บันทึกข้อความ

ส่วนราชการ กรมการขนส่งทางบก ศูนย์เทคโนโลยีสารสนเทศ โทร. ๑๐๙๓๐๔

ที่ คค ๐๔๒๐/ ว. ๗๑๙๙ **วันที่** ๙ ธันวาคม ๒๕๖๔

เรื่อง ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๕

เรียน รอบ., รอก., รอว., ตรข., ผอ.สำนัก, ผอ.กอง, ผสพ. ๑–๕ ,ขสจ.ทุกจังหวัด และ หสข.ทุกสาขา

ตามที่ กรมการขนส่งทางบกได้ส่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมการขนส่งทางบก ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ (ฉบับทบทวน) ให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) พิจารณาให้ความเห็นชอบก่อนใช้เป็นแนวทางในการปฏิบัติ และ สพธอ. ได้มีหนังสือที่ ดส (สพธอ) ๕๑๑/๑๑๘๙ ลงวันที่ ๒๓ พฤศจิกายน ๒๕๖๔ เรื่อง แจ้งผลการพิจารณานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางบก (ฉบับทบทวน) โดยนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศดังกล่าวได้รับความเห็นชอบแล้ว นั้น

กรมการขนส่งทางบก โดยศูนย์เทคโนโลยีสารสนเทศ ขอแจ้งให้ทราบถึงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมการขนส่งทางบก ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ซึ่งประกอบด้วย แนวปฏิบัติและแผนการดำเนินการที่เกี่ยวข้องในด้านระบบสารสนเทศ ๓ ด้าน ดังนี้

๑) นโยบายและแนวปฏิบัติในการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕

๒) แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ พ.ศ. ๒๕๖๕

๓) แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมการขนส่งทางบก พ.ศ. ๒๕๖๕

ทั้งนี้ ศูนย์เทคโนโลยีสารสนเทศจะได้นำรายละเอียดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕ และแผนการดำเนินการที่เกี่ยวข้องประกาศไว้ที่อินทราเน็ต และเว็บไซต์ของกรมการขนส่งทางบกต่อไป และสามารถสแกนรายละเอียดตาม QR Code ที่ท้ายหนังสือฉบับนี้

จึงเรียนมาเพื่อทราบ และกรุณาแจ้งเจ้าหน้าที่ทุกระดับเพื่อทราบและถือปฏิบัติต่อไป

(นายจิรุตม์ วิศาลจิตร)

อขบ.

shorturl.asia/2OINf

ประกาศกรมการขนส่งทางบก
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ อธิบดีกรมการขนส่งทางบกโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศกรมการขนส่งทางบก เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๕"

ข้อ ๒ บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศฉบับนี้ ให้ใช้ประกาศฉบับนี้แทน

ข้อ ๓ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีวัตถุประสงค์ดังต่อไปนี้

๓.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศของกรมการขนส่งทางบก ทำให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพและมีประสิทธิผล

๓.๒ เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ โดยอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๓.๓ เพื่อเผยแพร่ให้ผู้ใช้งานและผู้รับบริการที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ ได้รับทราบและต้องยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๓.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติที่มีความสอดคล้องกับนโยบายในการรักษาความปลอดภัยด้านสารสนเทศให้ผู้บริหาร ผู้ใช้งาน และผู้ดูแลระบบที่ปฏิบัติงานให้กับกรมการขนส่งทางบกตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศของกรมการขนส่งทางบกในการดำเนินงานและปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามเอกสารแนบท้ายอย่างเคร่งครัด

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางบก

๔.๑ การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ

กรมการขนส่งทางบกมีนโยบายที่จะให้บริการระบบสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวก รวดเร็ว และให้ความคุ้มครองข้อมูลประชาชนที่ไม่พึงเปิดเผย ภายใต้บทบัญญัติของกฎหมาย ซึ่งครอบคลุม ๔ ด้าน ดังนี้

๔.๑.๑ การเข้าถึงระบบสารสนเทศ เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผล

๔.๑.๒ การเข้าถึงระบบเครือข่าย เพื่อป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต

๔.๑.๓ การเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๔.๑.๔ การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่นและระบบสารสนเทศ ต้องมีการควบคุมและจำกัดการเข้าถึงของผู้ใช้งานและผู้รับบริการ เข้าใช้ฟังก์ชั่นต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชั่น

๔.๒ การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

กรมการขนส่งทางบกมีนโยบายที่จะรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีระบบการควบคุมด้านสารสนเทศในการจัดทำเอกสารอิเล็กทรอนิกส์ โครงสร้างพื้นฐานกุญแจสาธารณะและหน่วยงานบริการพื้นฐานต่างๆ การบริการจัดการข้อมูลและเอกสารอิเล็กทรอนิกส์ และการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ ที่มีมาตรฐานในการรักษาความมั่นคงปลอดภัยเป็นที่ยอมรับ

