2569

นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมพัฒนาสังคมและสวัสดิการ
กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

คำนำ

ในปัจจุบัน การดำเนินงานของภาครัฐมีการพึ่งพาระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์เป็นกลไกหลักในการขับเคลื่อนภารกิจและการให้บริการประชาชน กรมพัฒนาสังคมและสวัสดิการจึงตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ อีกทั้งยังเป็นการป้องกันภัยคุกคามรูปแบบต่างๆ ที่อาจส่งผลกระทบต่อความต่อเนื่องในการดำเนินงานของกรม

เอกสารฉบับนี้จัดทำขึ้นเพื่อกำหนดทิศทาง มาตรฐาน และแนวปฏิบัติให้ข้าราชการ รวมถึงเจ้าหน้าที่ทุกระดับ ได้มีความรู้ความเข้าใจ และถือปฏิบัติอย่างเคร่งครัด โดยเนื้อหาครอบคลุมตั้งแต่การจัดการสินทรัพย์ การควบคุมการเข้าถึงระบบ การบริหารจัดการเหตุการณ์ไม่พึงประสงค์ ไปจนถึงแผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติ กรมฯ หวังเป็นอย่างยิ่งว่านโยบายฉบับนี้จะเป็นเครื่องมือสำคัญในการสร้าง ความเชื่อมั่น และยกระดับมาตรฐานการรักษาความปลอดภัยสารสนเทศให้สอดคล้องกับมาตรฐานสากลและกฎหมายที่เกี่ยวข้องอย่างยั่งยืน

กองยุทธศาสตร์และแผนงาน
กรมพัฒนาสังคมและสวัสดิการ

สารบัญ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ในมาตรา 5 “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ หรือต่อไปนี้เรียกว่า “กรม” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ กรมจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

วัตถุประสงค์

1. เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศเครือข่ายคอมพิวเตอร์ของกรม ทำให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล
2. เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมตามมาตรฐาน ISO/IEC 27001
3. เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้ข้าราชการและเจ้าหน้าที่ทุกระดับในกรมได้รับทราบและปฏิบัติตามอย่างเคร่งครัด
4. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร ข้าราชการ เจ้าหน้าที่ ผู้แลระบบและบุคคลภายนอกที่ปฏิบัติงานร่วมกับกรม ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศของกรม
5. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ
6. เพื่อส่งเสริมให้ข้าราชการและเจ้าหน้าที่ของกรมมีความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

องค์ประกอบนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของกรม จะประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม เพื่อที่จะทำให้กรมมีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรของกรม ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของกรม ซึ่งข้าราชการและเจ้าหน้าที่ของกรม และหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด โดยจักแบ่งสาระสำคัญออกเป็น 9 หมวด ประกอบด้วย

หมวดที่ 1 นโยบายความมั่นคงปลอดภัย
หมวดที่ 2 การจัดการสินทรัพย์สารสนเทศ
หมวดที่ 3 การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย
หมวดที่ 4 การบริหารจัดการด้านการดำเนินงาน
หมวดที่ 5 การสร้างความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
หมวดที่ 6 การจัดหาพัฒนาและบำรุงรักษาระบบสารสนเทศ
หมวดที่ 7 การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ
หมวดที่ 8 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ
หมวดที่ 9 การจัดองค์กรปฏิบัติการเมื่อเกิดสถานการณ์ฉุกเฉิน

คำนิยาม

คำศัพท์	ความหมาย
กรม	กรมพัฒนาสังคมและสวัสดิการ
ผู้บังคับบัญชา	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมพัฒนาสังคมและสวัสดิการ
กลุ่มเทคโนโลยีสารสนเทศ	หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ ระบบปฏิบัติการ ชุดคำสั่งโปรแกรมและเครือข่ายภายในกรมพัฒนาสังคมและสวัสดิการ
หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ	ผู้มีอำนาจในการบริหารจัดการเทคโนโลยีสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ
ความมั่นคงปลอดภัยด้านสารสนเทศ	ความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ
มาตรฐาน (Standard)	บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
วิธีการปฏิบัติ (Procedure)	รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
แนวทางปฏิบัติ (Guideline)	แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้บรรลุเป้าหมายได้ง่ายขึ้น
ผู้ใช้งาน	บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งองค์กรกำหนดไว้
ผู้บริหาร	ผู้มีอำนาจบริหารในระดับสูงของกรมพัฒนาสังคมแลสวัสดิการ
ผู้ดูแลระบบ (System Administrator)	เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
เจ้าหน้าที่	ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการขององค์กร
หน่วยงานภายนอก	องค์กรหรือหน่วยงานที่กรมพัฒนาสังคมและสวัสดิการอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะรับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
สิทธิ์ของผู้ใช้งาน	สิทธิ์และหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับระบบสารสนเทศ

ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
สารสนเทศ (Information)	ข้อเท็จจริงที่ได้จากการการนำข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
ระบบคอมพิวเตอร์	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
ระบบเครือข่าย (Network System)	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของกรมได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Intranet)
ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
ระบบอินเทอร์เน็ต (Intranet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
ระบบเครือข่ายไร้สาย (Wireless LAN : WLAN)	ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ รวมถึงการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์กับอุปกรณ์เครือข่ายโดยปราศจากการใช้สายสัญญาณในการเชื่อมต่อ แต่ใช้คลื่นวิทยุเป็นช่องทางการสื่อสารแทน
ระบบเทคโนโลยีสารสนเทศ (Information Technology System)	ระบบของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศ ที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและการควบคุมการสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศเป็นต้น
อุปกรณ์ประมวลผล (Computing Device)	อุปกรณ์ที่มีหน่วยประมวลผล หน่วยความจำ ส่วนบันทึกข้อมูล ส่วนการเชื่อมต่อเครือข่าย ส่วนรับข้อมูล และส่วนแสดงผล เช่น คอมพิวเตอร์แบบตั้งโต๊ะ คอมพิวเตอร์แบบพกพา เป็นต้น
อุปกรณ์เคลื่อนที่ (Mobile Device)	อุปกรณ์ประมวลผลแบบพกพก ที่มีขนาดเล็กสามารถใช้เพียงมือเดียวในการใช้งาน ส่วนของการรับข้อมูลเป็นแบบสัมผัส ททโดยไม่

	ต้องใช้ Keyboard และสามารถเชื่อมต่อเครือข่ายแบบไร้สาย เครือข่ายโทรศัพท์ได้ เช่น Smartphone, Tablet เป็นต้น
พื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร (Information System Workspace)	พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
General working area	พื้นที่ทำงานทั่วไป พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์แบบพกพาประจำโต๊ะทำงาน
System administrator area	พื้นที่ทำงานของผู้ดูแลระบบ
IT equipment or network area	พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์แบบพกพาประจำโต๊ะทำงาน
Data storage area	พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์
เจ้าของข้อมูล (Information Owner)	ผู้ที่รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือเป็นผู้ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
เจ้าของระบบงาน (System Owner)	ผู้มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในหน่วยงาน
สินทรัพย์ (Asset)	ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
จดหมายอิเล็กทรอนิกส์ (e - mail)	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่จะส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้
สื่อสังคมออนไลน์ (Social Media)	สังคมออนไลน์ที่ผู้ใช้อินเทอร์เน็ตสามารถแลกเปลี่ยนประสบการณ์ซึ่งกันและกันโดยใช้สื่อต่างๆ เป็นตัวแทนในการสนทนา ทั้งในรูปแบบสื่อสิ่งพิมพ์ สื่อสนทนา การส่งข้อความ วีดีโอ ภาพกราฟิก
การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การตรวจสอบ การอนุมัติ และการกำหนดสิทธิในการผ่านเข้าสู่ระบบสารสนเทศให้แก่ผู้ใช้งาน โดยที่เจ้าของข้อมูลอนุญาตให้ใช้งานระบบสารสนเทศนั้นได้
รหัสผ่าน (Password)	ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์	ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
สถานการณ์ความเสี่ยง	ความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศของกรม สามารถแยกเป็นภัยต่างๆ ได้ 4 ประเภท ได้แก่ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error), ภัยที่เกิดจาก Software, ภัยที่เกิดจากไฟไหม้หรือระบบไฟฟ้า และภัยที่เกิดจากน้ำท่วม (อุทกภัย)
สถานการณ์ความไม่แน่นอนและภัยพิบัติ	บุคลากรของหน่วยงาน สถานการณ์หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผยหรือเปลี่ยนแปลง ทำลาย ปฏิเสธการทำงานหรือการกระทำอื่นๆ
แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ	ข้อปฏิบัติในการแก้ไขปัญหาเมื่อเกิดสถานการณ์ความไม่แน่นอนหรือภัยพิบัติ แบ่งเป็น 3 ด้าน แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ (Contingency Plan) แผนดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan) และแผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and RecoveryProcedure)
ปัญญาประดิษฐ์ (Artificial Intelligence : AI)	ระบบคอมพิวเตอร์ที่ถูกออกแบบให้มีความสามารถในการเรียนรู้ การคิดวิเคราะห์ การตัดสินใจ และการสร้างสรรค์เนื้อหา ซึ่งรวมถึง Machine Learning (ML) และ Generative AI ที่นำมาใช้เพื่อสนับสนุนงานบริการทางสังคมของหน่วยงาน
วิทยาการคำนวณเชิงควอนตัม (Quantum Computing)	เทคโนโลยีการประมวลผลขั้นสูงที่ใช้หลักการทางควอนตัมฟิสิกส์ ซึ่งในอนาคตอันใกล้จะมีขีดความสามารถในการถอดรหัสลับ (Cryptography) มาตรฐานปัจจุบันที่หน่วยงานใช้งานอยู่
สถาปัตยกรรมความน่าเชื่อถือเป็นศูนย์ (Zero Trust Architecture: ZTA)	แนวคิดการรักษาความมั่นคงปลอดภัยที่ตั้งอยู่บนพื้นฐานว่า "อย่าเชื่อถือสิ่งใดโดยเด็ดขาด จนกว่าจะได้รับการตรวจสอบ" (Never Trust, Always Verify) โดยไม่คำนึงว่าผู้ใช้งานหรืออุปกรณ์นั้นจะอยู่ภายในหรือภายนอกเครือข่ายของหน่วยงาน

หมวดที่ 1 นโยบายความมั่นคงปลอดภัย
(Security Policy)

วัตถุประสงค์

เพื่อกำหนดทิศทางหลักการและกรอบของข้อกำหนดในการป้องกันทรัพย์สินที่เกี่ยวข้องกับสารสนเทศให้ปลอดภัยจากภัยคุกคามที่อาจก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลและระบบงานสารสนเทศ เพื่อผลักดันให้มีการควบคุมภายในด้านสารสนเทศที่รัดกุมตามแนวความเสี่ยง (Risk Based Approach) ที่สอดคล้องกับมาตรฐานสากล และเพื่อสนับสนุนให้ผู้ใช้งานตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศรวมถึงความสำคัญในการบริหารจัดการความเสี่ยงด้านสารสนเทศ

ข้อกำหนดตามกฎหมาย/มาตรฐานระดับสากล

1. กฎหมายธุรกรรมทางอิเล็กทรอนิกส์
2. กฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์
3. กฎหมายลิขสิทธิ์
4. มาตรฐานสากล ISO/IEC 27001

ข้อปฏิบัติ

1. ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับชอบความเสี่ยงความเสียหายต่อระบบสารสนเทศของกรม ซึ่งเกิดจากการละเลย ละเว้นการควบคุมความมั่นคงปลอดภัยสารสนเทศ
2. ให้การสนับสนุนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ
3. ต้องจัดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยการประเมินความเสี่ยงดังกล่าวต้องพิจารณาถึงบริบทภายใน (Internal Context) บริบทภายนอก (External Context) ผู้ มีส่วนได้ส่วนเสีย (Interested Party) วิสัยทัศน์ พันธกิจที่กรมกำหนดไว้
4. ต้องจัดให้มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงบริบทต่างๆ และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศของกรม
5. ต้องประเมินผลสัมฤทธิ์ของนโยบายที่ประกาศใช้ เพื่อนำมาปรับปรุงนโยบาย แผนกลยุทธ์ให้สอดคล้องกับภัยคุกคามในปัจจุบัน และที่อาจเกิดขึ้นในอนาคต
6. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศต้องจัดทำเป็นลายลักษณ์อักษรตามวัตถุประสงค์และขอบเขตต้องได้รับการอนุมัติ เพื่อประกาศใช้และถือปฏิบัติทั่วทั้งกรม โดยให้มีผลบังคับใช้กับข้าราชการ เจ้าหน้าที่ และหน่วยงานภายนอก (External Party) ที่เกี่ยวข้องกับการใช้ข้อมูลและสินทรัพย์สารสนเทศของกรม

7. ต้องสนับสนุนให้มีการอบรมเพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
8. ต้องตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยโดยผู้ตรวจประเมินภายในหรือผู้ตรวจสอบจากภายนอกอย่างน้อยปีละ 1 ครั้ง และติดตามผลการประเมินเพื่อปรับปรุง ป้องกัน หรือแก้ไขปัญหาที่พบ
9. ห้ามมิให้บุคลากรนำข้อมูลส่วนบุคคล ข้อมูลกลุ่มเปราะบาง หรือข้อมูลความลับทางราชการป้อนเข้าสู่ระบบปัญญาประดิษฐ์สาธารณะ (Public Generative AI) ที่ไม่ได้รับการรับอนุญาตจากกรมพัฒนาสังคมและสวัสดิการ หรือได้รับการรับรองความปลอดภัยจากกลุ่มเทคโนโลยีสารสนเทศโดยเด็ดขาด

