได้รับการอนุมัติคำขอโดยผู้มีอำนาจ
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ

- ต้องเก็บรายละเอียดของคำขอไว้เป็นหลักฐาน

๒.๒ ผู้อำนวยการกอง เจ้าของข้อมูลและสารสนเทศ (Information Owner) และผู้อำนวยการกองเจ้าของระบบงาน (Application Owner) ที่เกี่ยวข้องกับการเปลี่ยนแปลงนั้น ๆ จะต้องพิจารณาเหตุผลทางราชการของคำขอเปลี่ยนแปลง และทำการลงนามอนุมัติในคำขอเปลี่ยนแปลง

๒.๓ ทุกครั้งที่มีการเปลี่ยนแปลงระบบงาน จะต้องมีการจัดเตรียมและปรับปรุงคู่มือในการใช้งานระบบงานและคู่มือในการอบรมให้กับผู้ใช้งาน ต้องมีการจัดทำและปรับปรุงให้สอดคล้องกับการเปลี่ยนแปลงระบบงานอยู่เสมอ

๓. การกำหนดบทบาทและหน้าที่การเปลี่ยนแปลง

๓.๑ ต้องมีการกำหนดบทบาทและความรับผิดชอบของแต่ละบุคคลที่เกี่ยวข้องกับกระบวนการควบคุมการเปลี่ยนแปลงอย่างชัดเจน เพื่อการควบคุมที่ดี ต้องไม่ทำโดยบุคคลเดียวกัน

๓.๒ โปรแกรมที่ใช้งานจริงสำหรับระบบงานนั้น ๆ ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิในการโอนย้ายโปรแกรมที่พร้อมใช้งานไปยังส่วนที่ใช้งานจริง

๓.๓ ต้องแบ่งแยกส่วนที่ใช้สำหรับงานต่อไปนี้ออกจากกัน ได้แก่ ส่วนการพัฒนาระบบงาน ส่วนที่ใช้สำหรับโอนย้ายโปรแกรมก่อนการย้ายเข้าส่วนที่ใช้งานจริง ส่วนที่ใช้ทดสอบระบบสำหรับผู้ใช้งาน และส่วนที่ใช้งานจริง ในแต่ละส่วนต้องมีการควบคุมการเข้าใช้งานที่ดี

๔. การเปลี่ยนแปลงระบบคอมพิวเตอร์ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูล

๔.๑ การเปลี่ยนแปลงต่อระบบคอมพิวเตอร์ ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูลจะต้องได้รับอนุมัติจากผู้อำนวยการกองที่ดูแลระบบงานนั้น ๆ เป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการหยุดชะงักของการปฏิบัติราชการ หรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

๔.๒ การเปลี่ยนแปลงระบบงานใด ๆ ต้องไม่รบกวนหรือขัดขวางการปฏิบัติงานของระบบงานปัจจุบัน และการเปลี่ยนแปลงดังกล่าวนั้น จะต้องสามารถใช้งานร่วมกับข้อมูลและระบบงานที่มีการใช้อยู่ในปัจจุบันได้ด้วย

๔.๓ การเปลี่ยนแปลงอุปกรณ์หรือสื่อที่ใช้ในการจัดเก็บข้อมูล ต้องทำการลบข้อมูลที่ไม่ใช้งานแล้วทั้งหมดของ สป.พน. อย่างถาวรออกจากอุปกรณ์หรือสื่อที่ใช้สำหรับเก็บข้อมูลที่มีการเปลี่ยนแปลง

๕. การเปลี่ยนแปลงระบบเครือข่าย ได้แก่ Network Firewalls และ Router เป็นต้น

๕.๑ ผู้ร้องขอจะต้องกรอกรายละเอียดลงในแบบฟอร์มการเปลี่ยนแปลง/แก้ไขระบบเครือข่าย (Change Request Form by Admin) โดยผ่านการอนุมัติจากผู้บังคับบัญชา เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการหยุดชะงักของการปฏิบัติราชการ หรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

๕.๒ การเปลี่ยนแปลงใด ๆ ของระบบเครือข่ายของ สป.พน. ต้องปฏิบัติตามคู่มือที่กำหนดไว้ เช่น การเปลี่ยนแปลงระบบเครือข่าย รวมถึงการเพิ่มซอฟต์แวร์ของระบบเครือข่าย การเปลี่ยนแปลงหมายเลขของเครือข่าย การกำหนดค่าของ Routers ใหม่ การเพิ่มเติมคู่สาย เพื่อใช้ในการเชื่อมต่อระบบ เป็นต้น

๕.๓ ผู้ดูแลระบบจะต้องทำบันทึกข้อมูลของระบบเก่าเก็บไว้ เพื่อใช้แก้ปัญหาในการนำระบบเก่ามาใช้ในกรณีที่ระบบใหม่เกิดปัญหา โดยพิจารณาว่าข้อมูลใดมีความสำคัญต่อระบบ เช่น บัญชีผู้ใช้งานและรหัสผ่าน ค่า Configuration ของระบบ เป็นต้น

๕.๔ ผู้ดูแลระบบจะต้องเก็บข้อมูลต่าง ๆ รวมทั้งคู่มือที่มาพร้อมกับระบบใหม่ไว้อย่างดี เพื่อใช้ในการแก้ปัญหาในครั้งต่อไป

๕.๕ ผู้ดูแลระบบจะต้องบันทึกข้อมูลที่มีการเปลี่ยนแปลงต่าง ๆ ไว้ในแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form)

๖. การเปลี่ยนแปลง Source Code

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

๖.๒ ผู้ทำหน้าที่ในการเปลี่ยนแปลงแก้ไขต้องถูกจำกัดสิทธิในการเข้าถึงส่วนระบบงานที่ใช้จริง ผู้ทำการแก้ไขจะได้รับอนุญาตให้ทำการคัดสำเนา Source Code เพื่อใช้ในการแก้ไขพัฒนาโปรแกรมในส่วนที่ใช้สำหรับการพัฒนาระบบงาน และทำการย้ายโปรแกรมที่แก้ไขเสร็จเข้าสู่ส่วนที่ใช้สำหรับโอนย้ายโปรแกรมก่อนการย้ายเข้าส่วนที่ใช้งานจริงเท่านั้น

๗. การควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ

ผู้ดูแลระบบหรือหน่วยงานที่ดูแลระบบต้องจัดให้มีการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจที่จัดซื้อ โดยมีแนวทางปฏิบัติดังนี้

๗.๑ หลีกเลี่ยงการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ

๗.๒ ในกรณีที่หลีกเลี่ยงไม่ได้ในการเปลี่ยนแปลงแก้ไข ให้ขออนุญาตเจ้าของลิขสิทธิ์เพื่อเปลี่ยนแปลงแก้ไข หรือมอบให้ผู้ขายดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจให้