๔.๓ การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

กรมการขนส่งทางบกมีนโยบายในการบริการจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีระบบแยกประเภทและจัดเก็บระบบสารสนเทศเป็นหมวดหมู่ มีระบบสำรองของสารสนเทศที่สมบูรณ์พร้อมใช้งาน รวมทั้งต้องมีแผนฉุกเฉินในการใช้งานระบบสารสนเทศเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๔.๔ การตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศอย่างสม่ำเสมอ

กรมการขนส่งทางบกมีนโยบายให้มีการตรวจสอบ ประเมินความเสี่ยง และกำหนดมาตรการในการควบคุมความเสี่ยงด้านระบบสารสนเทศ โดยกลุ่มตรวจสอบภายในหรือผู้ตรวจสอบอิสระอย่างน้อยปีละ ๑ ครั้ง

๔.๕ การสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศให้กับผู้ดูแลระบบ ผู้ใช้งาน และผู้รับบริการ

กรมการขนส่งทางบกมีนโยบายในการสร้างความตระหนักรู้ความเข้าใจโดยการนำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแผนการดำเนินการที่เกี่ยวข้องกับระบบสารสนเทศ เผยแพร่การใช้งานระบบสารสนเทศที่ถูกต้องเหมาะสมทางเว็บไซต์ภายใน (Intranet) และเว็บไซต์ภายนอก (Internet) ของกรมการขนส่งทางบกให้แก่ผู้ดูแลระบบ ผู้ใช้งาน และผู้รับบริการทราบ

ข้อ ๕ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางบก

๕.๑ การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ กำหนดประเภทของข้อมูล ลำดับความสำคัญหรือลำดับขั้นความลับของข้อมูล และผู้รับบริการในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๕.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งานและผู้รับบริการ เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งานและผู้รับบริการ ตรวจสอบบัญชีผู้ใช้งานและผู้รับบริการ อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งานและ

ผู้รับบริการ เพื่อให้ผู้ใช้งานและผู้รับบริการที่มีสิทธิเท่านั้นที่สามารถเข้าใช้งานระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิการเข้าถึงข้อมูลให้เหมาะสมตรงตามหน้าที่ความรับผิดชอบของผู้ใช้งานและผู้รับบริการ ต้องมีการทบทวนสิทธิการใช้งานและตัดสิทธิการใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตแล้ว และตรวจสอบการละเมิดความปลอดภัยเสมอ

๕.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน กำหนดรหัสผ่านที่มีคุณภาพ การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านภายในระยะเวลาที่กำหนด การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานหรือมีผู้ดูแล

๕.๔ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ต้องกำหนดเส้นทางการเชื่อมต่อระบบสารสนเทศ โดยผ่านระบบรักษาความปลอดภัยตามที่กรมการขนส่งทางบกกำหนดไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งโซน (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๕.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งานหรือผู้รับบริการ และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่างๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์ และป้องกันโปรแกรมไม่ประสงค์ดีต่างๆ

๕.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชั่น ต้องกำหนดสิทธิการเข้าถึงระบบสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชั่นต่างๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเทอร์เน็ต (Internet) ระบบอินทราเน็ต (Intranet) และระบบงานต่างๆ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงาน รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ทั้งนี้ แนวปฏิบัติต่างๆ ดังกล่าวข้างต้นให้ปฏิบัติตามรายละเอียดในแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์เทคโนโลยีสารสนเทศ กรม ตามเอกสารแนบท้ายอย่างเคร่งครัด

ข้อ ๖ จัดทำระบบสำรองของสารสนเทศ ดังนี้

๖.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองของสารสนเทศที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานอย่างเหมาะสม

๖.๒ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบระบบสารสนเทศและระบบสำรองของสารสนเทศ

๖.๓ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถดำเนินงานได้อย่างปกติต่อเนื่อง โดยต้องปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการงานตามภารกิจ

๖.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองของสารสนเทศและแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ ปีละ ๑ ครั้ง

๖.๕ มีการปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรองของสารสนเทศ ปีละ ๑ ครั้ง

ข้อ ๗ ตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ กำหนดให้มีมาตรการในการตรวจสอบควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านระบบสารสนเทศ กำหนดวิธีประเมินความเสี่ยงได้อย่างถูกต้อง ชัดเจน มีประสิทธิภาพ และกำหนดหน้าที่ผู้รับผิดชอบ เพื่อให้ทราบระดับความเสี่ยงและความมั่นคงปลอดภัยด้านระบบสารสนเทศของกรมการขนส่งทางบก โดยต้องตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ ปีละ ๑ ครั้ง

ข้อ ๘ สร้างความรู้ความเข้าใจให้ผู้ดูแลระบบ ผู้ใช้งาน และผู้รับบริการระบบสารสนเทศ เพื่อให้เกิดความเข้าใจและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศที่ไม่ถูกต้อง และส่งเสริมพัฒนาบุคลากรที่เกี่ยวข้องให้มีความสามารถในการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัย โดยผู้ดูแลระบบ ผู้ใช้งาน และผู้รับบริการต้องถือปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๙ ของกรมการขนส่งทางบกอย่างเคร่งครัด