หมวดที่ 2 การจัดการสินทรัพย์สารสนเทศ
(Information Asset Management)

วัตถุประสงค์

เพื่อให้มีการระบุทรัพย์สินของกรมและกำหนดหน้าที่ความรับผิดชอบในการป้องกันสินทรัพย์จากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจขึ้นอย่างเหมาะสม โดยประกอบด้วย

- นโยบายการบริหารจัดการสินทรัพย์ (Asset Management Policy)
- นโยบายการจัดชั้นความลับสารสนเทศ (Information Classification Policy)

นโยบายการบริหารจัดการสินทรัพย์ (Asset Management Policy)

วัตถุประสงค์

เพื่อให้มีการระบุสินทรัพย์ของกรมและกำหนดหน้าที่ความรับผิดชอบในการป้องภัยและปกป้องสินทรัพย์อย่างเหมาะสม

ข้อปฏิบัติ

1. ต้องจัดทำและเก็บทะเบียนสินทรัพย์ ซึ่งรวมถึงสินทรัพย์ข้อมูลและเอกสาร (Information and Document Asset) สินทรัพย์ซอฟท์แวร์ (Software Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) และปรับปรุงข้อมูลให้ถูกต้องอยู่เสมอ
2. ต้องมีการตรวจสอบสินทรัพย์ (Inventory Check) ต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ทุกประเภท ตามระยะเวลาที่กำหนดไว้ หรือเมื่อ มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น
3. ต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์ เมื่อมีสินทรัพย์ใหม่หรือสินทรัพย์ที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น
4. ต้องกำหนดบุคคล หรือผู้รับผิดชอบข้อมูลและสินทรัพย์ทั้งหมดด้านเทคโนโลยีสารสนเทศของกรมอย่างชัดเจน
5. ต้องกำหนด แสดง บันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูลสารสนเทศและสินทรัพย์
6. ต้องจัดทำข้อกำหนดการใช้งานสินทรัพย์ การบำรุงรักษาให้เหมาะสมกับการใช้งานสินทรัพย์แต่ละประเภทแก่ผู้ใช้งาน ตามประกาศของกรม

6.1 การใช้งานอุปกรณ์คอมพิวเตอร์

วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งาน การบำรุงรักษา การป้องกันและปกป้องภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมยและสิ่งที่สร้างความเสียหายที่อาจขึ้นอย่างเหมาะสม

- ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่กรมเป็นผู้จัดหามานั้น ถือเป็นทรัพย์สินของกรม มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของกรม
- เจ้าหน้าที่ ตลอดจนหน่วยงานภายนอกที่ได้รับการว่าจ้างโดยกรม จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงไว้ซึ่งความถูกต้องโดยหมายรวมถึงข้อมูล และระบบสารสนเทศของกรม
- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ ของกรม อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน
- อุปกรณ์คอมพิวเตอร์ของกรม ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใดๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้นๆ
- การคืน หรือส่งซ่อมอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของกรมให้เป็นหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศเท่านั้น ห้ามมิให้ผู้ใช้งานดำเนินการซ่อม หรือส่งซ่อมด้วยตนเอง
- ไม่ใช่อุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของกรมผิดวัตถุประสงค์และหลีกเลี่ยงการใช้อุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ในสภาวะแวดล้อมที่มีผลกระทบต่ออุปกรณ์
- ห้ามมิให้ผู้ใช้งานทำการปิด ยกเลิก การกระทำใดๆ ที่อาจส่งผลต่อระบบการป้องกันไวรัสหรือระบบป้องกันมัลแวร์อื่นใด ที่ติดตั้งอยู่บนระบบคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่
- หากพบว่าโปรแกรมป้องกันไวรัสในอุปกรณ์ประมวลผล หรืออุปกรณ์เคลื่อนที่ทำงานผิดพลาด หรือไม่ทำงาน หรือสงสัยว่าอุปกรณ์ดังกล่าวติดมัลแวร์ หรือพบข้อมูลภัยคุกคาม ผู้ใช้งานต้องยุติการเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายและให้แจ้งกลุ่มงานเทคโนโลยีสารสนเทศทราบในทันที
- ไม่ติดตั้ง หรือใช้งานโปรแกรมเพิ่มเติม โดยไม่ได้รับอนุญาต และไม่ติดตั้งหรือใช้งานโปรแกรมที่สุ่มเสี่ยงกับการกระทำผิดกฎหมายและละเมิดลิขสิทธิ์ในอุปกรณ์ประมวลผล อุปกรณ์เคลื่อนที่ของกรม

6.2 การใช้งานโทรสาร เครื่องพิมพ์ เครื่องถ่ายเอกสาร และอุปกรณ์ต่อพ่วงอื่น วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งาน การบำรุงรักษา การป้องกันและปกป้องภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมยและสิ่งที่สร้างความเสียหายที่อาจขึ้นอย่างเหมาะสม

- ผู้ใช้งานต้องรับผิดชอบในการใช้งานโทรสาร เครื่องพิมพ์ เครื่องถ่ายเอกสาร และอุปกรณ์ต่อพ่วงอื่นของกรม อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน
- ผู้ใช้งานต้องปกป้องความมั่นคงปลอดภัยของข้อมูลลับอย่างเต็มที่ เมื่อจำเป็นต้องส่งข้อมูลนั้นผ่านเครื่องโทรสาร ตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. 2544
- หากผู้ใช้งานได้รับข้อมูลจากการส่งโทรสารที่ผิดพลาด ตัวอย่าง เช่น ส่งโทรสารผิด หมายเลขผิดส่วนงาน เป็นต้น ผู้ใช้งานต้องแจ้งให้ผู้ส่งโทรสารนั้นรับทราบ และทำลายเอกสารข้อมูลนั้น
- ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น
- ผู้ใช้งานต้องขออนุญาตจากเจ้าของข้อมูลก่อนทำการถ่ายเอกสารหรือสแกนเอกสารที่มีข้อมูลลับ โดยสำเนาเอกสารนั้นต้องได้รับการปกป้องดูแลในระดับเทียบเท่ากับเอกสารต้นฉบับตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. 2544
- มีบันทึกเกี่ยวกับการติดต่อสื่อสารข้อมูลผ่านเครื่องโทรสารที่สามารถติดตามและสอบกลับได้ (ระบุหมายเลข และจำนวนเอกสาร)

7. ต้องกำหนดวิธีปฏิบัติงานเรื่องการส่งคืนทรัพย์สิน (Return of assets) เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลง ของข้าราชการ เจ้าหน้าที่ หรือหน่วยงานภายนอกที่ใช้สินทรัพย์ของกรมต้องคืนทรัพย์สินของกรมทั้งหมดที่ตนเองถือครองให้ครบถ้วน

นโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy)

วัตถุประสงค์

เพื่อให้สารสนเทศของกรมได้รับการปกป้องที่เหมาะสม และสอดคล้องกับความสำคัญของสารสนเทศนั้นๆ

ข้อปฏิบัติ

1. **ชั้นความลับของสารสนเทศ (Classification of Information)**
    - การจัดระดับชั้นความลับต้องพิจารณาถึงข้อกำหนดด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
    - ต้องกำหนดประเภทของข้อมูล ระดับความสำคัญ ลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง และช่องทางการเข้าถึง เพื่อป้องกันสารสนเทศให้มีความปลอดภัยด้วยวิธีการที่เหมาะสมตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. 2544
    - ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
    - เจ้าของข้อมูล จะต้องมีการตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม
    - วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
    - การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล
    - ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
    - ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรม เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น
    - เอกสารหรือสิ่งตีพิมพ์ ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับนั้น
    - กรมต้องจัดทำและปรับปรุงบัญชีรายการอัลกอริทึมการเข้ารหัสลับที่หน่วยงานใช้งานอยู่ เพื่อวางแผนยกระดับการเข้ารหัสให้เป็นไปตามมาตรฐานที่ทนทานต่อการโจมตีจากควอนตัมคอมพิวเตอร์ (Post-Quantum Cryptography: PQC) ในอนาคต

2. การจัดการสินทรัพย์ (Handling of Asset)

- ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น
- ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการหรือระบบสารสนเทศอย่างเหมาะสม
- สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่างๆ เช่น USB-Drive, CD-Rom เป็นต้น ที่มีข้อมูลลับของกรม บันทึกอยู่ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

หมวดที่ 3 การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย (Information and Network Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของกรม และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคล ที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของกรมได้อย่างถูกต้อง ประกอบด้วย

- กระบวนการหลักในการควบคุมการเข้าถึงระบบ
- การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
- การบริหารจัดการการเข้าถึงระบบเครือข่าย
- การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
- การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
- การใช้งานอินเทอร์เน็ต
- การใช้งานจดหมายอิเล็กทรอนิกส์
- การใช้สื่อสังคมออนไลน์ในฐานะหน่วยงานของกรม
- การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

กระบวนการหลักในการควบคุมการเข้าถึงระบบ

1. สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น
2. ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
3. ผู้ดูและระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้
4. ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ
5. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐาน ในการตรวจสอบหากมีปัญหาเกิดขึ้น

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

1. ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการ ขออนุญาตเข้าระบบงานนั้น การกำหนดสิทธิของผู้ใช้งานต้องได้รับการควบคุมอย่างเหมาะสมตามความต้องการในการใช้งาน ระดับความสำคัญ และต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน
2. เจ้าของข้อมูลและ **“เจ้าของระบบงาน”** จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จำนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น
3. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ
4. การเข้าถึงระบบสารสนเทศที่สำคัญ และระบบฐานข้อมูลกลุ่มเป้าหมายของกรมพัฒนาสังคมและสวัสดิการ จะต้องอยู่ภายใต้หลักการให้สิทธิเท่าที่จำเป็น ตามหลักการ Zero Trust Architecture

การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม

1. การลงทะเบียนเจ้าหน้าที่ใหม่ของกรม ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ สำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป ต้องทำภายใน 24 ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน 7 วัน
2. กำหนดสิทธิการใช้ระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e - mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้ง ต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
3. ผู้ใช้งาน ต้องลงนามรับทราบสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด
4. การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านเจ้าหน้าที่
    4.1 ผู้ดูแลระบบ ที่รับผิดชอบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ
    4.2 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยพิจารณาดังนี้

4.2.1 ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้นๆควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

4.2.2 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

4.2.3 ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน

ข้อปฏิบัติการลงทะเบียนผู้ใช้งาน (User Registration)

1. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ
2. ผู้ดูแลระบบ ต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน
3. ผู้ดูแลระบบ ต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
4. ผู้ดูแลระบบ ต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว
5. ผู้ดูแลระบบ ต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน
6. การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

การบริหารจัดการการเข้าถึงระบบเครือข่าย (Network Access Management)

1. ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ
2. ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
3. ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน
4. ผู้แลระบบ ควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (enforced path) จากเครื่องลูกข่าย ไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้
5. ผู้ดูแลระบบต้องรับผิดชอบในการตรวจสอบและดูแลอุปกรณ์ที่เกี่ยวข้องในระบบเครือข่ายทั้งหมด รวมทั้งอุปกรณ์ที่ใช้สำหรับการเข้าถึงระยะไกล (Remote Equipment) และอุปกรณ์ที่อยู่ในพื้นที่ของผู้ใช้งานตามเอกสารการตรวจสอบและดูแลระบบเทคโนโลยีสารสนเทศ
6. ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการ

ทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้ทราบทุกครั้ง

7. ระบบเครือข่ายทั้งหมดของกรมที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกกรม ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามรถในการตรวจจับ มัลแวร์ (Malware) ด้วย
8. การเข้าสู่ระบบงานเครือข่ายภายในกรม โดยผ่านอินเทอร์เน็ตจำเป็นต้องมีการล็อกอิน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง
9. IP address ภายในของระบบงานเครือข่ายภายในกรม จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรับรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของกลุ่มเทคโนโลยีสารสนเทศได้โดยง่าย
10. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
11. การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น
12. การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ เท่านั้น
13. อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมโยงเครือข่าย ต้องปิด Service Port ที่ไม่จำเป็นและการส่งข้อมูลการทำงานของอุปกรณ์เครือข่าจะต้องไม่ใช่ค่า Default Community, Default Username และ Default Password
14. ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งตนไม่มีสิทธิ์ในการเข้าถึงข้อมูลนั้น

การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

1. กำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน
2. มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที
3. เปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น ftp หรือ ping เป็นต้น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการเพิ่มเติมด้วย และการกำหนด Access Control Port List ของตัวอุปกรณ์สื่อสารเพื่อลดช่องโหว่ต่างๆ อย่างเหมาะสม

4. ติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น web server
5. มีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไข หรือบำรุงรักษา
6. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย จะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ เท่านั้น
7. การสำรองค่า Configuration ของเครื่องคอมพิวเตอร์แม่ข่ายทุกครั้งที่ติดตั้ง หรือมีการเปลี่ยนแปลง หรือตามระยะเวลาที่กำหนด
8. อุปกรณ์แม่ข่ายและอุปกรณ์เครือข่ายต้องกำหนดรหัสผ่านสำหรับบัญชีรายชื่อซึ่งใช้ในการบริหารจัดการอุปกรณ์บนระบบเครือข่าย
9. ผู้ดูแลระบบเครือข่ายต้องสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยเดือนละครั้ง และทดสอบการสำรองข้อมูลอย่างน้อยปีละ 2 ครั้ง โดยสอดคล้องกับความสำคัญของระบบ