๗.๓ ในการเปลี่ยนแปลงซอฟต์แวร์แพ็กเกจ ให้ฝ่ายที่รับผิดชอบเก็บตัวซอฟต์แวร์ต้นฉบับไว้อีกชุดหนึ่ง

๗.๔ ตัวซอฟต์แวร์แพ็กเกจที่แก้ไขจะต้องได้รับการตรวจสอบเป็นอย่างดีว่าจะไม่มีผลกระทบต่อระบบ

๘. การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

หน่วยงานที่ดูแลรับผิดชอบด้านระบบเครือข่ายและคอมพิวเตอร์ หน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยงและหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ร่วมกันกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว ซึ่งมีแนวทางปฏิบัติดังต่อไปนี้

๘.๑ ต้องกำหนดหน้าที่ความรับผิดชอบที่ชัดเจน เช่น การเฝ้าระวังภัยคุกคาม การประเมินความเสี่ยงของภัยคุกคาม การ Patch ปิดช่องโหว่ในระบบ การตรวจสอบทรัพย์สินที่ได้จัดหมวดหมู่ไว้ เป็นต้น

๘.๒ ต้องร่วมกันวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาด ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ทุก ๑๒ เดือน

๘.๓ ในกรณีที่จะทำการ Update Patch ของระบบสำคัญ ๆ ต้องมีการทดสอบและประเมินก่อนว่าจะไม่ก่อให้เกิดความเสียหายต่อระบบ แต่ถ้าไม่สามารถ Update Patch ได้ ก็ให้พิจารณาดังต่อไปนี้

๘.๓.๑ ปิด Service หรือการทำงานที่เกี่ยวข้องกับช่องโหว่

๘.๓.๒ ปรับปรุงหรือเพิ่มระดับ Security ในการเข้าถึงที่บริเวณรอบนอกเครือข่าย โดยเพิ่ม Firewall หรือ IPS (Intrusion Prevention System) เป็นต้น

๘.๓.๓ เพิ่มการเฝ้าระวัง เพื่อตรวจจับหรือป้องกันการโจมตีเครือข่าย

๘.๓.๔ สร้างความตระหนักเกี่ยวกับช่องโหว่ที่เกิดขึ้น

๘.๓.๕ เก็บ Log ของเหตุการณ์ที่เกิดขึ้นทั้งหมดเพื่อใช้ในการตรวจสอบ

๘.๓.๖ กระบวนการบริหารจัดการช่องโหว่ที่มีดำเนินการ ต้องเฝ้าระวัง ให้มั่นใจว่ามีประสิทธิภาพและประสิทธิผล

๘.๓.๗ ระบบที่มีความเสี่ยงสูงจะต้องมีการเตรียมการเป็นอันดับแรกตามลำดับความสำคัญ

๙. แนวทางปฏิบัติของการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (โดยผู้ใช้งาน)

๙.๑ ผู้ร้องขอจะต้องกรอกรายละเอียดลงในแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form by User) โดยผ่านการอนุมัติจากผู้บังคับบัญชา และ/หรือ Process Owner ส่งแบบคำขอการแก้ไข/เปลี่ยนแปลงระบบสารสนเทศไปยังหน่วยงานผู้ดูแลระบบ เช่น หน่วยงานระบบด้าน Hardware Software Database Network เป็นต้น

๙.๒ ในกรณีเร่งด่วน อนุโลมให้ผู้ร้องขอ ส่งแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form by User) ทางโทรสารหรือช่องทางอื่น ๆ ก่อนการส่งต้นฉบับ

๙.๓ หน่วยงานผู้ดูแลระบบกำหนดหมายเลขคำขอเมื่อได้รับแจ้ง โดยใช้ชื่อย่อหน่วยงาน หมายเลข/ปีพ.ศ. เช่น กก.๑/๒๕๕๔

๙.๔ หน่วยงานผู้ดูแลระบบ พิจารณาตามคำขอ โดยศึกษา วิเคราะห์ ผลกระทบจากการแก้ไข แนวทางในการกลับคืนสู่สภาพเดิม (Recovery) กำหนดแนวทางการดำเนินงาน ระยะเวลาและผู้ดำเนินการแก้ไข เช่น ผู้วิเคราะห์ ผู้จัดทำหรือปรับปรุงโปรแกรม ผู้ทดสอบระบบ เป็นต้น

๙.๕ หน่วยงานผู้ดูแลระบบ แจ้งผลการวิเคราะห์กลับไปยังผู้อนุมัติแบบคำขอฯ ในข้อ ๙.๑ เพื่อรับทราบ และ/หรือยืนยัน พร้อมให้แจ้งรายชื่อผู้ดำเนินการทำ User Acceptance Test (UAT) ในกรณีที่หน่วยงานผู้ดูแลระบบเป็นผู้ร้องขอ ที่มีผลกระทบต่อระบบโดยรวม ได้แก่ การเปลี่ยนแปลงเวอร์ชั่นโปรแกรม การแก้ไขระบบเครื่อง Server อุปกรณ์เครือข่าย จะต้องมีการทดสอบยอมรับระบบ (UAT) ก่อนนำไปในระบบใช้งานจริงเสมอ โดยหน่วยงานผู้ดูแลระบบแจ้งหน่วยงานที่เกี่ยวข้องทราบ เพื่อร่วมดำเนินการทำ UAT ต่อไป

๙.๖ หน่วยงานผู้ดูแลระบบดำเนินการตามผลการยืนยันในข้อ ๙.๔

๙.๗ หน่วยงานผู้ดูแลระบบต้องดำเนินการให้ผู้ร้องขอ และ/หรือผู้ใช้งานที่เกี่ยวข้องทำการทดสอบยอมรับระบบ (UAT) พร้อมลงนาม

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

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

๙.๑๐ หน่วยงานผู้ดูแลระบบ แจ้งผู้เกี่ยวข้องนำส่วนที่เปลี่ยนแปลงแก้ไขเข้าสู่ระบบใช้งานจริง (Production) และแจ้งกลับผู้ร้องขอ

๙.๑๑ Process Owner และหน่วยงานผู้ดูแลระบบ ติดตามตรวจสอบ (Monitor and Track Error) ว่าระบบสามารถทำงานได้ถูกต้องตามวัตถุประสงค์ภายในระยะเวลาที่เหมาะสม

๙.๑๒ เมื่อได้ดำเนินงานแล้ว หน่วยงานผู้ดูแลระบบต้องจัดเก็บเอกสารที่เกี่ยวข้อง ได้แก่ แบบคำขอแก้ไขระบบสารสนเทศ แนวทางการดำเนินงาน รายละเอียดการดำเนินงาน เอกสารการทดสอบ คู่มือ ให้สามารถใช้อ้างอิงได้