ข้อ ๙ ติดตามการดำเนินงานและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับสภาพแวดล้อมและกฎหมายที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๐ กำหนดความรับผิดชอบ

๑๐.๑ ระดับนโยบาย

๑๐.๑.๑ อธิบดีกรมการขนส่งทางบก ในฐานะผู้บริหารระดับสูงสุดของกรม (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศที่มีความสำคัญเกิดความเสียหาย หรืออันตรายใดๆ แก่กรม หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๐.๑.๒ รองอธิบดีกรมการขนส่งทางบก (ฝ่ายวิชาการ) ในฐานะผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๐.๑.๓ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะและคำปรึกษากับเจ้าหน้าที่ปฏิบัติงาน

๑๐.๒ ระดับปฏิบัติ เป็นผู้รับผิดชอบดูแล และดำเนินการในส่วนที่เกี่ยวข้องกับภารกิจหน้าที่ที่เกี่ยวข้อง ประกอบด้วย ศูนย์เทคโนโลยีสารสนเทศ ผู้ดูแลระบบ ผู้ใช้งาน ผู้รับบริการ กลุ่มตรวจสอบภายใน และฝ่ายอาคารสถานที่

๑๐.๒.๑ ความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy)

๑๐.๒.๒ ความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

๑๐.๒.๓ ความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

๑๐.๒.๔ ความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-Mail Policy)

๑๐.๒.๕ ความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

๑๐.๒.๖ ความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

๑๐.๒.๗ ความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (IDS/IPS Policy)

๑๐.๒.๘ การสำรองและกู้คืนข้อมูล (Backup and Recovery)

๑๐.๒.๙ การใช้เครื่องคอมพิวเตอร์และอุปกรณ์พกพา

๑๐.๒.๑๐ การเข้าถึงห้องเครื่องคอมพิวเตอร์และห้องเครือข่ายสื่อสารข้อมูล

๑๐.๒.๑๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑๐.๒.๑๒ การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๑๐.๒.๑๓ การปฏิบัติงานภายนอกสำนักงาน (Teleworking)

ข้อ ๑๑ ให้ศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบก เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากประกาศเป็นต้นไป

ประกาศ ณ วันที่ - ๙ ธ.ค. ๒๕๖๔

นายจิรุตม์ วิศาลจิตร
(อธิบดีกรมการขนส่งทางบก)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบก

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร โดยในปีงบประมาณ พ.ศ. ๒๕๕๙ กรมการขนส่งทางบก ได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นไปตามมาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ แล้วนั้น และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ข้อที่ ๓ หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน และต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรม มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง รวมถึงมีการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศที่ไม่ถูกต้องหรือจากภัยคุกคามต่าง ๆ จากผู้ไม่ประสงค์ดี จึงต้องทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม ประจำปี พ.ศ. ๒๕๖๕ เพื่อเป็นแนวทางในการปฏิบัติ โดยให้เป็นปัจจุบันตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ

๑. วัตถุประสงค์

ศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบก ได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด โดยมีวัตถุประสงค์ ดังนี้

๑. เพื่อปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางบก ให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องและเป็นปัจจุบันเหมาะสมกับสถานการณ์ และเป็นไปตามกฎหมาย พระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ ที่เกี่ยวข้องในเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๒. เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ โดยอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๓. เพื่อกำหนดแนวทางและวิธีปฏิบัติสำหรับบุคลากรและบุคคลที่ปฏิบัติงานให้กับกรมการขนส่งทางบก ในการยืนยันตัวตน การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ และบุคลากรของกรมการขนส่งทางบกได้รับทราบและถือปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด

๔. เพื่อให้มีแผนเตรียมความพร้อมกรณีฉุกเฉินกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามปกติ การสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และให้สามารถกู้คืนข้อมูลได้ภายในระยะเวลาที่เหมาะสม

๕. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศอย่างสม่ำเสมอ

๖. เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ และสร้างความเข้าใจเกี่ยวกับข้อมูลการรักษาความมั่นคงปลอดภัยและระบบสารสนเทศให้แก่บุคลากรที่เกี่ยวข้อง โดยให้มีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

๒. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบก ดังนี้

ส่วนที่ ๑ นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy)

ส่วนที่ ๒ นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ส่วนที่ ๓ นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

ส่วนที่ ๔ นโยบายความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

ส่วนที่ ๕ นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

ส่วนที่ ๖ นโยบายความมั่นคงปลอดภัยของการเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access control Policy)

ส่วนที่ ๗ นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System)

ส่วนที่ ๘ นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery)