การบริหารจัดการบันทึกและตรวจสอบ

1. กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่นบันทึก การเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ firewall log เป็นต้น เพื่อประโยชน์ในการตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน
2. มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
3. มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์สารสนเทศ

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

1. การเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายองค์กร ต้องควบคุมบุคคลที่จะเข้าสู่ระบบขององค์กรจากระยะไกลโดยกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน ต้องมีการตรวจสอบข้อมูล และพิสูจน์ตัวตนของผู้ใช้งาน
2. วิธีการใดๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของกรมในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด
3. การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ และจะต้องทำการอนุมัติให้เป็นรายครั้ง หรือเป็นช่วงระยะเวลาจำกัดแล้วแต่กรณีและความจำเป็น

4. มีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม
5. สิทธิ์ในการใช้งาน Remote Access เพื่อปฏิบัติงานชั่วคราวเป็นสิทธิ์ที่กรมจะให้เฉพาะผู้ใช้งานผู้ให้บริการภายนอกเป็นการชั่วคราวเท่านั้น ไม่สามารถถ่ายโอนกันได้
6. การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น
7. อุปกรณ์ที่ทำหน้าที่ Remote Access ต้องมีการปรับปรุงช่องโหว่อย่างสม่ำเสมอ
8. กรมมีสิทธิ์เรียกร้องความรับผิดชอบ หากระบบคอมพิวเตอร์ของกรมได้รับความเสียหายโดยการติดตั้งไวรัสคอมพิวเตอร์ จากการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว

การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร ดังนี้

- แสดงชื่อผู้ใช้งาน (Username)
- ใส่รหัสผ่าน (Password)

เมื่อมีการพิสูจน์ตัวตน ระบบจะตรวจสอบสิทธิการใช้งานตามขั้นตอนอย่างมีประสิทธิภาพ โดยระบบจะยอมให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตผ่านเข้าสู่เครือข่าย และใช้บริการได้ตามสิทธิที่กำหนดไว้ เท่านั้น

การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

1. ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
2. ผู้ดูและระบบ ต้องกำหนดสิทธิในการเข้าถึงอย่างเหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ
3. ผู้ดูแลระบบ ต้องมอบหมายสิทธิให้มีความสอดคล้องกับนโยบายควบคุมการเข้าถึง
4. ผู้ดูแลระบบ ต้องจัดเก็บเอกสารการมอบหมายสิทธิแก่ผู้ใช้งาน
5. กรณีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ระบบบริหารจัดการรหัสผ่าน (Password management system)

1. ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคลเพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้
2. ระบบบริหารจัดการรหัสผ่านต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนปฏิบัติ เพื่อยืนยันรหัสผ่านใหม่
3. ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเลือกรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่น
4. ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุกๆ 6 เดือน

5. ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชีผู้ใช้งานและทำการล็อกอินเข้าใช้งานระบบเป็นครั้งแรก
6. ระบบบริหารจัดการรหัสผ่านต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน เช่น ให้แสดงเป็นเครื่องหมาย (*) บนหน้าจอ เป็นต้น
7. ระบบบริหารจัดการรหัสผ่านควรป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้ หรือที่จำเป็นต้องมีการส่งไปในเครือข่ายเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

1. ผู้ดูแลระบบ ต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
2. ผู้ดูแลระบบ ต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราวและควรเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น
3. ผู้ดูแลระบบ ต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและควรกำหนดรหัสผ่านที่แตกต่างกัน
4. ผู้ดูแลระบบ ต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้จดหมายอิเล็กทรอนิกส์เป็นช่องทางในการส่งและกำหนดผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

1. ผู้ดูแลระบบ ดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน 1 ครั้ง / ปี เป็นอย่างน้อย
2. ผู้ดูแลระบบ ทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง เช่น สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป
3. ผู้ดูแลระบบ ทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน
4. ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูงเพื่อใช้ในการทบทวนในภายหลัง
5. สิทธิการเข้าถึงของหน่วยงานภายนอก หรือผู้ให้บริการภายนอก (Third Party) ต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการดำเนินงาน หมดสัญญา หรือสิ้นสุดข้อตกลงทันที และต้องมีการปรับปรุงให้เป็นปัจจุบัน

การกำหนดสิทธิหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการการปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรม เพื่อป้องการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

การใช้งานรหัสผ่าน (Password Use)

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

1. ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น
2. ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง
3. ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย
4. ผู้ใช้งานควรเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือมีผู้อื่นล่วงรู้
5. ผู้ใช้งานควรตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำที่กำหนดไว้
6. ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคง่ายต่อการจดจำ
7. ผู้ใช้งานไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม
8. ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น 123, abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น 111, aaa เป็นต้น
9. รหัสผ่านที่ดีต้องมีลักษณะดังนี้
   9.1 ความยาวอย่างน้อย 8 ตัวอักษรหรือตามที่ผู้ดูแลระบบกำหนด
   9.2 ส่วนประกอบของอักษรอักขระพิเศษหรือตัวเลขประสมกันตามลักษณะ ดังนี้
      - ตัวอักษรใหญ่ เช่น A, B, C, ...
      - ตัวอักษรเล็ก เช่น a, b, c, ...
      - ตัวเลข เช่น 0, 1, 2, ...
      - สัญลักษณ์พิเศษ เช่น !, @, #, $, ...
10. ผู้ใช้งานควรเปลี่ยนรหัสผ่านตามกรอบระยะเวลาที่กำหนด
11. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช่รหัสเดิมที่เคยตั้งมาแล้ว
12. ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุกๆ 3 เดือน สำหรับผู้ดูแล และ 6 เดือน สำหรับผู้ใช้งานระบบ
13. ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน
14. ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง
15. ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนเองร่วมกับผู้อื่น
16. ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ใช้งาน

การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

1. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์พกพา (Laptop)
2. ผู้ใช้งานควรล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ได้ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต
3. ผู้ดูแลระบบควรกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

การควบคุมทรัพย์สินสารสนเทศ

การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและผู้ใช้งานต้องออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน อนึ่งผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 ทั้งนี้ต่อสอดคล้อง กับการกำหนดประเภทข้อมูลและการจัดระดับชั้นความลับของข้อมูล (Information Classification, Labeling and Handling)

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2561 เช่น การทำซ้ำ คัดลอก ดัดแปลง ติดตั้งชุดคำสั่งที่ละเมิดลิขสิทธิ์ลงบนระบบคอมพิวเตอร์ของกรม โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์ บุคคลนั้นจะมีความผิดฐานละเมิดลิขสิทธิ์

การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

1. ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
2. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพ เมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
3. ในการเข้าใช้ระบบปฏิบัติการใส่ User และ Password ทุกครั้ง
4. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของกรมร่วมกัน
5. ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
6. ห้ามเปิดหรือใช้โปรแกรมประเภท Peer – to – Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา หรือกลุ่มเทคโนโลยีสารสนเทศ
7. ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟท์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว
8. ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟต์แวร์ที่กรมจัดเตรียมไว้ให้ผู้ใช้งาน เพื่อนำไปใช้งานที่อื่น
9. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกรม เพื่อประโยชน์ทางการค้า
10. ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

11. ห้ามผู้ใช้งานใช้ระบบสารสนเทศของกรม เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
12. โปรแกรมประยุกต์ (Application) ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลของกรมทั้งที่ได้มาจากการพัฒนาขึ้นโดยเจ้าหน้าที่หรือได้รับการจัดซื้อมาต้องได้รับการตรวจสอบ ควบคุม และอนุมัติการใช้งานอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบ ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของกรม
13. ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของกรม มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้ถูกต้อง

การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

1. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไขทันที
2. ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกำระทำของผู้อื่น
3. ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือแจกจ่ายให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
4. ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities)

1. มีการกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมอรรถประโยชน์ ระดับสิทธิของผู้ขออนุมัติ การระบุ และการพิสูจน์ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน
2. ต้องจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน
3. มีการจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์
4. ต้องยกเลิกหรือลบโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

การหมดเวลาใช้งานระบบสารสนเทศ (Session time - out)

1. กำหนดให้ระบบสารสนเทศ เช่น ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการตัดและหมดเวลาการใช้งาน หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 10 นาที
2. กำหนดให้ระบบสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 10 นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ
3. กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบใบเสร็จรับเงิน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

การใช้งานอินเทอร์เน็ต (Use of Internet)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2562 เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้งานระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของกรม ถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

- ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่กรมจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้ ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial – up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากกลุ่มเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร
- เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราว์เซอร์
- การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
- ผู้ใช้งาน ต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของกรม เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
- กรณีที่ผู้ใช้งานพบเว็บไซต์ที่ไม่เหมาะสม หรืออาจกระทบต่อความปลอดภัย ความมั่นคงของกรม ผู้ใช้งานต้องยกเลิกการติดต่อกับเว็บไซต์ดังกล่าวและแจ้งกลุ่มเทคโนโลยีสารสนเทศให้ทราบทันที
- ผู้ใช้งาน จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกรม

- ผู้ใช้งาน ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ละเมิดสิทธิของผู้อื่น และข้อมูลที่อาจก่อความเสียหายให้กรม
- ผู้ใช้งาน ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรม ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต
- ผู้ใช้งาน ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
- ผู้ใช้งาน ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้ จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
- ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
- ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่างๆ การดาวน์โหลดทุกประเภทต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
- ห้ามมิให้ใช้งาน Bandwidth จำนวนมากโดยเฉพาะอย่างยิ่งการใช้งานโปรแกรมประเภท P2P File Sharing
- ห้ามมิให้ใช้โปรแกรม/สคริปต์/คำสั่ง หรือการส่งข้อความใดๆ โดยมีเจตนารบกวน ลดประสิทธิภาพการให้บริการ หรือระงับการใช้งานของผู้ใช้งาน ทั้งโดยผ่านระบบภายใน หรือผ่านระบบเครือข่ายต่างๆ
- ห้ามมิให้ส่งข้อความ ไม่ว่าจะด้วยภาษา ความถี่ หรือขนาดของข้อความ การแสดงความคิดเห็น หรือส่งข้อความใดๆ ที่ไม่เกี่ยวข้องกับการทำงานไปหาบุคคลจำนวนมาก (Newsgroup Spam)
- ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช่ข้อความยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรม รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่นๆ
- หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรม ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ตผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัดจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวปฏิบัติการในใช้งานจดหมายอิเล็กทรอนิกส์

- ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรม ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น
- ผู้ดูแลระบบ ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่ และรหัสผ่าน สำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม
- รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น (*) ในการพิมพ์แต่ละตัวอักษร
- ผู้ดูแลระบบ ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง
- ผู้ดูแลระบบ ควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการล็อกเอาท์ออกจากหน้าจอและตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อให้ใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง
- ผู้ใช้งาน ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์
- ผู้ใช้งาน ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3 – 6 เดือน
- ผู้ใช้งาน ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อกรมหรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรม
- ข้อห้าม ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับ – ส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน
- ผู้ใช้งาน ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของกรม เพื่อการทำงานของกรม เท่านั้น
- หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการล็อกเอ้าท์ออกจากระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
- ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe เป็นต้น
- ผู้ใช้งาน ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่ง ที่ไม่รู้จัก
- ผู้ใช้งาน ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของกรม ทำให้เกิดความแตกแยกระหว่างกรม ผ่านทางจดหมายอิเล็กทรอนิกส์
- ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลในหัวข้อจดหมายอิเล็กทรอนิกส์

- ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนเองให้เหลือจำนวนน้อยที่สุด
- ผู้ใช้งาน ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์
- ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

การใช้สื่อสังคมออนไลน์ในฐานะหน่วยงานของกรม

วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแลการเผยแพร่ข้อมูลและการเข้าถึงเครือข่ายสังคมออนไลน์ (Social Media) ในฐานะหน่วยงานของกรม

แนวปฏิบัติในการใช้งานสื่อสังคมออนไลน์ในฐานะหน่วยงานของกรม

1. ข้อความ ภาพ เสียง วีดีโอคลิป หรือการกระทำใดๆ ที่เผยแพร่บนสื่อสังคมออนไลน์ (Social Media) อันสามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบทั้งทางด้านสังคมและด้านกฎหมาย
2. ห้ามมิให้เผยแพร่ข้อมูลบนสื่อสังคมออนไลน์ ที่เกี่ยวข้องกับกรณีดังต่อไปนี้
   2.1 ข้อมูลปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น หรือความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน
   2.2 ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
   2.3 ข้อมูลใดๆ ที่มีลักษณะอันลามก อนาจาร หรือขัดต่อศีลธรรมอันดี
   2.4 ข้อมูลที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
3. การกระทำใดๆ ที่เผยแพร่บนสื่อสังคมออนไลน์ ต้องไม่เป็นการละเมิดทรัพย์สินทางปัญญาของผู้อื่น ต้องมีการอ้างถึงแหล่งข้อมูลอย่างชัดเจน
4. การเผยแพร่ข้อมูลหรือการแสดงความเห็นใดๆ บนสื่อสังคมออนไลน์ที่อาจทำให้ผู้อื่นเข้าใจว่าเป็นความคิดเห็นของกรม ผู้เผยแพร่ต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความเห็นส่วนตัว มิใช่ความเห็นของกรม เว้นแต่จะเป็นความเห็นของกรมอย่างแท้จริง หรือได้รับการอนุญาตจากผู้มีอำนาจที่เกี่ยวข้อง
5. การสร้าง Page หรือ Account ที่เป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการของหน่วยงานของกรม ต้องแจ้งให้ผู้บังคับบัญชาทราบ แล้วแต่กรณี และต้องแจ้งรายชื่อของผู้ดูแล Page (Admin) หรือเจ้าของ Account นั้นให้ผู้บังคับบัญชาทราบด้วย และผู้ดูแลมีหน้าที่ต้องมอบสิทธิ์ในการดูแล