๑๐. แนวทางปฏิบัติของการเปลี่ยนแปลง/แก้ไขระบบ (โดยผู้ดูแลระบบ)

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

๑๐.๒ ผู้ดูแลระบบ ต้องระบุรายละเอียดในการเปลี่ยนแปลง/แก้ไขระบบเครือข่ายอย่างชัดเจน ได้แก่ วันเวลาที่แจ้ง รายละเอียดของผู้ดูแลระบบ สถานที่ปฏิบัติงานแก้ปัญหา วิธีการแจ้ง ปัญหา/สาเหตุการแก้ไข รายละเอียดของการปฏิบัติงาน ระยะเวลาในการแก้ไข ระบบที่ได้รับผลกระทบ

๑๐.๓ ผู้ดำเนินการแก้ไขต้องมีการเตรียมแผนสำรองฉุกเฉิน ในกรณีที่การเปลี่ยนแปลง/แก้ไขระบบเครือข่ายนั้นเกิดปัญหา เมื่อเกิดการล้มเหลวในการเปลี่ยนแปลง/แก้ไขระบบเครือข่าย ผู้ดำเนินการแก้ไขจะต้องสามารถเปลี่ยนกลับมาใช้ระบบเดิมได้ตามปกติ

๑๐.๔ ผู้ดำเนินการแก้ไขต้องมีการทดสอบให้มั่นใจก่อนใช้งานระบบจริง

๑๐.๕ เมื่อได้ดำเนินงานแล้ว ผู้ดำเนินการแก้ไขต้องลงนามและจัดเก็บเอกสารที่เกี่ยวข้อง เช่น แบบฟอร์มฯ ที่ผู้แจ้งปัญหาหรือผู้ดูแลระบบแจ้งมา เอกสารหรือรายละเอียดของระบบทั้งก่อนและหลังการแก้ไข เป็นต้น เพื่อให้สามารถใช้อ้างอิงได้

หมวด ๑๑
ความสัมพันธ์กับผู้ให้บริการภายนอก
(Supplier Relationships)

เพื่อป้องกันการเข้าถึงทรัพย์สินขององค์กรจากผู้ให้บริการภายนอก โดยกำหนดแนวทางปฏิบัติการบริหารจัดการ และทำข้อตกลงเป็นลายลักษณ์อักษรกับผู้ให้บริการภายนอกในการเข้าถึงทรัพย์สินขององค์กร มีแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศต่อผู้ให้บริการภายนอก ดังนี้

- **แนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการภายนอก**
- **แนวปฏิบัติด้านการบริหารจัดการการส่งมอบบริการ**

แนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการภายนอก

๑. วัตถุประสงค์

แนวปฏิบัตินี้กำหนดขึ้นเพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ในการป้องกันการเข้าถึงทรัพย์สิน และระบบเทคโนโลยีสารสนเทศที่สำคัญขององค์กรตามข้อตกลง การให้บริการของผู้ให้บริการภายนอก

๒. การกำหนดความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการภายนอก

กำหนดกระบวนการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการภายนอกโดยมีแนวทางปฏิบัติดังนี้

๒.๑ ต้องกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรจากผู้ให้บริการภายนอกอย่างเหมาะสม

๒.๒ ต้องกำหนดความมั่นคงปลอดภัยในข้อตกลงกับผู้ให้บริการภายนอกเป็นลายลักษณ์อักษร

๒.๓ ต้องกำหนดลำดับชั้นความลับของข้อมูลและสารสนเทศที่อยู่ในระบบเทคโนโลยีสารสนเทศและไม่อยู่ในระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ให้บริการภายนอกโดยไม่ได้รับอนุญาต

๒.๔ ต้องจัดอบรมด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวเนื่องกับผู้ให้บริการภายนอก ให้กับเจ้าหน้าที่ที่มีส่วนเกี่ยวข้อง

๓. การกำหนดข้อตกลงความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก

เจ้าของข้อมูลและสารสนเทศ ต้องจัดทำ และลงนามยอมรับข้อตกลงกับผู้ให้บริการภายนอกเป็นลายลักษณ์อักษร มีแนวทางการจัดทำข้อตกลงดังนี้

๓.๑ ต้องให้คำแนะนำในการจัดทำข้อตกลง แจ้งให้เจ้าของข้อมูลและสารสนเทศที่เกี่ยวข้องทราบคำแนะนำในการจัดทำข้อตกลงให้สอดคล้องกับการปฏิบัติตามข้อกำหนด ระเบียบปฏิบัติ กฎหมาย และนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๓.๒ ผู้ให้บริการภายนอก ต้องลงนามรับทราบ และยอมรับสัญญาปกปิดความลับ (Non-Discloser Agreement)

๓.๓ ผู้ให้บริการภายนอก ต้องมีส่วนร่วมในการแก้ไขเหตุการณ์ที่ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ (Incident) ที่ผู้ให้บริการภายนอกมีส่วนเกี่ยวข้อง รวมถึงการกู้คืนข้อมูลและระบบเทคโนโลยีสารสนเทศให้กลับสู่สภาวะการทำงานปกติ

๓.๔ ผู้ให้บริการภายนอก ต้องควบคุมการรับจ้างช่วง (Subcontract) โดยจัดทำรายละเอียด การควบคุมให้องค์กร หรือ เจ้าของข้อมูลและสารสนเทศทราบเพื่อป้องกันผลกระทบที่อาจเกี่ยวเนื่องกับการปฏิบัติงาน

๓.๕ ผู้ให้บริการภายนอก ต้องกำหนดรายชื่อทีมงานที่เกี่ยวข้อง รวมถึงผู้ที่สามารถติดต่อได้ ในกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

แนวปฏิบัติด้านการบริหารจัดการการส่งมอบบริการ

๑. วัตถุประสงค์

เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ในการรักษาระดับความสัมพันธ์กับผู้ให้บริการภายนอก ในการบริหารจัดการการส่งมอบบริการตามข้อตกลงที่กำหนดไว้

๒. การเฝ้าระวัง และการตรวจสอบการให้บริการของผู้ให้บริการ

๒.๑ เจ้าของข้อมูลและสารสนเทศและสารสนเทศ ต้องกำหนดมาตรการในการเฝ้าระวัง และตรวจสอบการให้บริการของผู้ให้บริการภายนอก

๒.๒ เจ้าของข้อมูลและสารสนเทศต้องเฝ้าระวังระดับของบริการให้เป็นไปตามข้อตกลง (Service Level Agreement: SLA) ที่ทำไว้กับหน่วยงานภายนอก

๒.๓ เจ้าของข้อมูลและสารสนเทศต้องกำหนดการประชุม เพื่อตรวจสอบความคืบหน้าในการส่งมอบงานของผู้ให้บริการภายนอก