ส่วนที่ ๙ นโยบายการใช้เครื่องคอมพิวเตอร์และอุปกรณ์พกพา

ส่วนที่ ๑๐ นโยบายการควบคุมการเข้าถึงห้องเครื่องคอมพิวเตอร์และห้องเครือข่ายสื่อสารข้อมูล

ส่วนที่ ๑๑ นโยบายด้านการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๑๒ นโยบายการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

ส่วนที่ ๑๓ นโยบายการปฏิบัติงานภายนอกสำนักงาน (Teleworking)

ส่วนที่ ๑๔ การกำหนดหน้าที่ความรับผิดชอบ

คำนิยาม

(๑) นโยบาย หมายถึง นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(๒) กรม หมายถึง กรมการขนส่งทางบก

(๓) ผู้บริหาร หมายถึง อธิบดี รองอธิบดี หรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรม

(๔) ผู้ใช้งาน หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของกรมการขนส่งทางบก รวมถึงบุคคลภายนอกที่เป็นหน่วยงานราชการ รัฐวิสาหกิจ ผู้ประกอบการที่เกี่ยวข้อง หรือผู้ที่ได้รับอนุญาตให้ใช้ระบบสารสนเทศและระบบเครือข่ายของกรม

(๕) ผู้รับบริการ หมายถึง ผู้ที่มารับบริการจากกรมโดยตรง หรือผ่านทางช่องทางการสื่อสารอื่นๆ ซึ่งจะต้องเป็นผู้รับบริการหลัก รวมถึงบุคคล ประชาชน หรือองค์กรเอกชน องค์กรรัฐและองค์กรในลักษณะอื่นๆ

(๖) ผู้บุกรุก (Hacker) หมายถึง ผู้ที่พยายามที่จะเจาะเข้าระบบโดยไม่ได้รับอนุญาต หรือผู้ใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์ แต่ไม่ได้มีจุดมุ่งหมายเพื่อทำลายหรือในด้านลบ แต่อย่างไรก็ตาม การที่เจาะเข้าระบบสารสนเทศของผู้อื่นนั้นเป็นสิ่งผิดกฎหมาย

(๗) สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศที่กรมการขนส่งทางบกกำหนดให้เข้าถึงระบบเท่านั้น

(๘) สินทรัพย์ (Asset) หมายถึงเครื่องคอมพิวเตอร์ ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลสารสนเทศ ระบบเครือข่าย ระบบสารสนเทศหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของหน่วยงาน

(๙) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือ การมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

(๑๐) ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) ความน่าเชื่อถือ (Reliability) ทั้งนี้ เพื่อป้องกันการสูญเสีย สูญหาย การถูกขโมย การเข้าถึงหรือการเปิดเผยโดยไม่ได้รับอนุญาต การปลอมแปลง การปฏิเสธความรับผิดหรือการกระทำใดก็ตามที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศ

(๑๑) เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๒) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของกรมการขนส่งทางบกถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๑๓) ระบบสารสนเทศ หมายถึง ระบบงานของกรมที่จะนำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างระบบงานเพื่อให้บริการหรือสนับสนุนการปฏิบัติงานและนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

(๑๔) ระบบอินเทอร์เน็ต หมายถึง ระบบเครือข่ายสื่อสารที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของกรมเข้ากับเครือข่ายอินเทอร์เน็ตสากล

(๑๕) หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานที่ไม่ได้อยู่ภายใต้สังกัดกรมการขนส่งทางบกที่กรมการขนส่งทางบกอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

(๑๖) จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อมูลระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน โดยข้อมูลที่รับส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียงในรูปแบบดิจิตอล ที่สามารถส่งไปยังผู้รับคนเดียวหรือหลายคนได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP๓ และ IMAP

(๑๗) ผู้ดูแลระบบ หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบสารสนเทศและระบบเครือข่ายไม่ว่าส่วนใดส่วนหนึ่ง

(๑๘) ผู้ดูแลการใช้งานระบบคอมพิวเตอร์ (User Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่รับผิดชอบในการกำหนดสิทธิให้กับผู้ใช้งานแต่ละหน่วยงาน

(๑๙) บัญชีชื่อผู้ใช้งาน (Username) หมายถึง บัญชีของผู้ใช้งานที่ได้รับอนุญาต (Authorized user) ให้สามารถใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศของกรมการขนส่งทางบก โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาทที่กรมการขนส่งทางบกกำหนด

(๒๐) รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

(๒๑) การเข้ารหัสลับ (Encryption) หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

(๒๒) การพิสูจน์ตัวตน (Authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ เพื่อยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

(๒๓) ระบบเครือข่ายไร้สาย (WLAN= Wireless Local Area Network) หมายถึง ระบบการสื่อสารข้อมูลที่นำมาใช้ทดแทนหรือเพิ่มต่อกับระบบเครือข่ายแลนใช้สายแบบดั้งเดิมโดยใช้การส่งคลื่นความถี่วิทยุในย่านวิทยุ RF และคลื่นอินฟราเรดในการรับและส่งข้อมูลระหว่างคอมพิวเตอร์ แต่ละเครื่องผ่านทางอากาศ ทะลุกำแพง เพดาน หรือสิ่งก่อสร้างอื่นๆ โดยปราศจากความต้องการของการเดินสาย