Page หรือ Account นั้นคืนแก่กรมเมื่อพ้นจากหน้าที่ที่ต้องดูแลหรือพ้นสภาพจากการเป็นเจ้าหน้าที่ของกรม

6. ห้ามมิให้เผยแพร่ข้อมูลที่เป็นทรัพย์สินทางปัญญาของกรมบนสื่อสังคมออนไลน์ ก่อนได้รับอนุญาตอย่างเป็นทางการจากผู้บังคับบัญชา
7. ไม่ใช้สื่อสังคมออนไลน์ส่วนบุคคล ในการปฏิสัมพันธ์กับผู้อื่นที่เป็นผู้ใช้บริการ ผู้ให้บริการ หรือผู้รับจ้างที่เกี่ยวข้องกับกรม และไม่ใช้สื่อสังคมออนไลน์ของกรม ในการปฏิสัมพันธ์กับผู้อื่นที่มิได้เป็นผู้ใช้บริการหรือผู้ที่เกี่ยวข้องกับกรม
8. พึงงดเว้นการใช้สื่อสังคมออนไลน์ของกรม ในการวิพากษ์ วิจารณ์ ตลอดจนแสดงความเห็นในเรื่องที่เป็นข้อมูลภายในกรม หรืออาจส่งผลกระทบต่อกรมได้

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของกรม โดยการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่าย

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1. ผู้ใช้งาน ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรม จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร
2. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
3. ผู้ดูแลระบบ จะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อกับเครือข่ายไร้สาย
4. ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตี สามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้
5. ผู้ดูแลระบบ ควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่า สัญญาณรั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่คุมได้
6. ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (default) มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

7. ผู้ดูแลระบบ ควรเปลี่ยนค่า ชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าทางการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้ง่าย
8. ผู้ดูแลระบบ ต้องกำหนดค่าใช้ WEB หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น
9. ผู้ดูแลระบบ ควรจะมีการติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายใน
10. ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์แวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

หมวดที่ 4 การบริหารจัดการด้านการดำเนินงาน (Operations Management)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย โดยประกอบด้วย

- การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection from Malware)
- การสำรองข้อมูล (Backup Data)
- การเฝ้าระวังด้านความมั่นคงปลอดภัย (Security Monitoring)
- การจัดการการเปลี่ยนแปลง (Change Management)

การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์

เพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดี รวมทั้งป้องกันช่องโหว่ของระบบปฏิบัติการสำหรับระบบงานหรืออุปกรณ์ของสำนักงานและกำหนดให้มีระเบียบและขั้นตอนวิธีปฏิบัติที่เหมาะสม

แนวทางปฏิบัติในการป้องกันโปรแกรมที่ไม่ประสงค์ดี

1. กำหนดให้เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์พกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus)
2. ห้ามผู้ใช้งานนำเครื่องคอมพิวเตอร์ ซอฟต์แวร์ที่มีการฝัง Malicious Mobile Code หรือข้อมูลที่มีมัลแวร์มาติดตั้งใช้งาน
3. ผู้ใช้งานต้องสำรองข้อมูลสำคัญเก็บไว้ในที่ที่ปลอดภัย โยสื่อจัดเก็บข้อมูลแบบพกพาหรือบนพื้นที่ที่กลุ่มเทคโนโลยีสารสนเทศจัดสรรไว้ให้เพื่อลดปัญหาการกู้คืนสภาพข้อมูลที่ถูกทำลาย
4. ห้ามผู้ใช้งานปรับแต่ง หรือยกเลิกการทำงานของระบบ Antivirus ที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่กรมจัดหาให้
5. ผู้ใช้งานต้องมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ระบบ Antivirus ที่ใช้ โดยตรวจสอบการ Update ให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถ Update ซอฟต์แวร์ระบบ Antivirus
6. หากผู้ใช้งานพบว่าไฟล์ข้อมูลไม่สามารถเปิดได้ หรือถูกเปลี่ยนนามสกุลไฟล์พร้อมมีข้อความเรียกค่าไถ่ ให้รีบปลดสาย LAN และตัดการเชื่อมต่อ Wi-Fi ของเครื่องนั้นทันที ห้ามปิดเครื่อง (Shutdown) โดยเด็ดขาดเพื่อรักษาสภาพหลักฐานในหน่วยความจำ และห้ามเจรจาจ่ายเงินค่าไถ่ด้วยตนเอง จากนั้นให้แจ้งกลุ่มเทคโนโลยีสารสนเทศเพื่อเข้ากักกันพื้นที่ในทางเทคนิค และดำเนินการดึงข้อมูลจากระบบสำรองข้อมูลที่ถูกแยกส่วนไว้มาทำการกู้คืน จากนั้นจึงนำเรียนผู้บังคับบันชาเพื่อรายงานสถานการณ์ต่อไป

การสำรองข้อมูล (Backup Data)

วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและกู้คืนระบบ โดยมีวัตถุประสงค์ เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

แนวทางปฏิบัติในการสำรองข้อมูลและระบบคอมพิวเตอร์

1. ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของกรม
2. การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก
3. มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ
4. การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย
5. ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลให้กับเจ้าหน้าที่คนอื่นเพื่อช่วยสำรองข้อมูล ในกรณีที่ผู้ดูและระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้
6. ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ
7. ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือการสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Increment Backup)
8. การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีรหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

    9.1 **มาตรการเข้ารหัสลับข้อมูล (Cryptographic Controls)** ต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูลโดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดยกเว้นกรณีที่ไม่สามารถเข้ารหัสได้ ต้องจัดให้มีการควบคุมการเข้าถึงอย่างเหมาะสมด้วย

    9.2 **การบริหารจัดการกุญแจเข้ารหัสลับข้อมูล** ต้องกำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล โดยให้มีการปฏิบัติตามขั้นตอนการจัดการกุญแจเข้ารหัสลับข้อมูล และให้เป็นไปตามวิธีการดังกล่าวอย่างสม่ำเสมอซึ่งประกอบด้วย

9.2.1 ต้องพิจารณาประเภทกลุ่มข้อมูลที่นำมาใช้เข้ารหัสว่าสอดคล้องกับการจัดระดับชั้นความลับของข้อมูล และแนวทางการดำเนินการกำกับข้อมูล

9.2.2 ต้องเลือกใช้การเข้ารหัสข้อมูลให้สมารถดำเนินการได้ 2 แบบ ดังนี้

- แบบ Symmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสเดียวกัน (Secret Key)
- แบบ Asymmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสคู่ (Public/Private Key)

9.2.3 ดำเนินการสร้างกุญแจรหัสจากโปรแกรมที่น่าเชื่อถือ โดยแนวทางการสร้างกุญแจรหัสและการบริหารจัดการกุญแจรหัส (Key Management)

9.2.4 ดำเนินการนำข้อมูลผ่านกระบวนการเข้ารหัส เพื่อนำข้อมูลที่เข้ารหัสไปใช้ตามจุดประสงค์ต่อไป

9. นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

การปฏิบัติเกี่ยวกับการสำรองข้อมูล

1. ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการตามความถี่ดังนี้

ลำดับ	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
1	Mail Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในเมล์บ็อกซ์	1 ครั้งต่อเดือน
2	Web Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	1 ครั้งต่อเดือน
3	Database Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	1 ครั้งต่อสัปดาห์
4	Firewall Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูล Rule ของ Firewall	1 ครั้งต่อเดือน
5	Server ของระบบงานต่างๆ	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลบน Server อื่นๆ	1 ครั้งต่อเดือน
หมายเหตุ ทุกรายการที่ปรากฏในตารางจะใช้วิธีแบคอัพแบบ Full Backcp			

2. ผู้ดูและระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการแบคอัพ (Back up) ตามรายละเอียด ในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

การกู้คืนระบบ

1. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงานต่อหัวหน้ากลุ่มเทคโนโล ยีสารสนเทศหรือผู้ที่ได้รับมอบหมายเท่านั้น
2. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามคบวามเหมาะสมเพื่อกู้คืนระบบ
3. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการใช้งานของผู้ใช้ระบบ ให้แจ้งให้ผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์
4. ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง

การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) นโยบายเกี่ยวกับการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ ต้องมอบหมายให้บุคลากรที่เกี่ยวข้องดำเนินการดังต่อไปนี้

1. กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง
2. กำหนดชนิดภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ
3. ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้
4. จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง
5. ทดสอบ/ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง อย่างน้อยปีละ 1 ครั้ง

การเฝ้าระวังด้านความมั่นคงปลอดภัย (Security Monitoring)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ ต้องให้มีการจัดเก็บข้อมูลจราจรบนเครือข่ายที่สอดคล้องกับข้อกำหนดตามพระราชบัญญัติการกระทำผิดทางคอมพิวเตอร์ และต้องกำหนดขั้นตอนวิธีปฏิบัติในการติดตั้งเวลาของระบบคอมพิวเตอร์กลางให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลา ในกรณีเกิดเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศกรม

การบันทึกข้อมูลเหตุการณ์ (Event logging)

ให้บันทึกกิจกรรมการใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการของระบบ และเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้ซึ่งประกอบด้วย

1. ชื่อผู้ใช้ วัน เวลา การเข้าระบบและออกระบบ
2. บันทึก IP Address และ Protocol ต้นทาง ปลายทาง
3. บันทึกจำนวนครั้งในการพยายามเข้าสู่ระบบทั้งที่สำเร็จและไม่สำเร็จ
4. บันทึกการเปลี่ยนค่า Configuration ของระบบ
5. มีการแจ้งเตือนเมื่อมีการพยายามเข้าถึงโดยไม่ได้รับอนุญาต
6. บันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ รวมถึงบันทึกการเปลี่ยนแปลงอุปกรณ์คอมพิวเตอร์และเครือข่าย

การป้องกันข้อมูลบันทึกเหตุการณ์ (Protect of Log Information)

1. ตรวจสอบการเปลี่ยนแปลงการให้บริการของระบบสารสนเทศ
2. ตรวจสอบการเชื่อมต่อการทำงานของอุปกรณ์ภายนอก
3. ตรวจสอบการใช้บัญชีผู้ดูแลระบบหรือเทียบเท่า
4. ตรวจสอบความจุของพื้นที่ในการจัดเก็บข้อมูลบันทึกเหตุการณ์ให้เพียงพอต่อการดำเนินงานสอดคล้องกับหลักการ และกฎหมายที่เกี่ยวข้อง
5. การสำรองข้อมูลบันทึกเหตุการณ์ จะต้องถูกดำเนินการอย่างเหมาะสม

การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

1. กำหนดให้มีการติดตามข่าวสารที่เกี่ยวกับช่องโหว่ในระบบต่างๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว
2. ต้องกำหนดหน้าที่ความรับผิดชอบแก่ผู้ที่เกี่ยวข้องในการเฝ้าระวังภัยคุกคาม การประเมินความเสี่ยงของภัยคุกคาม เป็นต้น
3. จัดให้มีแผนการเฝ้าระวังภัยคุกคาม การวิเคราะห์ความเสี่ยงของแผน และการประเมินภัยคุกคามที่เกี่ยวข้องความมั่นคงปลอดภัยระบบสารสนเทศทุกๆ 3 เดือน

การตั้งเวลาให้ถูกต้อง (Clock Synchronization)

การตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ในระบบสารสนเทศกรมให้ถูกต้องตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตามแหล่งเวลาที่กำหนดไว้ โดยการตั้งเวลาด้วย Network Time Protocol (NTP)

การจัดการการเปลี่ยนแปลง (Change Management)

วัตถุประสงค์

เพื่อควบคุมการเปลี่ยนแปลงระบบสารสนเทศอันจะทำให้เกิดความเสี่ยงต่อความเสียหายจากการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบสารสนเทศ

แนวปฏิบัติการจัดการการเปลี่ยนแปลง

1. เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ ต้องมีเอกสารเป็นทางการในการร้องขอการเปลี่ยนแปลงทุกครั้ง