๒.๔ เจ้าของข้อมูลและสารสนเทศต้องกำหนดให้ผู้ให้บริการภายนอกมีส่วนร่วมในการประชุมเพื่อทบทวน และป้องกันเหตุการณ์ที่ไม่พึงประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

๓. การบริหารจัดการการเปลี่ยนแปลงการให้บริการ

ผู้อำนวยการ ที่เป็นเจ้าของระบบเทคโนโลยีสารสนเทศต้องควบคุมการเปลี่ยนแปลง ที่สำคัญต่อระบบ หรือกระบวนการการปฏิบัติงานที่ให้บริการกับหน่วยงานภายในองค์กร ซึ่งเกี่ยวข้องกับผู้ให้บริการภายนอก เช่น การปรับปรุงหรือพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบาย และขั้นตอนปฏิบัติสำหรับความมั่นคงปลอดภัยสารสนเทศ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น โดยจะต้องปรับปรุงเอกสารที่เกี่ยวข้องให้ทันสมัยเมื่อมีการเปลี่ยนแปลง ให้สอดคล้องกับแนวปฏิบัติ การบริหารจัดการการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ

หมวด ๑๒
การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด
(Information Security Incident Management)

จุดประสงค์ เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ สป.พน. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของ สป.พน. โดยมีนโยบายดังนี้

- **แนวปฏิบัติในการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด**

แนวปฏิบัติในการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๑. วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ สป.พน. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของ สป.พน.

๒. การตอบโต้ต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์และการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟท์แวร์

เพื่อลดความเสียหายจากเหตุการณ์ละเมิดความมั่นคงปลอดภัยและระบบทำงานบกพร่อง เช่น ซอฟต์แวร์ประสงค์ร้าย (Malware) ถูกแพร่กระจาย ระบบถูกบุกรุก เป็นต้น และให้บุคลากรใน สป.พน. ได้เรียนรู้จากประสบการณ์ความเสียหายดังกล่าว

๒.๑ การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย

๒.๑.๑ ผู้ใช้งาน ต้องรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบโดยเร่งด่วน

๒.๑.๒ ในกรณีที่ไม่สามารถติดต่อ ผู้ดูแลระบบ ได้ในขณะนั้น ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้น และรายงานให้หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทราบด้วย

๒.๑.๓ ผู้ดูแลระบบ ร่วมกับหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องประเมินขอบเขต (Scope) และความรุนแรง (Severity) ของปัญหา โดยหากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้าง รุนแรง หรือมีผลต่อชื่อเสียงของ สป.พน. จะต้องรายงานให้หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และผู้บริหารเทคโนโลยีสารสนเทศระดับสูงทราบโดยด่วน เพื่อหาแนวทางแก้ไขและป้องกันไม่ให้เกิดในครั้งต่อไป

๒.๒ การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย

๒.๒.๑ ผู้ใช้งาน ต้องรายงานจุดอ่อน ช่องโหว่ หรือภัยที่พบในระบบสารสนเทศที่ใช้งานอยู่ให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบโดยเร่งด่วน

๒.๒.๒ ในกรณีที่ไม่สามารถติดต่อ ผู้ดูแลระบบ ได้ในขณะนั้น ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้น และรายงานให้หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทราบด้วย

๒.๒.๓ ผู้ดูแลระบบ ร่วมกับหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องประเมินขอบเขต (Scope) และความรุนแรง (Severity) ของปัญหา โดยหากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้าง รุนแรง หรือมีผลต่อชื่อเสียงของ สป.พน. จะต้องรายงานให้หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ทราบโดยด่วน เพื่อหาแนวทางแก้ไขและป้องกันไม่ให้เกิดในครั้งต่อไป

๒.๓ การรายงานการทำงานที่บกพร่องหรือทำงานผิดปกติของซอฟต์แวร์

๒.๓.๑ ผู้ใช้งาน ต้องรายงานการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟต์แวร์ที่ใช้งานอยู่ให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบโดยเร่งด่วน

๒.๓.๒ ในกรณีที่ไม่สามารถติดต่อ ผู้ดูแลระบบ ได้ในขณะนั้น ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้น และรายงานให้หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทราบด้วย

๒.๓.๓ ผู้ดูแลระบบ ร่วมกับหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องประเมินขอบเขต (Scope) และความรุนแรง (Severity) ของปัญหา โดยหากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้าง รุนแรง หรือมีผลต่อชื่อเสียงของ สป.พน. จะต้องรายงานให้หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ทราบโดยด่วน เพื่อหาแนวทางแก้ไขและป้องกันไม่ให้เกิดในครั้งต่อไป

๓. การบริหารจัดการและการปรับปรุงแก้ไขต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ต้องยึดหลักปฏิบัติดังต่อไปนี้

๓.๑. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ

ผู้อำนวยการที่มีระบบงานสารสนเทศที่สำคัญ ได้แก่ DPIS, GDX, CRM ฯลฯ เป็นต้น ต้องมีการกำหนดหน้าที่ความรับผิดชอบและกำหนดขั้นตอนปฏิบัติ เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

๓.๒. การเรียนรู้จากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์

๓.๒.๑ ผู้ดูแลระบบ ต้องบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

๓.๒.๒ ผู้ดูแลระบบ มีหน้าที่จัดทำสรุปรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัยให้ผู้บังคับบัญชาและหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยเดือนละ ๑ ครั้ง

๓.๒.๓ หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและหน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง ต้องร่วมกันวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาด ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ทุก ๑๒ เดือน

๓.๓ การเก็บรวบรวมหลักฐาน

๓.๓.๑ หน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องดำเนินการให้หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญ ได้แก่ DPIS, GDX, CRM ฯลฯ ให้มีการรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในการวิเคราะห์ สืบสวน

หรือเป็นหลักฐานในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

๓.๓.๒ หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่า ได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบองค์กร และกฎหมาย (เช่น ๙๐ วัน หรือ ๑ ปี เป็นต้น)

๓.๓.๓ กลุ่มนิติการและหน่วยงานที่มีระบบงานสารสนเทศที่สำคัญ ต้องศึกษากฎเกณฑ์ที่เกี่ยวข้อง ได้แก่ ถ้อยแถลงในกฎหมายแพ่งหรืออาญา ซึ่งระบุถึงลักษณะของหลักฐานที่ต้องเก็บรวบรวมมา เพื่อใช้ในการดำเนินการทางกฎหมายกับผู้กระทำผิด เป็นต้น

๓.๓.๔ หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องศึกษาถึงลักษณะของหลักฐานที่มีความสมบูรณ์และมีคุณภาพ เพื่อสามารถนำไปใช้ในกระบวนการของศาลได้