(๒๔) Software-defined Wide-area Network **(SD-WAN)** หมายถึง การใช้แนวคิดตามเทคโนโลยีอย่าง Software-Defined Networking (SDN) มาประยุกต์ใช้กับเครือข่าย WAN เพื่อให้องค์กรสามารถควบรวมฟังก์ชั่นการทำงานในหลายรูปแบบ ให้สามารถอยู่บนแพลตฟอร์มเดียวกัน

(๒๕) Multiprotocol Label Switching (MPLS) หมายถึง โปรโตคอลที่ IETF กำหนดขึ้นสำหรับการทำงานรับส่งข้อมูลของสวิตซ์เร้าเตอร์ที่มีการกำหนดเส้นทางไว้ให้ไปถึงจุดหมายได้เร็วขึ้น ด้วยกระบวนการในการจัดส่ง IP-Packet

(๒๖) SSL VPN หมายถึง การนำโครงข่ายสาธารณะมาใช้เป็นสื่อในการส่งข้อมูลระหว่างหน่วยงานภายในองค์กร โดยการใช้การเข้ารหัสข้อมูล สร้างระบบเครือข่ายเสมือนขึ้นเพื่อให้ข้อมูลที่ส่งผ่านระหว่างต้นทางและปลายทางยังคงมีความปลอดภัย

(๒๗) เทคโนโลยีเครือข่ายเสมือนส่วนตัว (Virtual Private Network :VPN) หมายถึง เป็นเทคโนโลยีการเชื่อมต่อเครือข่ายนอกอาคาร (WAN - Wide Area Network) เป็นระบบเครือข่ายภายในองค์กรซึ่งเชื่อมเครือข่ายในแต่ละสาขาเข้าด้วยกัน โดยอาศัย Internet เป็นตัวกลาง มีระบบเข้ารหัสป้องกันการลักลอบใช้ข้อมูลได้

(๒๘) DMZ (Demilitarized Zone) หมายถึง เป็นคำจำกัดความของโซนอีกประเภทหนึ่งที่ไม่ใช่ทั้ง Internal (เครือข่ายภายใน) และ External (เครือข่ายภายนอกหรือเครือข่ายอินเทอร์เน็ต) แต่หมายถึงเครือข่ายที่ต้องมีการสื่อสารกับทั้งเครือข่ายภายในและเครือข่ายภายนอก

(๒๙) มาตรฐานสากล ISO/IEC ๒๗๐๐๑ หมายถึง เป็นมาตรฐานที่พัฒนาขึ้นโดย ISO (Information security management system, ITSM) เพื่อสร้างความมั่นใจถึงความมีประสิทธิผลและประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศองค์กร รวมถึงการดำเนินการที่สอดคล้องตามข้อกำหนดด้านระบบความมั่นคงปลอดภัยทั้งของลูกค้า ข้อกฎหมาย และระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้องด้วย

(๓๐) สื่อบันทึกพกพา หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Disk หรือ Floppy disk เป็นต้น

(๓๑) อุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile computing devices) หมายถึง อุปกรณ์คอมพิวเตอร์ขนาดเล็กที่สามารถพกพาหรือเคลื่อนย้ายไปกับตัวบุคคล ไปยังสถานที่ต่างๆ ได้โดยง่ายและมีน้ำหนักเบา เช่น เครื่องคอมพิวเตอร์โน้ตบุ๊ก โทรศัพท์มือถือ หรือแท็บเล็ต เป็นต้น

(๓๒) ไวรัสหรือชุดคำสั่งไม่พึงประสงค์ หมายถึง รหัสคอมพิวเตอร์ที่ฝังตัวเองในไฟล์หรือโปรแกรมใดก็ตามที่จะแพรกระจายตัวเองจากคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์อีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งผ่านทางเครือข่ายสาธารณะ หรือชุดคำสั่งที่เข้ามาโดยไม่ได้รับอนุญาตหรือโดยไม่รู้ตัวและทำความเสียหายแกระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศต่างๆ อาจสร้างความเดือดร้อนรำคาญ ทำให้เครื่องคอมพิวเตอร์ทำงานช้าหรือทำงานผิดปกติหรือทำงานใน

ลักษณะที่ไม่เป็นประโยชน ไมสร้างสรรค์หรือไม่เป็นผลดีต่อเครื่องคอมพิวเตอร์นั้น ซึ่งความรุนแรงในการก่อความเสียหายอาจแตกต่างกันตามแต่ละชนิดของไวรัสหรือชุดคำสั่งไมพึงประสงค์นั้น