2. จัดทำบันทึกการเปลี่ยนแปลงทุกครั้ง โดยประกอบด้วยข้อมูลที่สำคัญ ดังต่อไปนี้
    - วันที่รับเรื่อง และวันที่ทำการเปลี่ยนแปลง
    - เจ้าของข้อมูล และผู้ดูแลระบบ
    - วิธีการเปลี่ยนแปลง
    - ผลของการเปลี่ยนแปลง
3. ต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นปัจจุบัน ตามความเหมาะสมของทรัพยากรชนิดต่างๆ
4. ต้องมีการวางแผนจัดการขีดความสามารถของระบบ อย่างน้อยปีละ 1 ครั้ง โยพิจารณาจากความต้องการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารในอนาคต สภาพการใช้งานทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี เป็นต้น
5. การเปลี่ยนแปลงระบบเครือข่าย อุปกรณ์คอมพิวเตอร์ และสื่อที่ใช้ในการจัดเก็บข้อมูลจะต้องได้รับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงโยไม่ได้รับอนุญาต หรือการแก้ไขโดยไม่ตั้งใจ ซึ่งอาจมีผลต่อการให้บริการ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
6. การเปลี่ยนแปลงอุปกรณ์หรือสื่อที่ใช้มนการจัดเก็บข้อมูล ต้องทำการลบข้อมูลตามขั้นตอนการปฏิบัติการทำลายสื่อบันทึกข้อมูลสารสนเทศ
7. เมื่อมีการเปลี่ยนแปลงระบบเครือข่าย ต้องมีการบันทึกข้อมูลของระบบเก่าเก็บไว้เพื่อใช้ในการอ้างอิงการทำงานของระบบเดิม
8. การเปลี่ยนแปลง Source Code ระบบงาน ต้องมีการดำเนินการบนระบบทดสอบโดยแยกจากระบบงานจริง และจัดเก็บอย่างเป็นระบบตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับของข้อมูล
9. การจัดหาหรือพัฒนาระบบสารสนเทศใหม่ของกรมพัฒนาสังคมและสวัสดิการ จะต้องถูกออกแบบให้มีสถาปัตยกรรมที่สามารถถอดเปลี่ยนหรืออัปเกรดอัลกอริทึมการเข้ารหัสได้อย่างรวดเร็ว เพื่อรองรับการเปลี่ยนผ่านสู่มาตรฐาน Post-Quantum Cryptography โดยไม่กระทบต่อการทำงานหลักของระบบ

หมวดที่ 5 การสร้างความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน และเป็นมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับกับผู้ใช้งานและผู้ให้บริการภายนอก

การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์ (Computing System Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรฐานการควบคุมและป้องกัน การรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศโดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้ จะมีผลบังคับใช้กับผู้ใช้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรม

การควบคุมการเข้าออก

1. กรมมีการกำหนดในพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสมโดยกำหนดพื้นที่รักษาความมั่นคงปลอดภัยของระบบสารสนเทศเพื่อจุดประสงค์ในการบเฝ้าระวัง ควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้
2. กำหนดสิทธิให้กับเจ้าหน้าที่ ที่มีสิทธิ์ในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับหมอบหมาย ดังนี้
    - 2.1 จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกห้องควบคุมระบบคอมพิวเตอร์” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย
    - 2.2 กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า – ออก ดังกล่าวโดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกห้องควบคุมระบบคอมพิวเตอร์”
    - 2.3 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกห้องควบคุมระบบคอมพิวเตอร์เป็นประจำ และให้มีการปรับปรุงรายการผู้มีสิทธิเข้าออกห้องควบคุมระบบคอมพิวเตอร์ ปีละครั้ง เป็นอย่างน้อย
    - 2.4 บุคคลภายนอกเข้ามาติดต่อต้องลงชื่อขออนุญาตการเข้า – ออก ในแบบฟอร์มการเข้า – ออกให้ถูกต้องและจะต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา
    - 2.5 กรณีผู้มาติดต่อนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในห้องควบคุมระบบคอมพิวเตอร์ จะต้องลงบันทึกรายการอุปกรณ์ลงในใบนำทรัพย์สินเข้าออกพื้นที่ด้วย
    - 2.6 บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าห้องควบคุมระบบคอมพิวเตอร์ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

3. ประกาศห้ามผู้ไม่เกี่ยวข้องเข้าห้องควบคุมระบบคอมพิวเตอร์ เว้นแต่ได้รับอนุญาตให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว แบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General working area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) เป็นต้น

ความมั่นคงปลอดภัยด้านสารนสนเทศสำหรับสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ (Securing Offices, Rooms and Facilities)

การปฏิบัติงานในพื้นที่สำนักงาน

1. ต้องจัดให้มีมาตรการความมั่นคงปลอดภัยด้านสารสนเทศให้กับสำนักงาน ห้องทำงานและเครื่องมือต่างๆ ได้แก่ เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก
2. ต้องมีการควบคุมการเข้าออกพื้นที่สำนักงานของผู้ติดต่อเฉพาะพื้นที่ที่จัดเตรียมไว้ให้เท่านั้น
3. ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์ และพื้นที่การเตรียม หรือประกอบอุปกรณ์สารสนเทศ โดยผู้ให้บริการภายนอก (Third Party) หรือหน่วยงานภายนอกเพื่อป้องกันการเข้าถึงสินทรัพย์ของกรมโดยไม่ได้รับอนุญาตและจัดเป็นบริเวณแยกออกมาต่างหาก
4. สำนักงานจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณดังกล่าว
5. ต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพวีดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

ความปลอดภัยของอุปกรณ์ (Equipment Security)

1. ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น
2. เจ้าของระบบงานต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ ได้แก่ จัดให้มีการซ่อมบำรุงตามรอบที่กำหนดโดยเฉพาะระบบที่มีความสำคัญ เป็นต้น เพื่อให้สามารถใช้งานได้อย่างต่อเนื่องและมีความพร้อมใช้งานอยู่เสมอ
3. ต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของสำนักงานเมื่อถูกนำไปใช้งานนอกพื้นที่กรม
4. ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ตามขั้นตอนการปฏิบัติการทำลายสื่อบันทึกข้อมูลสารสนเทศ

ความปลอดภัยของระบบกระแสไฟฟ้าสำรอง (Power Supplies) และระบบป้องกันภัย

1. ต้องมีระบบไฟฟ้าสำรองอัตโนมัติ เพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง และต้องมีการตรวจสอบกระแสไฟฟ้าสำรองและบำรุงรักษาอย่างน้อยปีละ 1 ครั้ง
2. ต้องจัดให้มีระบบเตือนภัย/ป้องกันภัย ได้แก่ ระบบดับเพลิง ระบบแจ้งเตือนอัคคีภัย
3. ต้องมีการวางแผนและซักซ้อมการปฏิบัติเพื่อรับมือกับเหตุการณ์ฉุกเฉินต่างๆ อย่างน้อยปีละ 1 ครั้ง และเป็นไปตามขั้นตอนการเตรียมการของแผนรองรับเหตุการณ์ฉุกเฉิน
4. ระบบงานที่สำคัญของกรมจะต้องมีการปฏิบัติตามนโยบายแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ เพื่อลดผลกระทบที่จะเกิดขึ้นกับการดำเนินงานของกรม

ความปลอดภัยของโต๊ะทำงานและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk Clear Screen)

1. ต้องควบคุมสินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ ฯลฯ ให้ปลอดภัยจากการเข้าถึงโดยผู้ไม่มีสิทธิ์
2. จัดเก็บเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับของข้อมูล
3. การทำลายเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับของข้อมูลและขั้นตอนการปฏิบัติการทำลายสื่อบันทึก
4. ข้อมูลที่มีความสำคัญมาก รวมถึงข้อมูลในคอมพิวเตอร์ ต้องเคลื่อนย้ายโดยผู้เป็นเจ้าของข้อมูลเท่านั้น ไม่เคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล
5. ข้อมูลที่มีความสำคัญ มีการรักษาความลับต้องมีการเข้ารหัสเมื่อถูกจัดเก็บ
6. ทุกครั้งเมื่อมีการเว้นว่างจากการใช้งานระบบ ควรออกจากระบบงานนั้น และป้องกันหน้าจอคอมพิวเตอร์ทุกครั้งเมื่อว่างเว้นจากการใช้งาน เพื่อป้องกันการเข้าถึงระบบงาน และการเข้าถึงเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต

การควบคุมทั่วไป (General Controls)

1. กำหนดให้มีผู้รับผิดชอบในการตรวจตราสถานที่ย้ายสินทรัพย์ออก เพื่อให้มั่นใจได้ว่าไม่มีข้อมูลใดหลงเหลืออยู่ และมีการกำหนดความรับผิดชอบในการดูแลให้ครอบคลุมส่วนที่เก็บเอกสาร (ตู้เก็บแฟ้มเอกสาร, ห้องเก็บรักษาแฟ้มข้อมูล)
2. การเคลื่อนย้ายสินทรัพย์ของสำนักงานผู้ดูแลระบบแต่ละส่วนงานต้องทำเป็นบันทึกและขออนุญาตจากผู้บังคับบัญชาทุกครั้ง
3. ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่างๆ เมื่อมีการเปลี่ยนแปลงหรือเคลื่อนย้ายเพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของกรม

หมวดที่ 6 การจัดหาพัฒนาและบำรุงรักษาระบบสารสนเทศ (Information System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อให้การพัฒนาและการบำรุงรักษาระบบสารสนเทศดำเนินการได้โดยสอดคล้องกับนโยบายความมั่นคงปลอดภัย และเพื่อให้เกิดความถูกต้องสมบูรณ์ของข้อมูลในระบบสารสนเทศของกรม

ข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ

1. การจัดหาและการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงจากระบบที่มีอยู่เดิม ต้องมีการวิเคราะห์และระบุข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ
2. ระบบสารสนเทศที่พัฒนาขึ้นต้องผ่านการตรวจสอบการประมวลผลทั้งส่วนข้อมูลนำเข้า และผลลัพธ์จากการประมวลผล รวมทั้งต้องมีกลไกในการตรวจจับข้อผิดพลาดและบันทึกไว้เพื่อการตรวจสอบและแก้ไข
3. ระบบสารสนเทศที่พัฒนาขึ้นต้องมีการควบคุมการเข้าถึงชุดคำสั่งของระบบ
4. ในการพัฒนาระบบสารสนเทศต้องมีการกำหนดขั้นตอนวิธีปฏิบัติอย่างเป็นทางการเพื่อใช้ควบคุมการเปลี่ยนแปลงแก้ไข และต้องมีการตรวจสอบการทำงานหลังจากการเปลี่ยนแปลงนั้นๆ
5. ระบบสารสนเทศเป็นบริการสาธารณะต้องได้รับการป้องกันอย่างเหมาะสมจากการเปิดเผย เปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต
6. เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบที่สำคัญต้องมีการทบทวนและทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือต่อความมั่นคงปลอดภัยของกรม
7. การจ้างพัฒนาระบบจากผู้ให้บริการภายนอก ต้องมีการควบคุม เฝ้าระวัง ติดตามการดำเนินงาน เพื่อให้เป็นไปตามขอบเขตการดำเนินงาน และสอดคล้องกับนโยบาย ขั้นตอนปฏิบัติของกรมที่กำหนดไว้
8. การป้องกันข้อมูลสำหรับการทดสอบ ควรหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่ในระบบให้บริการมาใช้ในการทดสอบ ในกรณีมีการสำเนาข้อมูลจากระบบงานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบงานจริง

หมวดที่ 7 การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ (Third party access control)

วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอก อาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบสารสนเทศของกรม เป็นไปอย่างมั่นคง ปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบ การใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

แนวทางปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

1. หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ กำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับ หรือการแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศได้
2. การควบคุมการเข้าใช้งานระบบสารสนเทศของหน่วยงานภายนอก
   2.1 บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของกรม จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ
   2.2 จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้ งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้
      2.2.1 เหตุผลในการขอใช้
      2.2.2 ระยะเวลาในการใช้
      2.2.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
      2.2.4 การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล
   2.3 หน่วยงานภายนอกที่ทำงานให้กรม ทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในกรม หรือนอกสถานที่จำเป็นต้องลงนามในสัญญาไม่เปิดเผยข้อมูลกรม โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบ
   2.4 เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนด การเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล
   2.5 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของกรม ผู้ดูแลระบบต้องควบคุมการปฏิบัติติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาคงวามถูกต้องข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
   2.6 “กรม” มีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบสารสนเทศ เพื่อให้มั่นใจได้ว่า “กรม” สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

2.7 กำหนดให้ผู้บริการหน่วยงานภายนอก จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

2.8 ผู้ดูแลระบบและส่วนงานที่รับผิดชอบในการประสานงานกับผู้ให้บริการภายนอก ต้องกำกับให้มีการดูแลให้บุคคล หรือผู้ใช้บริการภายนอกแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการและระดับการให้บริการ

2.9 ในกรณีที่มีการเปลี่ยนแปลงการดำเนินงาน ผู้ให้บริการจากภายนอกต้องแจ้งให้หัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบและอนุมัติการเปลี่ยนแปลงนั้น ก่อนการดำเนินงาน เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

2.10 กรณีที่มีการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติ และมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการสื่อสารให้ผู้ให้บริการภายนอกรับทราบ

หมวดที่ 8 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของกรม ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และมีวิธีการที่สอดคล้องและได้รับผลสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของกรม

แนวปฏิบัติในการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

1. การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของกรม
2. ผู้ใช้งานต้องรายเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของกรม ให้กลุ่มเทคโนโลยีสารสนเทศทราบทันที
3. ตัวอย่างลักษณะเหตุการณ์น่าสงสัย ดังนี้
   3.1 รหัสผ่านไม่สามารถใช้งานได้ โดยไม่ทราบสาเหตุ
   3.2 พบการเข้าใช้งานระบบ หรือบัญชีที่ผิดปกติ
   3.3 พบสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน เช่น แฟ้มเอกสารที่น่าสงสัย โปรแกรมที่ไม่เคยใช้งานหรือการเปลี่ยนแปลงค่าต่างๆ เป็นต้น
   3.4 พบความพยายามในการเข้าถึงระบบอย่างผิดวิธี ทั้งที่สำเร็จและไม่สำเร็จ
   3.5 การให้บริการของระบบเกิดหยุดชะงัก หรือไม่สามารถให้บริการ
   3.6 พบการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์
   3.7 พบว่าอุปกรณ์สารสนเทศใดๆ เกิดความเสียหาย หรือทำงานผิดปกติ
4. เมื่อพบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใดๆ ของระบบ ผู้พบ ต้องไม่เปิดเผยเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา และแจ้งให้กลุ่มเทคโนโลยีสารสนเทศทราบ ทั้งนี้ห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง
5. ผู้ดูแลระบบ ต้องประเมินเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ทำการจัดแยกกลุ่มเหตุการณ์ หรือจุดอ่อนด้านความมั่นคงปลอดภัย และจัดลำดับความสำคัญตามเกณฑ์ที่กำหนดไว้ และแจ้งส่วนงานที่เกี่ยวข้องทราบเพื่อแก้ไขในกรณีที่พบว่าเหตุการณ์ หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ที่ส่งผลกระทบด้านความมั่นคงปลอดภัยสารสนเทศ
6. กรณีเกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ผู้ดูแลระบบต้องร่วมกับส่วนงานที่รับผิดชอบประเมินขอบเขต (Scope) และความรุนแรง (Severity) ของปัญหา หากพบว่าเป็นปัญหาที่จะมีผลกระทบรุนแรง หรือมีผลต่อชื่อเสียงของกรม จะต้องรายงานให้หัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบโดยด่วนเพื่อหาแนวทางแก้ไขและป้องกันต่อไป

7. ผู้ดูแลระบบต้องบันทึกเหตุละเมิดด้านความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคามหรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไขจากเหตุการณ์ที่เกิดขึ้น และรายงานผลให้หัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบ
8. กรณีที่เหตุการณ์ความมั่นคงปลอดภัยส่งผลให้เกิดการรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคลของกลุ่มเปราะบางหรือบุคลากรของกรม ผู้รับผิดชอบต้องดำเนินการประเมินความเสี่ยงและแจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ พร้อมทั้งสื่อสารและกำหนดมาตรการเยียวยาผู้ได้รับผลกระทบตามกระบวนการที่กฎหมายกำหนดอย่างเคร่งครัด

หมวดที่ 9 การจัดองค์กรปฏิบัติการเมื่อเกิดสถานการณ์ฉุกเฉิน

กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตรและแผนงาน กรมพัฒนาสังคมและสวัสดิการ ได้มีการวางมาตรการระบบรักษาความปลอดภัย โดยกำหนดอำนาจหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการวางระบบรักษาความปลอดภัย (Security) และระบบการบริหารความเสี่ยงของระบบสารสนเทศเพื่อเตรียมพร้อมในการแก้ไขสถานการณ์ฉุกเฉินได้อย่างต่อเนื่อง รวดเร็วและมีประสิทธิภาพ กรมพัฒนาสังคมและสวัสดิการได้ดำเนินการจัดแบ่งหงน้าที่ และบุคลากรผู้รับผิดชอบดำเนินงาน ดังนี้

- การจัดองค์กรปฏิบัติการเมื่อเกิดสถานการณ์ฉุกเฉิน หรือสายการบังคับบัญชา
- การประเมินความเสี่ยง
- แผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

การจัดองค์กรปฏิบัติการเมื่อเกิดสถานการณ์ฉุกเฉิน หรือสายการบังคับบัญชา (lines of authority)

1. **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)**
   - 1.1 กำหนดนโยบายให้กลุ่มเทคโนโลยีสารสนเทศ
   - 1.2 ให้คำปรึกษาแก่หัวหน้ากลุ่มเทคโนโลยีสารสนเทศในฐานะประธานกลุ่มเทคโนโลยีสารสนเทศ
2. **หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ**
   - 2.1 เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นกับระบบสารสนเทศ
   - 2.2 มีอำนาจสั่งการให้ทุกหน่วยปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นกับระบบสารสนเทศ
   - 2.3 ประชุมหารือกับคณะกรรมการบริหารจัดการระบบเครื่องข่ายคอมพิวเตอร์ และคณะกรรมการอื่นที่เกี่ยวข้อง
   - 2.4 ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม
   - 2.5 รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

3. **ผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย (LAN Administrator and Staffs)**
   - 3.1 ตัดระบบเครือข่ายที่เชื่อมต่อไปยังพื้นที่ที่เกิดเหตุฉุกเฉิน
   - 3.2 วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ
   - 3.3 รายงานหัวหน้ากลุ่มเทคโนโลยีสารสนเทศให้ทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว
   - 3.4 ดำเนินการตรวจสอบวัสดุ อุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้หัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบ หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้ว อุปกรณ์ที่ต้องตรวจสอบ ได้แก่
     - 3.4.1 ทำการตรวจสอบระบบ firewall
     - 3.4.2 ทำการตรวจสอบ virus, worm, spy ware
     - 3.4.3 ทำการตรวจสอบ UPS
     - 3.4.4 ทำการตรวจสอบ Transaction log files
     - 3.4.5 ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ

3.4.6 ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ

3.4.7 ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล

3.4.8 ทำการตรวจสอบ Configuration ของระบบ

4. ผู้ประสานงานและดูแลสภาพความพร้อมของระบบเครือข่าย

4.1 ดำเนินการให้ผู้ที่เกี่ยวข้องปฏิบัติตามแผนฯ

4.2 ประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง

4.3 ตรวจสอบความเสียหายของทรัพย์สิน ทั้งระบบคอมพิวเตอร์และระบบเครือข่าย

4.4 เตรียมเครื่องมือ อุปกรณ์ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้อง เพื่อดำเนินการกู้ระบบโดยเร็ว

4.5 ประสานขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทที่ปรึกษาในการกู้ระบบ

4.6 ทำการสำรองข้อมูลในส่วนของข้อมูล (data) ทุกวัน และสำรองข้อมูลทั้งระบบสัปดาห์ละ 1 วัน

4.7 ทำการเก็บโปรแกรมและแฟ้มข้อมูล, tape backup, รายชื่อโปรแกรม, เอกสารที่เกี่ยวข้องกับระบบปฏิบัติการและโปรแกรม, สำเนาคู่มือต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ปลอดภัย

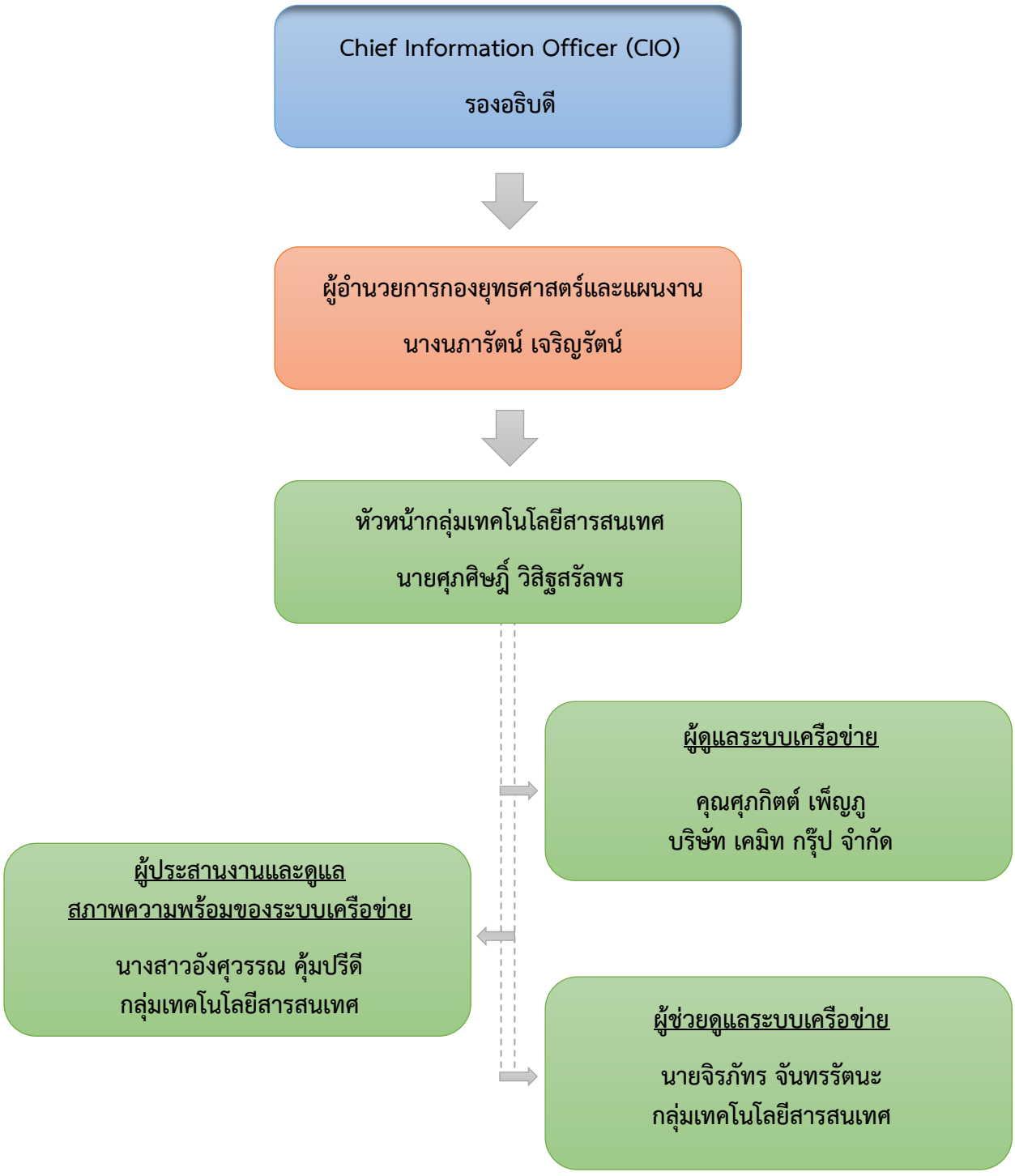
4.8 นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสารสนเทศสามารถดำเนินการต่อไปได้

5. หัวหน้าหน่วยงานที่เกิดเหตุ (On – site manager)

5.1 แจ้งเหตุฉุกเฉิน เคลื่อนย้ายตนเองและผู้อื่นออกจากสถานที่เกิดเหตุโดยเร็ว

5.2 แจ้งข้อมูลเกี่ยวกับสถานที่เกิดเหตุให้กับหัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบ เพื่อประสานงานในการรักษาความปลอดภัยระบบสารสนเทศ พร้อมทั้งนำทรัพย์สินที่ได้ทำการขนย้ายออกมา นำเก็บเข้าที่เมื่อเหตุการณ์เข้าสู่ภาวะปกติแล้ว โดยต้องตรวจดูสภาพและสอบทานบัญชีทรัพย์สินก่อน แล้วจึงทำรายงานเสนอผู้บังคับบัญชา

แผนผังสายการบังคับบัญชา (Lines of authority) เมื่อเกิดสถานการณ์ฉุกเฉิน



การประเมินสถานการณ์ความเสี่ยง
(Risk Analysis)

จากการติดตามตรวจสอบความเสี่ยงในระบบสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ พบว่าความเสี่ยงที่อาจเป็นอันตรายต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ สามารถแยกเป็นภัยต่างๆ ได้ 4 ประเภท ดังนี้

1. ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error)
2. ภัยที่เกิดจาก Software
3. ภัยที่ไฟไหม้ (อัคคีภัย) หรือระบบไฟฟ้า
4. ภัยจากน้ำท่วม (อุทกภัย)
5. ภัยจากแผ่นดินไหว
6. ภัยสงคราม หรือเหตุการณ์ความไม่สงบในพื้นที่

1. ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักหรือหยุดทำงานส่งผลทำให้ไม่สามารถใช้งานระบบสารสนเทศได้อย่างเต็มประสิทธิภาพ

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error)

กลุ่มเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศไว้ ดังนี้

- จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจ ในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด ทำให้เจ้าหน้าที่ มีความรู้ความเข้าใจในการใช้งานและบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ให้มีประสิทธิภาพมากยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human error ลงน้อยลง
- เพื่อให้การบริหารจัดการ User ID บนระบบสารสนเทศ เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ส่วนบริหารทรัพยากรบุคคล ต้องแจ้งให้ส่วนงานที่รับผิดชอบทราบทันทีเมื่อมีการดำเนินการดังต่อไปนี้
  - การว่าจ้างงาน
  - การเปลี่ยนแปลงสภาพการว่าจ้างงาน
  - การลาออกหรือสิ้นสุดการเป็นบุคลากรกรม
  - การโอนย้ายส่วนงาน
  - การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

ผู้รับชอบต้องดำเนินการเปลี่ยนแปลง/เพิกถอน/ยกเลิก/ระงับ สิทธิ์ของผู้ใช้งานที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศเพื่อให้สอดคล้องกับการเปลี่ยนแปลงสถานะของการว่าจ้าง โดยต้องเก็บข้อมูลให้สามารถตรวจสอบประวัติการเปลี่ยนแปลงสิทธิ์ในระบบสารสนเทศที่เกิดขึ้นเหล่านั้นได้