๔. การรายงานเหตุการณ์น่าสงสัย

๔.๑ ผู้ใช้งาน มีหน้าที่รับผิดชอบในการรายงานเหตุการณ์ทันทีที่สงสัยว่าเป็นเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล

๔.๒ ถ้าหากพบเหตุการณ์ที่น่าสงสัยให้ทำการรายงานต่อผู้ดูแลระบบ หรือผู้อำนวยการทันที ได้แก่เหตุการณ์ต่อไปนี้

๔.๒.๑ พบว่ารหัสผ่านส่วนบุคคลของตนถูกล็อก โดยไม่ทราบสาเหตุ

๔.๒.๒ เวลาการเข้าใช้งานระบบครั้งล่าสุด (Last Logon Time) ที่ผิดปกติ

๔.๒.๓ พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน เช่น มีไฟล์ที่ไม่รู้จัก การเปลี่ยนแปลงของค่าต่าง ๆ เป็นต้น

๔.๒.๔ มีการไม่ปฏิบัติตามขั้นตอนความมั่นคงปลอดภัย

๔.๒.๕ พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล

๔.๒.๖ พบหรือคาดว่าข้อมูลในระบบจะถูกทำลาย แก้ไข หรือลบทิ้ง

๔.๒.๗ มีความพยายามที่จะเข้าใช้ระบบอย่างผิดวิธี ไม่ว่าจะสำเร็จหรือไม่

๔.๒.๘ การให้บริการของระบบเกิดการชะงัก หรือไม่สามารถให้บริการ

๔.๒.๙ เกิดการละเมิดสิทธิ์เข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล

๔.๒.๑๐ การแก้ไขค่าความปลอดภัยในระบบ ได้แก่ Hardware Software หรือ Firmware โดยผู้ใช้งานไม่ทราบ

หมวด ๑๓
การบริหารความต่อเนื่องในการดำเนินงาน
(Government Continuity Management)

จุดประสงค์ เพื่อป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมต่าง ๆ ทางราชการ ป้องกันกระบวนการปฏิบัติราชการที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือภัยที่มีต่อระบบสารสนเทศ และสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม โดยมีนโยบาย ดังนี้

- **แนวปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ**

แนวปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

๑. วัตถุประสงค์

เพื่อใช้ในการปกป้องข้อมูลและทรัพย์สินที่สำคัญที่สุด ต้องทำการสำรองข้อมูลและเก็บรักษาข้อมูลของระบบสารสนเทศที่สำคัญต่อการปฏิบัติราชการของ สป.พน. ไว้ พร้อมทั้งทำการกู้คืนข้อมูล เพื่อให้การปฏิบัติราชการของ สป.พน. เป็นไปอย่างต่อเนื่อง แนวปฏิบัตินี้เป็นส่วนหนึ่งของการสนับสนุนแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ และหน่วยงานที่รับผิดชอบระบบและข้อมูลจะต้องปฏิบัติอย่างเคร่งครัด เพื่อทำให้การปฏิบัติราชการของ สป.พน. เป็นไปอย่างมีประสิทธิภาพ ประสิทธิผล และอย่างต่อเนื่อง

๒. แนวปฏิบัติในการจัดทำแผน

๒.๑. ขั้นตอนเตรียมการของแผนรองรับเหตุการณ์ฉุกเฉิน

๒.๑.๑ สป.พน. ต้องจัดตั้งคณะทำงานแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงานเจ้าของข้อมูลและสารสนเทศ เจ้าของระบบงาน หน่วยงานที่ดูแลระบบเครือข่าย เป็นต้น

๒.๑.๒ กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศต้องประกอบด้วยหัวข้อหลัก ดังนี้

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

๒.๑.๓ แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศต้องพิจารณาดังนี้

- การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการปฏิบัติราชการและการให้บริการของ สป.พน.
- การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย โดยกำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน

- การดำเนินการเพื่อให้สามารถปฏิบัติราชการได้อย่างต่อเนื่อง ได้แก่ การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
- การกลับคืนสู่การทำงานปกติ เพื่อให้งานของ สป.พน. กลับสู่สภาวะปกติ ได้แก่ การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น
- ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบเตรียมพร้อมเมื่อเกิดเหตุฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๒. แนวทางปฏิบัติของการสำรองข้อมูลและการกู้คืนข้อมูล

๒.๒.๑. เจ้าของข้อมูลและสารสนเทศต้องตรวจสอบว่าข้อมูลสำคัญทั้งหมดที่เกี่ยวข้องกับการปฏิบัติราชการของ สป.พน. ได้มีการสำรองข้อมูลอย่างสม่ำเสมอและต่อเนื่อง เจ้าของข้อมูลและสารสนเทศแต่ละระบบมีหน้าที่ที่จะต้องประสานงานกับหน่วยงานดูแลข้อมูลที่เกี่ยวข้องเพื่อให้แน่ใจว่าข้อมูลและฐานข้อมูลได้มีการสำรองข้อมูลเอาไว้อย่างครบถ้วนและเตรียมพร้อมเพื่อนำกลับมาใช้เมื่อเกิดเหตุการณ์ฉุกเฉิน

๒.๒.๒. เจ้าของข้อมูลและสารสนเทศจะเป็นผู้กำหนดตารางเวลาและมีหน้าที่ในการสำรองข้อมูลสำหรับระบบที่รับผิดชอบ ตารางเวลาดังกล่าวต้องสอดคล้องกับผลการประเมินความเสี่ยงที่ยอมรับได้ของข้อมูลที่จัดเก็บ

๒.๒.๓. หน่วยงานที่รับผิดชอบการสำรองข้อมูล ต้องทำการทดลองนำเอาสื่อที่สำรองข้อมูลไว้มาทดสอบอย่างน้อยปีละครั้ง เพื่อให้มั่นใจได้ว่าสามารถนำข้อมูลกลับมาใช้ได้อีกเมื่อเกิดเหตุการณ์ฉุกเฉิน

๒.๒.๔. การทดสอบการนำข้อมูลกลับมาใช้นั้นให้ใช้ข้อมูลสำรองที่ได้จากของระบบงานจริงและกระทำบนระบบสำหรับการทดสอบเท่านั้น

๒.๓ แนวทางปฏิบัติของการสำรองข้อมูลและการกู้คืนข้อมูล (ผู้ดูแลระบบ)

๒.๓.๑ ผู้ดูแลระบบสารสนเทศที่สำคัญนั้น ๆ ต้องสำรองข้อมูลที่สำคัญเก็บไว้ตามระยะเวลาที่เหมาะสม

๒.๓.๒ ผู้ดูแลระบบต้องบันทึกรายละเอียดการสำรองข้อมูลโดยมีรายละเอียด เวลาเริ่มต้นและสิ้นสุด ชื่อผู้ทำการสำรองข้อมูล และชนิดของข้อมูลที่บันทึก