(๓๓) ทรัพย์สินทางปัญญา หมายถึง ผลงานใดๆ อันเกิดจากความคิดสร้างสรรค์ของมนุษย์ โดยทรัพย์สินทางปัญญาเป็นสินทรัพย์อีกประเภทหนึ่งที่นอกเหนือจากสังหาริมทรัพย์ และอสังหาริมทรัพย์ ประเภทของทรัพย์สินทางปัญญาประกอบด้วยลิขสิทธิ์ (Copyright) สิทธิบัตร (Patent) เครื่องหมายการค้า (Trademark) แบบผังภูมิของวงจร (Layout-Designs of Integrated Circuit) ความลับทางการค้า (Trade Secrets) และสิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication)

ส่วนที่ ๑
นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
(Acceptable Use Policy)

๑. วัตถุประสงค์

กำหนดกรอบและแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมการขนส่งทางบก ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC ๒๗๐๐๑ อีกทั้งลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังถูกโจมตีสิ้นสุดลง เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของกรม

๒.แนวทางปฏิบัติ

หมวด ๑ ว่าด้วยการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

ข้อ ๑ ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองห้ามใช้ร่วมกับผู้อื่นรวมทั้งห้ามทำการเผยแพร่แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๒ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆที่เกิดจากบัญชีของผู้ใช้งาน (Username)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๓ ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัยโดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า๑ ตัวอักษร และไม่เกิน ๑๖ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet)และตัวอักษรพิเศษ (Special character)

ข้อ ๔ ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้วภายใน ๖ เดือน

ข้อ ๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๖ เดือนหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๖ ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศขององค์กรโดย

(๑) การใช้งานคอมพิวเตอร์และคอมพิวเตอร์พกพาทั้งที่เป็นทรัพย์สินของกรม ส่วนตัว หรือของบุคคลภายนอกต้องทำการพิสูจน์ตัวตนผ่านระบบที่กรมการขนส่งทางบกจัดหาไว้(Authentication) ก่อนการใช้งาน

(๒) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน (Authentication) และต้องบันทึกข้อมูล เพื่อบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(๓) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้งและต้องทำการพิสูจน์ตัวตน (Authentication) ก่อนการใช้งานทุกครั้ง

(๔) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ(screen saver) โดยตั้งเวลาอย่างน้อย ๕ นาที

ข้อ ๗ หากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านการโดนล็อค หรือเกิดจากความผิดพลาดใดๆที่เกิดขึ้นจากผู้ใช้งาน หรือจากระบบ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

หมวด ๒ ว่าด้วยการบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๑ ผู้ใช้งานต้องไม่เข้าไปใน ส่วน Data Center ของกรมการขนส่งทางบกที่เป็นเขตหวงห้ามโดยเด็ดขาดเว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๒ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องเครื่องคอมพิวเตอร์แม่ข่ายและห้องเครือข่ายสื่อสารกรมการขนส่งทางบก เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายของกรมการขนส่งทางบกเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๔ ผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใดๆ

ข้อ ๕ ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อสารบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนบันทึกข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
Paper	ใช้เครื่องย่อยทำลายเอกสาร
Flash Drive	- ใช้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งเป็นมาตรฐานการเขียนทับข้อมูลเดิมแบบหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
CD/DVD	- ใช้เครื่องย่อยทำลายเอกสาร ใช้วิธีการทุบหรือบดให้เสียหาย
Tape	- ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
Hard Disk	- ใช้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งเป็นมาตรฐานการเขียนทับข้อมูลเดิมแบบหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

ข้อ ๖ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

ข้อ ๗ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่กรมการขนส่งทางบกมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเองการรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่กรมการขนส่งทางบกมอบหมาย

ข้อ ๘ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของกรมที่ได้รับมอบหมาย

ข้อ ๙ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุดหรือสูญหายตามมูลค่าทรัพย์สินหากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๑๐ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมคอมพิวเตอร์หรือคอมพิวเตอร์พกพา ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ ๑๑ ทรัพย์สินและระบบสารสนเทศต่างๆ ที่กรมจัดเตรียมไว้ให้ใช้งาน มีวัตถุประสงค์เพื่อการใช้งานของกรมเท่านั้นห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆไปใช้ในกิจกรรมที่กรมไม่ได้กำหนดหรือทำให้เกิดความเสียหายต่อกรม

ข้อ ๑๒ ความเสียหายใดๆที่เกิดจากการละเมิดตามข้อ๑๑ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งาน (User) ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด ๓ ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ ๑ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของกรมหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๒ ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของกรมถือเป็นทรัพย์สินของกรมห้ามไม่ให้ทำการเผยแพร่เปลี่ยนแปลงทำซ้ำหรือทำลายโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายหน้าที่ให้ปฏิบัติราชการแทน

ข้อ ๓ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของกรมหรือข้อมูลของผู้รับบริการหากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิดการเผยแพร่โดยไม่รับอนุญาตผู้ใช้งาน (User) ต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๔ ผู้ใช้งานต้องป้องกันดูแลรักษาไว้ซึ่งความลับความถูกต้องและความพร้อมใช้ของข้อมูล