- จัดจ้างบริษัทที่มีบุคลากรซึ่งมีความรู้ความชำนาญ ทำหน้าที่ดูแล ให้คำปรึกษา ตรวจสอบและบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ทั้งทางด้าน Hardware และ Software โดยมีเจ้าหน้าที่ผู้ชำนาญการร่วมปฏิบัติงานกับกลุ่มระบบเครือข่ายและคอมพิวเตอร์ เป็นประจำทุกวันทำการ
- กลุ่มเทคโนโลยีสารสนเทศ มีหน้าที่แจ้งให้บุคลากรของกรม ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบสารสนเทศของกรม ให้ทราบอย่างทั่วกัน

2. ภัยที่เกิดจาก Software เป็นภัยที่สร้างความเสียหายให้กับเครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต (Internet Worm), โทรจัน (Trojan) และข่าวไวรัสหลอกลวง (Hoax) ซึ่ง Software ประเภทนี้อาจรบกวนการทำงานและก่อให้เกิดความเสียหายให้กับระบบสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ อาจถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ของกรมพัฒนาสังคมและสวัสดิการ ใช้งานไม่ได้

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software

กรมพัฒนาสังคมและสวัสดิการ ได้ตระหนักถึงปัญหาเหล่านี้ จึงได้ทำการ

- ติดตั้งอุปกรณ์ Fort iGATE ซึ่งเป็นอุปกรณ์แบบ UTM (Unified Threat Management) ที่รวมความสามารถของ Firewall, IPS, VPN, Antivirus Gateway, Antispam, Traffic Shaping และ Web Filtering ไว้ในอุปกรณ์เดียวในการบริหารจัดการเครือข่าย
- แนะนำวิธีการป้องกันและการกำจัดภัยที่เกิดจาก Software ดังกล่าว ให้ข้าราชการและเจ้าหน้าที่ทุกระดับในกรมพัฒนาสังคมและสวัสดิการได้ศึกษาและสามารถแก้ไขปัญหาในเบื้องต้นได้

3. ภัยจากไฟไหม้ (อัคคีภัย) หรือระบบไฟฟ้าขัดข้อง จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบสารสนเทศ ซึ่งกรมพัฒนาสังคมและสวัสดิการ ได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่ง เพื่อไม่ให้เกิดภัยลักษณะดังกล่าวขึ้น

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากไฟไหม้ (อัคคีภัย) หรือระบบไฟฟ้าขัดข้อง

กรมพัฒนาสังคมและสวัสดิการ ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้ดำเนินการ ดังนี้

- ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ซึ่งระบบสำรองไฟฟ้าที่ใช้ควบคุมระบบเครือข่ายของกรมพัฒนาสังคมและสวัสดิการ สามารถสำรองไฟฟ้าเพื่อใช้งานได้นาน 15 นาที ในกรณีที่เกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการ ได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย
- ติดตั้งอุปกรณ์ดับเพลิงที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

4. ภัยจากน้ำท่วม (อุทกภัย) เป็นภัยที่เกิดขึ้นบ่อยครั้งในปัจจุบัน เนื่องจากปริมาณน้ำฝนที่ไม่สามารถคาดคะเนได้ ทำให้มีความเสี่ยงต่อการเกิดน้ำท่วมและจัดเป็นภัยร้ายแรงที่สร้างความเสียหายให้แก่ระบบสารสนเทศ ซึ่งกรมพัฒนาสังคมและสวัสดิการ ได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้ภัยในลักษณะดังกล่าวเกิดขึ้น

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากน้ำท่วม (อุทกภัย)

กรมพัฒนาสังคมและสวัสดิการ ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้ดำเนินการ ดังนี้

- เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามข่าวจากพยากรณ์อากาศของกรมอุตุนิยมวิทยา
- ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครื่องข่ายทั้งหมด เมื่อเกิดน้ำขังหรือระดับน้ำสูงกว่าปกติ และมีแนวโน้มว่าน้ำท่วมขังเพิ่มขึ้นเรื่อยๆ และน้ำท่วมขังมาจนถึงบริเวณหน้ากรมพัฒนาสังคมและสวัสดิการ
- ถอดเทป Back up ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย
- ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรกเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า
- เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ เป็นผู้เคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายไว้ในที่สูง
- ให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้า ในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย กรณีน้ำลดลงเรียบร้อยแล้ว
- เมื่อระบบไฟฟ้าใช้งานได้ตามปกติ ผู้ดูแลระบบและเจ้าหน้าที่ของบริษัทที่ทำหน้าที่ให้บริการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ และเจ้าหน้าที่ผู้ที่เกี่ยวข้องช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์กลับมาไว้ที่เดิม
- ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่
- เมื่อตรวจสอบแล้วพบว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อย แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

5. ภัยจากแผ่นดินไหว เป็นภัยธรรมชาติที่เกิดขึ้นอย่างฉับพลันและไม่สามารถแจ้งเตือนล่วงหน้าได้ ซึ่งอาจทำให้โครงสร้างอาคารชำรุด เสาไฟฟ้าล้ม สายสัญญาณขาด และส่งผลกระทบโดยตรงต่อห้องควบคุมระบบคอมพิวเตอร์ (Data Center) ระบบเครือข่าย และความปลอดภัยของเจ้าหน้าที่

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากสงครามพื้นที่เสี่ยง

กรมพัฒนาสังคมและสวัสดิการ ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้ดำเนินการ ดังนี้

- เมื่อเกิดแรงสั่นสะเทือน ให้เจ้าหน้าที่อพยพออกจากอาคารไปยังจุดรวมพลที่ปลอดภัยทันที โดยให้ความสำคัญกับความปลอดภัยของชีวิตเป็นอันดับแรกก่อนอุปกรณ์คอมพิวเตอร์

- ออกแบบและติดตั้งตู้จัดเก็บอุปกรณ์ (Rack) สำหรับเครื่องคอมพิวเตอร์แม่ข่าย ให้มีการยึดติดกับโครงสร้างพื้นอย่างแน่นหนา (Seismic Bracing) เพื่อป้องกันการล้มกระแทกเมื่อเกิดแรงสั่นสะเทือน
- เมื่อเหตุการณ์สงบและได้รับอนุญาตจากวิศวกรอาคารว่าปลอดภัย ให้เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศเข้าตรวจสอบสภาพความเสียหายของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย สายสัญญาณ และระบบไฟฟ้าสำรอง จากนั้นขอความร่วมมือในทุกหน่วยงานที่ได้รับผลกระทบ ตรวจสอบความเสียหายอุปกรณ์คอมพิวเตอร์
- หากระบบไฟฟ้าหลักของอาคารเกิดความเสียหาย ให้ใช้กระแสไฟฟ้าจากระบบสำรอง (UPS/Generator) เพื่อประคองระบบเครือข่าย และทำการปิดระบบ (Shutdown) เครื่องแม่ข่ายตามลำดับความสำคัญอย่างถูกต้อง เพื่อป้องกันความเสียหายของฐานข้อมูล
- ตรวจสอบความสมบูรณ์ของข้อมูลที่ได้สำรองไว้ (Backup Data) ในศูนย์สำรอง หรือระบบ Cloud เพื่อเตรียมความพร้อมสำหรับการกู้คืนระบบ (Restore) หากเครื่องแม่ข่ายหลักได้รับความเสียหายทางกายภาพ

6. ภัยสงคราม หรือเหตุการณ์ความไม่สงบในพื้นที่ เป็นภัยที่อาจก่อให้เกิดความเสียหายต่อชีวิต ทรัพย์สิน โครงสร้างพื้นฐานทางเทคโนโลยี และข้อมูลสำคัญของหน่วยงานอย่างฉับพลันและรุนแรง ในพื้นที่ที่มีความเสี่ยงภัยสงคราม การรักษาข้อมูลของหน่วยงานและการเก็บกู้อุปกรณ์ถือเป็นความท้าทายสูงสุดที่ต้องดำเนินการควบคู่ไปกับความปลอดภัยของบุคลากร

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากสงครามพื้นที่เสี่ยง

กรมพัฒนาสังคมและสวัสดิการ ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้กำหนดแผนรับมือทางเทคโนโลยีสารสนเทศ และการเก็บกู้ ย้าย รักษา ข้อมูลของหน่วยงาน ดังนี้

- **ก่อนเกิดเหตุการณ์**
  - กำหนดตัวบุคคลผู้รับผิดชอบในการเก็บรักษาข้อมูลอย่างชัดเจน
  - เตรียมความพร้อมเจ้าหน้าที่และเตรียมดำเนินการตามแผนความต่อเนื่องทางธุรกิจ (BCP) ของหน่วยงาน
  - ดำเนินการสำรองข้อมูลที่สำคัญทั้งหมดของหน่วยงาน
  - สำรวจความพร้อมอุปกรณ์สำรองข้อมูล เช่น การสำรองผ่านระบบ Cloud, การเตรียม External HDD/Flash Drive หรืออุปกรณ์จัดเก็บข้อมูลอื่นๆ (กรณีอุปกรณ์ไม่เพียงพอ ให้รีบแจ้งความต้องการมาที่ส่วนกลาง)
- **ระหว่างเกิดเหตุการณ์**
  - แจ้งหัวหน้าหน่วยงานให้รับทราบสถานการณ์โดยทันที
  - ดำเนินการตามแผนความต่อเนื่องทางธุรกิจ (BCP) ของหน่วยงาน
  - รายงานสถานการณ์ตามช่องทางที่กำหนดอย่างต่อเนื่อง
  - ทำการสำรองข้อมูลที่สำคัญ ผ่านระบบ Cloud, External HDD/Flash Drive หรืออุปกรณ์จัดเก็บข้อมูลอื่นๆ
  - ขนย้ายอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น Case CPU, HDD (แหล่งเก็บข้อมูล) ไปยังพื้นที่ปลอดภัย
  - ตรวจเช็คยอดอุปกรณ์ และประเมินความเสียหายที่เกิดขึ้นในเบื้องต้น

- **หลังเกิดเหตุการณ์**
    - ผู้รับผิดชอบดำเนินการตรวจเช็คยอดอุปกรณ์และความเสียหายที่เกิดขึ้นอย่างละเอียดอีกครั้ง
    - แจ้งรายงานสถานะให้ส่วนกลาง (กลุ่มเทคโนโลยีสารสนเทศ) รับทราบ
    - เมื่อสถานการณ์ปลอดภัย ให้ขนย้ายอุปกรณ์กลับเข้าสำนักงาน
    - ดำเนินการฟื้นฟูซ่อมแซมอุปกรณ์และกู้คืนข้อมูลที่เสียหายให้กลับมาพร้อมใช้งาน

การจัดเตรียมอุปกรณ์ที่จำเป็น

ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ กลุ่มเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ของกรม ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

1. แผ่น Boot Disk
2. แผ่นติดตั้งระบบปฏิบัติการ/ ระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
3. แผ่นสำรองข้อมูลและระบบงานที่สำคัญ
4. แผ่นโปรแกรม Anti-virus/ Spyware
5. แผ่น Driver อุปกรณ์ต่างๆ
6. ระบบสำรองไฟฉุกเฉิน
7. Hard Disk สำรอง
8. สำเนารายละเอียดการบันทึกค่าต่างๆ ในการติดตั้งอุปกรณ์ที่จำเป็น

แผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

ปัจจุบันภัยที่เกิดขึ้นบนระบบสารสนเทศมีอัตราการเกิดเพิ่มขึ้น ตามความก้าวหน้าของเทคโนโลยี ภัยอันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศอาจเกิดขึ้นได้โดยคน ซึ่งได้แก่เจ้าหน้าที่ บุคลากรของหน่วยงานที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ สถานการณ์ หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบสารสนเทศถูกดปิดเผย หรือเปลี่ยนแปลง ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่นๆ ตามความต้องการของภัย ดังนั้น เพื่อเป็นการลดภัยดังกล่าว ที่จะเกิดขึ้นในระบบสารสนเทศของกรม กลุ่มเทคโนโลยีสารสนเทศ กรมพัฒนาสังคมและสวัสดิการ จึงเห็นว่ามีความจำเป็นอย่างยิ่งที่กรม จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ เพื่อรองรับสถานการณ์ดังกล่าวที่อาจจะเกิดขึ้นกับระบบสารสนเทศของกรม แผนนี้จัดแบ่งออกเป็น 3 ด้าน ได้แก่

1. แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ (Contingency Plan)
2. แผนดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan)
3. แผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure)

วัตถุประสงค์

1. เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ
2. เพื่อให้ระบบสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ สามารถดำเนินการได้อย่างต่อเนื่อง
3. เพื่อเตรียมความพร้อมในการรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ (Contingency Plan)

กรณีเครื่องลูกข่าย

1. ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศของกรมทราบ หรือกรณีมีเหตุอันทำให้กลุ่มเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้กลุ่มเทคโนโลยีสารสนเทศจะต้องประกาศให้ทุกหน่วยงานในสังกัดกรมพัฒนาสังคมและสวัสดิการทราบ
2. เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว
3. ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อกลุ่มงาน/หน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ ที่พบการขัดข้องให้ดึงสาย LAN ออกจากชุมสายในชั้นนั้นออกให้หมด
4. ปิดระบบไฟฟ้าที่เข้าเครื่องทั้งหมด
5. ขนย้ายเครื่องไปไว้ในที่ปลอดภัย
6. ให้เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ แจ้งเหตุขัดข้องนั้นให้หัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบโดยเร็วที่สุด