๒.๓.๓ กรณีที่เกิดการผิดพลาดในการสำรองข้อมูล ผู้สำรองข้อมูลต้องบันทึกรายละเอียดของข้อผิดพลาดที่เกิดขึ้นพร้อมแนวทางแก้ไข

๒.๓.๔ ผู้ดูแลระบบต้องมีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมเพื่อให้สามารถกู้ข้อมูลกลับคืนได้ ป้องกันระบบจากการถูกโจมตี หรือความเสียหายที่อาจเกิดขึ้น

๒.๓.๕ ผู้ดูแลระบบต้องเข้ารหัสข้อมูลที่สำรองตามชั้นความลับ โดยใช้เทคโนโลยีที่เหมาะสม เพื่อป้องกันข้อมูลสำรองถูกเปิดเผย

๒.๔ แนวทางปฏิบัติของการเก็บรักษาข้อมูลและสารสนเทศ

๒.๔.๑ เจ้าของข้อมูลและสารสนเทศเป็นผู้จัดเก็บรักษาข้อมูลเกี่ยวกับระบบ ซึ่งได้แก่ ข้อมูลเกี่ยวกับระบบปฏิบัติการ (OS) ระบบเครือข่าย และซอฟต์แวร์ระบบงาน (ทั้ง Source Code และ Executable Files) โดยให้เป็นไปตามความต้องการที่เจ้าของข้อมูลและสารสนเทศในระบบนั้นกำหนด จำนวนครั้งและระยะเวลาในการเก็บรักษาข้อมูลดังกล่าวต้องสอดคล้องกับการประเมินความเสี่ยงของข้อมูลนั้น ๆ ด้วย

๒.๔.๒ ก่อนที่จะมีการปรับปรุงหรือเปลี่ยนแปลงระบบ หน่วยงานที่รับผิดชอบต้องทำการสำรองข้อมูลของระบบทุกครั้ง

๒.๔.๓ ถ้าการสำรองข้อมูลถูกดำเนินการที่เซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์หลัก (Host) และเป็นข้อมูลของระบบงานที่สำคัญจะต้องเพิ่มจำนวนครั้งในการสำรองข้อมูลของเซิร์ฟเวอร์นั้นด้วย

๒.๔.๔ ข้อมูลและสารสนเทศที่มีความสำคัญมากต่อการปฏิบัติราชการของ สป.พน. จะต้องทำการสำรองข้อมูลไว้ทุกวัน และข้อมูลสำรองดังกล่าวต้องมีการจัดเก็บไว้นอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลักอย่างเหมาะสม โดยตรวจสอบให้แน่ใจว่าสถานที่นั้นมีความปลอดภัย

๒.๔.๕ ระบบข้อมูลที่สำคัญทั้งหมดของ สป.พน. ต้องมีระบบการประมวลผลสำรอง ระบบเครือข่ายสำรอง เพื่อป้องกันการพึ่งพาระบบหลักเพียงระบบเดียว ในกรณีที่ระบบหนึ่งไม่สามารถทำงานได้สามารถใช้งานอีกระบบหนึ่งได้ทันทีเพื่อให้งานหลักของ สป.พน. ดำเนินต่อไปได้

๒.๔.๖ ข้อมูลและสารสนเทศที่ถูกจัดประเภทเป็นข้อมูลธรรมดา ซึ่งไม่ส่งผลกระทบต่อการดำเนินกิจการของ สป.พน. จำนวนครั้งในการสำรองข้อมูลนั้นขึ้นอยู่กับการพิจารณาของเจ้าของข้อมูลและสารสนเทศ และข้อมูลดังกล่าวจะถูกนำไปจัดเก็บในสถานที่ ที่มีความปลอดภัย

๒.๕ แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒.๕.๑ คณะทำงานฯ ทำหน้าที่ในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยดำเนินการ ดังนี้

- การประเมินความเสี่ยง (Risk assessment)
- การประมาณความเสี่ยง (Risk estimation)
- การประเมินค่าความเสี่ยง (Risk evaluation)
- จัดทำผลการวิเคราะห์ความเสี่ยง (Risk analysis)
- การจัดการความเสี่ยง (Risk management)
- จัดทำแผนปฏิบัติการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

๒.๕.๒ ดำเนินการทบทวนและตรวจสอบประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

หมวด ๑๔
การปฏิบัติตามข้อกำหนด
(Compliance)

จุดประสงค์ เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อการปฏิบัติราชการน้อยที่สุด โดยมีนโยบาย ดังนี้

- **แนวปฏิบัติตามข้อกำหนดทางกฎหมาย**

แนวปฏิบัติตามข้อกำหนดทางกฎหมาย

๑. วัตถุประสงค์

เพื่อเป็นแนวทางในการปฏิบัติสำหรับการใช้งานซอฟต์แวร์ของ สป.พน. และของบุคคลที่สาม ซึ่งมีการนำมาใช้ภายใน สป.พน. รวมถึงเรื่องของการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมายและข้อกำหนดในการใช้ซอฟต์แวร์ของผู้ใช้งาน และผู้ที่เกี่ยวข้องกับ สป.พน

๒. การระบุข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย

หน่วยงานดูแลรับผิดชอบด้านกฎหมาย ต้องระบุข้อกำหนดทางด้านกฎหมาย ระเบียบปฏิบัติ และสัญญาว่าจ้าง รวมทั้งสัญญาที่ทำกับหน่วยงานภายนอก ที่เกี่ยวข้องกับการดำเนินงานหรือการปฏิบัติราชการของ สป.พน. ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

๓. การปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ในการใช้งานทรัพย์สินทางปัญญา มีแนวทางปฏิบัติ ดังนี้

๓.๑ การจัดซื้อและการนำซอฟต์แวร์ของบุคคลที่สามมาใช้ใน สป.พน. ต้องเป็นไปตามข้อตกลงเรื่องการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมาย (Licensing Agreement) ที่ได้ทำไว้กับเจ้าของลิขสิทธิ์

๓.๒ ผู้ที่ใช้ซอฟต์แวร์บนระบบสารสนเทศของ สป.พน. ต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

๓.๓ มีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับ ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ และต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ มีการตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้อง

๓.๔ ซอฟต์แวร์ที่พัฒนาขึ้นโดย/หรือเพื่อ สป.พน. ถือเป็นทรัพย์สินของ สป.พน. ซึ่งครอบคลุมถึงซอฟต์แวร์หรือระบบงานที่พัฒนาโดยบุคคลภายนอกเพื่อให้กับ สป.พน. ทั้งนี้เพื่อเป็นการป้องกันข้อพิพาทในเรื่องกรรมสิทธิ์ของซอฟต์แวร์ที่อาจเกิดขึ้นหลังจากเสร็จสิ้นโครงการ

๓.๕ ซอฟต์แวร์ที่ถูกพัฒนาโดย เจ้าหน้าที่ ของ สป.พน. ในระหว่างเวลาทำงานถือเป็นทรัพย์สินของ สป.พน.