ข้อ ๕ ผู้ใช้งานต้องรักษาและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กรมจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่กรมต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับกรม ซึ่งกรมอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๖ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

หมวด ๔ ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ ๑ ผู้ใช้งานมีสิทธิที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆแต่ต้องไม่ดำเนินการดังนี้

๑.๑ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่านการลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือถอดรหัสผ่านของบุคคลอื่น

๑.๒ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆซึ่งทำให้ผู้ใช้มีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

๑.๓ พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๑.๔ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

๑.๕ นำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทยกรณีที่ผู้ใช้สร้างเว็บเพ็จบนเครือข่ายคอมพิวเตอร์

ข้อ ๒ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น โปรแกรมบิทเทอร์เรนท์ (Bit torrent) อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมาย

ข้อ ๓ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ออนไลน์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๔ ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภทรวมถึงอุปกรณ์อื่นใดของกรมการขนส่งทางบกที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูลข้อความรูปภาพหรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม กฎหมาย หรือความมั่นคงของประเทศ หรือกระทบต่อภารกิจของกรมการขนส่งทางบก

ข้อ ๕ ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของกรมการขนส่งทางบกเพื่อการรบกวน ก่อให้เกิดความเสียหายหรือใช้ในการโจรกรรมข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรมหรือกระทบต่อภารกิจของกรมการขนส่งทางบก

ข้อ ๖ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกรมการขนส่งทางบกเพื่อประโยชน์ทางการค้า

ข้อ ๗ ห้ามกระทำการใดๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของกรมการขนส่งทางบกโดยเด็ดขาดไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ ๘ ห้ามกระทำการรบกวนทำลายหรือทำให้ระบบสารสนเทศของกรมการขนส่งทางบกต้องหยุดชะงัก

ข้อ ๙ ห้ามใช้ระบบสารสนเทศของกรมการขนส่งทางบกเพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๑๐ ห้ามกระทำการใดๆอันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๑๑ ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของกรมการขนส่งทางบกโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด ๕ ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

ข้อ ๑ บรรดากฎหมายใดๆที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบขององค์กรถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้นดังนั้นหากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าวถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๒ การประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งได้กำหนดช่องทางในการสื่อสารและประกาศไว้ในเว็บไซต์หลักของกรมการขนส่งทางบก www.dlt.go.th และอินทราเน็ตของกรม http://Intranet.dlt.go.th พร้อมออกหนังสือเวียน เพื่อให้ทุกหน่วยงานในสังกัดกรมและเจ้าหน้าที่ทุกระดับได้เข้าถึง เข้าใจและสามารถปฏิบัติตามนโยบายและแนวปฏิบัติได้อย่างถูกต้อง

หมวด ๖ ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

ข้อ ๑ กรมได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญาดังนั้นซอฟต์แวร์ที่องค์กรอนุญาตให้ใช้งานหรือที่กรมมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ กรมถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๒ ซอฟต์แวร์ (Software) ที่กรมได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลงแก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด ๗ ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

ข้อ ๑ คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์(Antivirus) ตามที่กรมได้ประกาศให้ใช้เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องมือเพื่อการศึกษาพัฒนาระบบป้องกันโดยต้องได้รับอนุญาตจากผู้บังคับบัญชาผู้ที่ได้รับมอบหมาย

ข้อ ๒ บรรดาข้อมูลไฟล์ซอฟต์แวร์หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรงแกรมไม่พึงประสงค์ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๓ ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอเพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๔ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่พึงประสงค์ตลอดเวลารวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๕ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัสผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๖ ห้ามลักลอบทำสำเนาเปลี่ยนแปลงลบทิ้งซึ่งข้อมูลข้อความเอกสารหรือสิ่งใดๆที่เป็นทรัพย์สินของกรมการขนส่งทางบกหรือของผู้อื่นโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๗ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์มัลแวร์หรือโปรแกรมอันตรายใดๆที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของกรมการขนส่งทางบก

ข้อ ๘ กรณีเครื่องคอมพิวเตอร์หรือระบบมีปัญหาผู้ใช้งานต้องทำการสำรองข้อมูลที่จำเป็นของผู้ใช้งานเอง ก่อนที่จะทำการกู้คืนหรือตรวจสอบแก้ไขระบบ

หมวด ๘ ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

ข้อ ๑ ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

ส่วนที่ ๒
นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย
(Wireless Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย(Wireless LAN) ของกรม โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย (Wireless LAN)

๒. แนวทางปฏิบัติ

ข้อ ๑ ผู้ดูแลระบบต้องรับผิดชอบและควบคุมดูแลไม่ให้ผู้ใช้งานนำอุปกรณ์เครือข่ายไร้สายมาติดตั้งเองในระบบเครือข่ายของกรมการขนส่งทางบกโดยไม่ได้รับอนุญาต