กรณีเครื่องบริการ (Server) และอุปกรณ์เครื่องข่าย

1. ตัดการเชื่อมต่อระบบเครือข่ายโยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ
2. ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า
3. ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว
4. ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server หรือผู้เชี่ยวชาญด้านระบบเครือข่ายโดยเร็วที่สุด
5. ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด
6. ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบโดยเร็ว

แผนดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานได้อย่างต่อเนื่อง
(Continuity of Operation Plan)

เพื่อให้การแก้ไขระบบสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ ที่เกิดจากภัยพิบัติเป็นไปด้วยความรวดเร็ว สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ กรมพัฒนาสังคมและสวัสดิการได้ดำเนินการจัดแบ่งหน้าที่และบุคลากรผู้รับผิดชอบงาน ดังนี้

1. **Chief Information Officer (CIO)** : รองอธิบดี
2. **หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ** : นายศุภศิษฎ์ วิสิฐสรัลพร
3. **ผู้ดูแลระบบเครือข่าย** : นางสาวอังศุวรรณ คุ้มปรีดี
4. **ผู้ช่วยดูแลระบบเครือข่าย** : นายจิรภัทร จันทรรัตนะ
5. **ผู้ประสานงานและดูแลสภาพความพร้อมของระบบเครือข่าย :** นางสาวอังศุวรรณ คุ้มปรีดี
6. **เจ้าหน้าที่ผู้ดูแลระบบงานต่างๆ**

ระบบสารสนเทศของกรมพัฒนาสังคมและสวัสดิการ	ผู้รับผิดชอบ
1. ระบบงานบริการทางสังคม	นางสาวสุจรรยา กสิกิจ นางสาวนภาลัย พงษ์กาญจนะ
2. ระบบติดตามประเมินผลการดำเนินงานตามแผนปฏิบัติราชการ	นางสาวมิ่งขวัญ เพชรแก้วนา
3. ระบบเว็บไซต์หลักที่เผยแพร่ข่าวสารของหน่วยงาน	นายเมธา โตสวัสดิ์ นางสาวสุจรรยา กสิกิจ
4. ระบบเครือข่ายอินเทอร์เน็ตของหน่วยงาน	บริษัท เคมิท กรุ๊ป จำกัด
5. ระบบจัดทำงบประมาณประจำปี	นางสาวนภาลัย พงษ์กาญจนะ
6. ระบบฐานข้อมูลการจัดระเบียบขอทาน	กองคุ้มครองสวัสดิภาพ และเสริมสร้างคุณภาพชีวิต
7. ระบบพัฒนาคุณภาพชีวิตผู้รับบริการในสถานคุ้มครองคนไร้ที่พึ่ง (Qlifeplus)	กองคุ้มครองสวัสดิภาพ และเสริมสร้างคุณภาพชีวิต

<u>แผนการสำรองข้อมูลและกู้คืนข้อมูล (Back up Recovery Procedure)</u>

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery)

ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมรองรับการให้บริการเครื่องลูกข่ายต่างๆได้ ตลอด 24 ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดเนื่องจากเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณต้องทำงานด้านบริการ (Service) แก่เครื่องลูกข่ายให้สามารถใช้งานได้ปกติ การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จำเป็นต้องทำอย่างรวดเร็วเพื่อให้ใช้งานได้อย่างรวดเร็วที่สุด แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และแฟ้มข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน

1. จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง
4. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว
5. นำ BACKUP TAPE / CD - ROM / HARDDISK ที่ได้สำรองข้อมูลไว้มา Restore เพื่อให้งานดำเนินต่อไป
6. ทีมกู้ระบบ (ผู้ดูแลระบบ และบริษัทที่ปรึกษา) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง
7. ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆที่เกี่ยวข้อง

ภาคผนวก

แนวปฏิบัติเมื่อเกิดสถานการณ์ฉุกเฉิน
หรือปัญหาภัยพิบัติของกรมพัฒนาสังคมและสวัสดิการ

1. แนวทางปฏิบัติเที่อเกิดภัยพิบัติจากไฟไหม้ หรือระบบไฟฟ้าขัดข้อง

กรมพัฒนาสังคมและสวัสดิการ ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้ดำเนินการแบ่งหน้าที่ความรับผิดชอบ ดังนี้

1.1 กรณีเกิดภัยจากไฟไหม้

- เมื่อเจ้าหน้าที่ กรมพัฒนาสังคมและสวัสดิการ พบเห็นเหตุการณ์ไฟไหม้ ให้แจ้งผู้บังคับบัญชาทราบโดยทันที พร้อมทั้งมอบหมายให้นางสาวนภาลัย พงษ์กาญจนะ แจ้งตำรวจดับเพลิงและหน่วยงานที่เกี่ยวข้องเข้ามาให้การช่วยเหลือโดยเร็ว
- มอบหมายให้ นางสาวจีรกุล ฝ้ายตระกูล และนางสาวมิ่งขวัญ เพชรแก้วนา ปิดระบบไฟฟ้าที่เข้าสู่เครื่องคอมพิวเตอร์ทั้งหมด
- มอบหมายให้ นายศุภศิษฎ์ วิสิฐสรัลพร และนางสาวสุจรรยา กสิกิจ ทำการปิดระบบไฟฟ้าที่ควบคุมระบบเครือข่ายทั้งหมด เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับระบบเครือข่าย
- มอบหมายให้ นางสาวอังศุวรรณ คุ้มปรีดี, นางสาวศิรินภา ฮงฮุย , นางสาวสิริวรรณ บุญหนุน ทำการเก็บโปรแกรมและแฟ้มข้อมูล, tape backup, รายชื่อโปรแกรม, เอกสารที่เกี่ยวข้องกับระบบปฏิบัติการและโปรแกรม, สำเนาคู่มือต่างๆ ที่เกี่ยวของกับระบบสารสนเทศไว้ในสถานที่ปลอดภัย พร้อมทั้งช่วยกันขนย้ายเครื่องคอมพิวเตอร์ไปไว้ในที่ปลอดภัย
- มอบหมายให้ นายจิรภัทร จันทรรัตนะ ใช้น้ำยาดับเพลิงฉีดในสถานที่เกิดเหตุเพื่อควบคุมเพลิงไว้ก่อนในเบื้องต้น

1.2 กรณีเกิดปัญหาระบบไฟฟ้าขัดข้อง

- ให้เจ้าหน้าที่กรมพัฒนาสังคมและสวัสดิการ แจ้งเหตุขัดข้องดังกล่าวให้ผู้บังคับบัญชาทราบโดยทันที พร้อมทั้งมอบหมายให้นางสาวนภาลัย พงษ์กาญจนะ และนางสาวจีรกุล ฝ้ายตระกูล ประสานหน่วยงานที่เกี่ยวข้องเข้ามาดำเนินการแก้ไขเหตุขัดข้องดังกล่าวโดยเร็ว
- มอบหมายให้ นายศุภศิษฎ์ วิสิฐสรัลพร และ นางสาวอังศุวรรณ คุ้มปรีดี พิจารณาลำดับความสำคัญของการให้บริการ และประสิทธิภาพของเครื่องสำรองไฟฟ้า ในการพิจารณาปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย
- ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย หรือระบบเครือข่ายขัดข้องเนื่องมาจากเหตุไฟฟ้าขัดข้อง มอบหมายให้ นายเมธา โตสวัสดิ์ ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server หรือผู้เชี่ยวชาญด้านระบบเครือข่ายและแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

2. แนวทางปฏิบัติเมื่อมีการถูกเจาะระบบคอมพิวเตอร์

- เมื่อพบความผิดปกติของระบบคอมพิวเตอร์ หรือระบบงานสารสนเทศต่างๆ มอบหมายให้นางสาวนภาลัย พงษ์กาญจนะ หรือนางสาวสุจรรยา กสิกิจ แจ้งข้อมูลเหตุการณ์เบื้องต้นดังกล่าวให้ผู้บังคับบัญชาทราบโดยทันที
- เมื่อมีการถูกเจาะระบบคอมพิวเตอร์ หรือระบบงานสารสนเทศต่างๆ ขึ้น มอบหมายให้นายศุภศิษฎ์ วิสิฐสรัลพร , นางสาวอังศุวรรณ คุ้มปรีดี และ นายจิรภัทร จันทรรัตนะ ตรวจสอบความเสียหายและผลกระทบที่เกิดขึ้นกับการทำงานของเครื่องคอมพิวเตอร์, อุปกรณ์เครือข่าย และข้อมูลที่อยู่บนเครือข่ายทันที พร้อมทั้งประสานงานกับผู้ดูแลระบบหลักเพื่อขอแนวทางการแก้ไขปัญหาในเบื้องต้นก่อน
- มอบหมายให้ นางสาวจีรกุล ฝ้ายตระกูล หรือนางสาวมิ่งขวัญ เพชรแก้วนา ช่วยในการติดต่อและประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server หรือผู้เชี่ยวชาญด้านระบบเครือข่ายและแจ้งให้บริษัทที่รับผิดชอบ ช่วยดำเนินการแก้ไขปัญหาและช่วยประเมินคาวามเสียหายที่เกิดขึ้นพร้อมทั้งขอแนวทางป้องกัน เพื่อไม่ให้เกิดการถูกเจาะระบบคอมพิวเตอร์ได้อีกในอนาคต

3. แนวทางปฏิบัติเมื่อประกาศการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548

- การปฏิบัติหน้าที่ของข้าราชการ เจ้าหน้าที่ให้เป็นไปตามข้อกำหนด ประกาศ หรือคำสั่งต่างๆ ของทางราชการ
- ลักษณะงานที่บุคลากรสามารถปฏิบัติงานที่บ้านหรือที่พักอาศัยได้นั้น หากจำเป็นต้องมีการใช้งานระบบสารสนเทศ ให้ปฏิบัติตามข้อกำหนดในการใช้งานเช่นเดียวกับการปฏิบัติงานที่กรม เช่น การระมัดระวังการเข้าถึงเครื่องคอมพิวเตอร์, ข้อมูล, แฟ้มเอกสารโดยมิได้รับอนุญาต การเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น เป็นต้น
- ผู้ใช้งานระบบทุกคนเมื่อจะใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กรดังนี้
  - แสดงชื่อผู้ใช้งาน (Username)
  - ใส่รหัสผ่าน (Password)
- หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ มีหน้าที่ในการจัดบุคลากรออกเป็นกลุ่ม โดยจัดให้มีบุคลากรที่สามารถปฏิบัติงานด้านการบริการสารสนเทศแก่ผู้ปฏิบัติงานภายในกรม และบุคลากรที่สามารถปฏิบัติงานด้านการบริการสารสนเทศผ่านการทำงานที่บ้านหรือที่พักอาศัยได้

- จัดให้มีการทำระเบียนรายชื่อผู้ปฏิบัติหน้าที่ ระบบงานที่รับผิดชอบ และหมายเลขโทรศัพท์สำหรับติดต่อไว้ยังกลุ่มเทคโนโลยีสารสนเทศ
- กรณีที่จำเป็นต้องมีการเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายองค์กร ต้องควบคุมบุคคลที่จะเข้าสู่ระบบขององค์กรจากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน และต้องรับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศก่อนเท่านั้น

4. การปฏิบัติงานนอกสถานที่ตั้งในภาวะฉุกเฉิน

- กรณีที่บุคลากรไม่สามารถเดินทางมาปฏิบัติงานที่สำนักงานได้ ให้สามารถปฏิบัติงานจากภายนอกสถานที่ตั้งได้ โดยระบบสารสนเทศที่รองรับการทำงานจากภายนอกจะต้องทำงานอยู่บนสถาปัตยกรรมความน่าเชื่อถือ
- ห้ามมิให้บุคลากรบันทึกข้อมูลส่วนบุคคลของกลุ่มเป้าหมาย (Sensitive Personal Data) ลงในอุปกรณ์ส่วนตัว หรืออุปกรณ์จัดเก็บข้อมูลแบบพกพาโดยเด็ดขาด ให้ดำเนินการประมวลผลข้อมูลผ่านระบบคลาวด์ หรือระบบศูนย์ข้อมูลของกรมเท่านั้น

5. ระบบการสื่อสารและแจ้งเหตุสำรอง

- ในกรณีที่ระบบเครือข่ายอินเทอร์เน็ตหลักของกรมขัดข้องจากภัยพิบัติ ให้ผู้มีหน้าที่รับผิดชอบ ดำเนินการใช้ช่องทางการสื่อสารสำรองในการสั่งการและประเมินสถานการณ์
- ให้กลุ่มประชาสัมพันธ์และกลุ่มเทคโนโลยีสารสนเทศ ร่วมกันกำหนดช่องทางสื่อสารฉุกเฉินผ่านแพลตฟอร์มโซเชียลมีเดีย หรือแอปพลิเคชันอย่างเป็นทางการ เพื่อแจ้งเตือนแนวทางการเข้ารับบริการให้แก่กลุ่มเป้าหมายและประชาชนทั่วไปได้รับทราบสถานการณ์อย่างทันท่วงที

6. การบังคับใช้กฎหมายในภาวะฉุกเฉิน

- แม้ในสถานการณ์ฉุกเฉินหรือภัยพิบัติ การเข้าถึงและใช้งานระบบคอมพิวเตอร์ของกรมพัฒนาสังคมและสวัสดิการ ยังคงต้องอยู่ภายใต้การกำกับดูแลตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และระเบียบที่เกี่ยวข้องอย่างเคร่งครัด การอาศัยช่องโหว่ในช่วงเวลาฉุกเฉินเพื่อเข้าถึงข้อมูลโดยมิชอบ ถือเป็นความผิดร้ายแรง