๓.๖ เครื่องคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์แบบพกพา และเครื่องเซิร์ฟเวอร์ จะต้องตรวจสอบการใช้งานซอฟต์แวร์เป็นประจำว่าได้มีการปฏิบัติตามข้อตกลงเรื่องการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมายซอฟต์แวร์ทั้งหมด

๓.๗ หน่วยงานที่ดูแลรับผิดชอบด้านระบบเครือข่ายและคอมพิวเตอร์และผู้ดูแลระบบ ต้องคอยตรวจสอบซอฟต์แวร์ทั้งหมด ถ้าหากพบว่ามีการละเมิดข้อตกลงจะต้องประสานงานกับเจ้าของระบบเพื่อทำการยกเลิกการติดตั้งหรือลบทิ้งการใช้แชร์แวร์ (Share ware) และฟรีแวร์ (Free ware) จะมีทั้งสามารถทำงานได้อย่างมีประสิทธิภาพและไม่มีประสิทธิภาพหรือไม่มีความปลอดภัยหรือบางครั้งมีชุดคำสั่งที่ไม่พึงประสงค์แอบ

แฝงมาด้วย ซึ่งอาจก่อให้เกิดอันตรายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายได้ ซึ่งผู้ใช้งานซอฟต์แวร์ส่วนมากไม่สามารถประเมินการทำงานและความเสียหายที่เกิดขึ้นจากโปรแกรมได้ ดังนั้นจึงต้องขอรับคำปรึกษากับหน่วยงานดูแลรับผิดชอบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และต้องได้รับการพิจารณาอนุมัติจากผู้ดูแลระบบและผู้ที่เป็นเจ้าของข้อมูลและสารสนเทศ ในการนำแชร์แวร์และฟรีแวร์มาใช้กับระบบสารสนเทศของ สป.พน.

๓.๘ แชร์แวร์ทั้งหมดที่ได้รับอนุญาตให้นำมาใช้ได้และต้องการใช้ต่อหลังจากสิ้นสุดระยะเวลาการทดลองใช้ จะต้องได้รับอนุญาตและมีการลงทะเบียนขอสิทธิ์ในการใช้งานอย่างถูกต้อง และผู้ใช้งานซอฟต์แวร์ดังกล่าวต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์และรายละเอียดข้อบังคับต่าง ๆ ของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

๓.๙ ข้อควรระวัง ในบางครั้งข้อมูลหรือโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ตเป็นแฟ้มข้อมูลที่สามารถประมวลผลเองได้ (Executable Files) เช่น แฟ้มข้อมูลที่มีนามสกุล .exe, .com, .bat และ .dll เป็นต้น ซึ่งอาจมีชุดคำสั่งที่ไม่พึงประสงค์ฝังอยู่ ชุดคำสั่งดังกล่าวไม่เพียงแต่ส่งผลร้ายต่อเครื่องคอมพิวเตอร์เท่านั้น แต่อาจมีผลกระทบถึงระบบเครือข่ายทั้งหมดของ สป.พน. ด้วย

๓.๑๐ การ Download โปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จาก Vendor ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๓.๑๑ การติดตั้งซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์ระบบงาน (Operating System and Application Software) ต้องกระทำโดยบุคคลที่ได้รับอนุญาตเท่านั้น ถ้ามีการติดตั้งซอฟต์แวร์ใด ๆ ในเครื่องคอมพิวเตอร์ของ สป.พน. โดยไม่ได้รับอนุญาต แล้วเกิดข้อพิพาทเกี่ยวกับกฎหมายลิขสิทธิ์และรายละเอียดข้อบังคับต่าง ๆ ของผู้ผลิตซอฟต์แวร์นั้น ๆ ทาง **สป.พน. จะไม่ขอรับผิดชอบไม่ว่ากรณีใด ๆ**

๓.๑๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของ สป.พน. เป็นโปรแกรมที่ สป.พน. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๔. การป้องกันข้อมูลสำคัญของ สป.พน.

เพื่อเป็นการป้องกันข้อมูลสำคัญของ สป.พน. หน่วยงานต่าง ๆ ต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สป.พน. ได้แก่

- แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- แผนป้องกันและแก้ไขปัญหาจากภัยพิบัติต่อระบบสารสนเทศ

๕. การป้องกันข้อมูลส่วนตัวและการเข้ารหัส มีแนวทางการปฏิบัติดังนี้

๕.๑ ผู้ดูแลระบบ ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัวของ เจ้าหน้าที่ ได้แก่ ข้อมูลในจดหมายอิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล เป็นต้น เพื่อใช้เป็นหลักฐานอ้างอิงในทางกฎหมายในกรณีที่มีข้อพิพาทกัน

๕.๒ ผู้ดูแลระบบ ต้องศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายของประเทศ เกี่ยวกับการเข้ารหัสข้อมูล รวมทั้งเมื่อจำเป็นต้องโยกย้ายข้อมูลที่เข้ารหัสไว้ หรืออุปกรณ์ หรือเครื่องมือ หรือระบบที่ใช้ในการเข้ารหัสข้อมูลไปยังอีกประเทศหนึ่ง ให้ศึกษาและปฏิบัติตามข้อกำหนด หรือกฎหมายของประเทศนั้นด้วย

๖. การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิด มีแนวทางปฏิบัติดังนี้

๖.๑ อุปกรณ์ประมวลผลสารสนเทศของ สป.พน. มีไว้เพื่อใช้ในกิจการของ สป.พน. เท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บริหาร สป.พน.

๖.๒ อุปกรณ์ประมวลผลสารสนเทศที่ สป.พน. เช่ามาใช้งาน ต้องกำหนดให้มีหน่วยงานระดับผู้อำนวยการกองขึ้นไปเป็นผู้รับผิดชอบ และหน่วยงานที่เช่า จะต้องจัดทำบัญชีรายการของอุปกรณ์ประมวลผลสารสนเทศที่เช่ามาใช้งาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและทรัพย์สินของ สป.พน.

๖.๓ ผู้อำนวยการกองแต่ละหน่วยงาน ต้องกำหนดให้มีการป้องกันทรัพย์สินและอุปกรณ์ของ สป.พน. ได้แก่ Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน โดยต้องปฏิบัติตามระเบียบในการใช้งานการยืม-คืน

๖.๔ ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลงเพื่อใช้เป็นข้อมูลในการควบคุมทรัพย์สินของ สป.พน.

๖.๕ ผู้ใช้งานต้องไม่ทำการแก้ไขเปลี่ยนแปลง หรืออนุญาตให้ผู้ที่ไม่ได้รับอนุญาตทำการแก้ไขเปลี่ยนแปลงโปรแกรมหรืออุปกรณ์ประมวลผลสารสนเทศในเครื่องที่ตนรับผิดชอบ

๖.๖ ไม่อนุญาตให้ผู้ใช้งานติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องของ สป.พน. การเปลี่ยนแปลงต่อระบบคอมพิวเตอร์ ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูล จะต้องได้รับอนุมัติจากผู้อำนวยการกองที่ดูแลระบบงานนั้น ๆ เป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการหยุดชะงัก หรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

๖.๗ อุปกรณ์ประมวลผลสารสนเทศจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

๖.๘ อุปกรณ์ประมวลผลสารสนเทศต้องมีกระบวนการเพื่ออัปเดทระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ตามนโยบายการใช้งานระบบป้องกันซอฟต์แวร์ประสงค์ร้าย (Malware)สำหรับเครื่องคอมพิวเตอร์ของ สป.พน.

๗. การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด

หน่วยงานต่าง ๆ ซึ่งเป็นเจ้าของข้อมูลและสารสนเทศ ต้องใช้มาตรการการเข้ารหัสข้อมูล (Cryptographic controls) ตามที่ได้กำหนดในนโยบายการพัฒนาระบบสารสนเทศ

๘. การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย

ผู้อำนวยการแต่ละหน่วยงาน ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยของ สป.พน.

๙. การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร

เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคของ สป.พน. จึงต้องปฏิบัติตามแนวทางดังต่อไปนี้

๙.๑ ผู้ดูแลระบบต้องดูแลรักษา ตรวจสอบแก้ไข และเสนอ สป.พน. ให้ปรับปรุงระบบสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อให้ระบบสามารถใช้งานได้ดี มีเสถียรภาพ มีความมั่นคงปลอดภัย และมีประสิทธิภาพอยู่เสมอ

๙.๒ ผู้ดูแลระบบต้องขออนุญาตผู้อำนวยการในกรณีที่มีการร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยสารสนเทศและนโยบายฯ ในการประเมิน ตรวจสอบ ทดสอบ หาจุดอ่อน ช่องโหว่ อันเกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศ และทำการแก้ไขอย่างรวดเร็ว

๙.๓ ผู้อำนวยการแต่ละหน่วยงาน ต้องจัดให้มีการตรวจสอบบัญชีทรัพย์สินตามระยะเวลาที่กำหนดไว้ เพื่อตรวจสอบและแก้ไขปัญหาช่องโหว่ที่เกิดขึ้น

๙.๔ ผู้อำนวยการแต่ละหน่วยงานต้องกำหนดให้มีการตรวจสอบระบบไฟฟ้าสำรอง อย่างน้อยปีละ ๑ ครั้ง

๙.๕ ในกรณีที่มีการเคลื่อนย้าย ผู้ที่รับผิดชอบในการย้ายสถานที่ทำงานต้องทำการตรวจสอบความเรียบร้อยครั้งสุดท้ายทันทีหลังจากที่ทำการย้ายของเสร็จสิ้น รวมทั้งตรวจสอบพื้นที่และทรัพย์สินด้วย การย้ายสถานที่ทำงานเป็นช่วงเวลาที่ต้องระวังเรื่องการรักษาความปลอดภัยที่อาจมีการมองข้ามได้ โดยเฉพาะช่วงเวลาที่ต้องเร่งจัดการย้ายให้เสร็จสิ้น จึงต้องให้ความระมัดระวัง เพราะอาจมีการผ่อนปรนมาตรการรักษาความปลอดภัยต่อข้อมูลที่มีความสำคัญหรือต่อระบบเครือข่ายของ สป.พน. ได้

๙.๖ ผู้ใช้งานต้องมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันซอฟต์แวร์ประสงค์ร้าย (Malware)ที่ใช้ โดยตรวจสอบการ Update ซอฟต์แวร์ป้องกันซอฟต์แวร์ประสงค์ร้าย (Malware)ให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถ Update ซอฟต์แวร์ป้องกันซอฟต์แวร์ประสงค์ร้าย (Malware) ให้ทันสมัยได้

๙.๗ ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เช่น การตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันซอฟต์แวร์ประสงค์ร้าย (Malware) หลีกเลี่ยงในการเปิดไฟล์ที่เป็น Executable file ทั้งไฟล์ .EXE, .COM เป็นต้น

๙.๘ ผู้ใช้งานต้องตรวจสอบหาซอฟต์แวร์ประสงค์ร้าย (Malware) จากสื่อต่าง ๆ ได้แก่ Thump Drive, External Hard Drive ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๙.๙ ต้องมีการตรวจสอบการใช้งานระบบ (Monitoring System Use) อย่างสม่ำเสมอ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศ โดยต้องมีการประเมินความเสี่ยงและปฏิบัติตามที่กฎหมายกำหนด

๙.๑๐ การเข้าสู่ระบบของ สป.พน. จากอินเทอร์เน็ต หรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องตรวจสอบผู้ใช้งานจากสิ่งที่รู้อยู่ ได้แก่ รหัสผ่าน และเพื่อเพิ่มความปลอดภัยการพิสูจน์ตนต้องมีการใช้วิธีการเข้ารหัส (Cryptographic) ร่วมกับการควบคุม

๙.๑๑ ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอก สป.พน. หน่วยงานที่รับผิดชอบต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ สำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิที่ได้รับ และตรวจสอบการใช้งานอย่างสม่ำเสมอ

๑๐. มาตรการการตรวจประเมินระบบสารสนเทศ

ผู้อำนวยการที่ดูแลระบบงานสำคัญหรือระบบสารสนเทศที่มีข้อมูลความลับของ สป.พน. ได้แก่ DPIS, GDX, CRMฯลฯ เป็นต้น ต้องวางแผนการตรวจประเมินระบบทั้งหมด โดยการตรวจประเมินที่จะดำเนินการ จะต้องมีผลกระทบต่อระบบและกระบวนการดำเนินงานของ สป.พน. น้อยที่สุด

๑๑. การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบ

หน่วยงานดูแลรับผิดชอบด้านตรวจสอบภายใน หน่วยงานที่ดูแลรับผิดชอบด้านระบบเครือข่ายและคอมพิวเตอร์ และหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยสารสนเทศและนโยบายฯ ต้องร่วมกันหาทางป้องกันซอฟต์แวร์ที่ใช้ในการตรวจประเมินระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิดหรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น ๆ

ศูนย์เทคโนยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงพลังงาน
ชั้น 22 555/2 อาคารบี ENCO
ถ. วิภาวดีฯ เขตจตุจักร กทม. 10900
โทร. 02-140-6406