ข้อ ๒ การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน

ข้อ ๓ ห้ามผู้ใช้งานเปิดการใช้ad-hoc หรือ peer-to-peer Network

ข้อ ๔ การวางอุปกรณ์กระจายสัญญาณ (Access Point) ในตำแหน่งที่เหมาะสม โดยต้องวางหน้าไฟร์วอลล์หากมีความจำเป็นต้องวางในระบบเครือข่ายภายในต้องเพิ่มการรับรองด้วยการพิสูจน์ตัวตน (Authentication) และการเข้ารหัส (Encryption)

ข้อ ๕ ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๖ ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำ อุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๗ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point)

ข้อ ๘ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้ให้เข้าใช้ระบบเครือข่ายไร้สายได้เท่านั้น

ข้อ ๙ ผู้ดูแลระบบควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๑๐ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานต่อผู้บังคับบัญชาทราบทันที

ข้อ ๑๑ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

ข้อ ๑๒ ผู้ดูแลระบบต้องมีแผนงานในการตรวจสอบเครือข่ายไร้สายที่มีอยู่ (WAR DRIVE)ในองค์กรเป็นระยะๆ เพื่อป้องกันการลักลอบติดตั้งอุปกรณ์โดยไม่ได้รับอนุญาต

ส่วนที่ ๓
นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์
(Firewall Policy)

๑. วัตถุประสงค์

เพื่อควบคุมการสื่อสารระหว่างเครือข่ายภายในองค์กรกับเครือข่ายภายนอกกรม โดยการตั้งค่าของไฟร์วอลล์ (Firewall) และอุปกรณ์ที่อนุญาตให้เชื่อมโยงภายในกรม ให้มีประสิทธิภาพในการทำงาน รวมทั้งต้องทบทวนสิทธิของผู้ใช้งานอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ (System Administrators) เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบไฟร์วอลล์ (Firewall)

๒. แนวทางปฏิบัติ

ข้อ ๑ ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการระบบรักษาความปลอดภัยไฟร์วอลล์ทั้งหมด

ข้อ ๒ ผู้ดูแลระบบต้องกำหนดนโยบาย (Policy) การใช้งานไฟร์วอลล์

ข้อ ๓ ผู้ดูแลระบบต้องกำหนดค่า (Configuration) หรือกำหนดนโยบาย (Policy) เพื่อกลั่นกรองข้อมูลให้มีความปลอดภัยต่อระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ของกรมการขนส่งทางบก ป้องกันการบุกรุก ไวรัส รวมทั้ง malicious code ต่าง ๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบสารสนเทศ

ข้อ ๔ ผู้ดูแลระบบต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะผิดปกติ ต้องดำเนินการแก้ไข และรายงานผู้บังคับบัญชาโดยทันที

ข้อ ๕ ผู้ดูแลระบบต้องเปิดใช้งานไฟร์วอลล์ตลอดเวลา

ข้อ ๖ การเปิดใช้บริการ (Service) ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันเพิ่มเติม

ข้อ ๗ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๘ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๙ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๐ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๑๑ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำ ทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๑๒ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๓ ผู้ดูแลระบบมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๑๔ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องกระทำผ่าน VPN เท่านั้น และต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบ

ข้อ ๑๕ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ทันที

ข้อ ๑๖ ผู้ขอใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ โดยระบุข้อมูลดังนี้

๑. หมายเลข Port ที่ต้องการเปิด

๒. หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๓. วัตถุประสงค์ หรือ Application ที่ต้องการใช้งานผ่าน Port นั้น ๆ

๔. วันที่เริ่มใช้ และวันที่สิ้นสุดการใช้

ข้อ ๑๗ ในการขอใช้งานหากพบว่าขัดต่อนโยบาย ประกาศ ระเบียบ ของการมการขนส่งทางบกหรือกฎหมาย หรืออาจเกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศจะไม่อนุญาตให้ใช้งาน

ข้อ ๑๘ ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของกรม หรือกฎหมาย หรืออาจเกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศจะยกเลิกการให้บริการทันที

ส่วนที่ ๔
นโยบายความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์
(E-mail Policy)

๑. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail l) ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบ (System Administrators) เครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบ (System Administrators) เครือข่ายนั้นอย่างเคร่งครัด ซึ่งจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติ

ข้อ ๑ ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานโดยยื่นคำขอกับศูนย์เทคโนโลยีสารสนเทศ

ข้อ ๒ เมื่อผู้ใช้งาน (User)ได้รับรหัสผ่าน (Password) ในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ขององค์กรแล้ว และเมื่อมีการเข้าสู่ระบบในครั้งแรกควรเปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ ๓ ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบสารสนเทศหรือบนอุปกรณ์ใกล้เคียงอื่น

ข้อ ๔ ควรเปลี่ยนรหัสผ่าน (Password) ทุก ๓ เดือนหรือเมื่อพบความผิดปกติกับระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๕ ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

ข้อ ๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๗ การส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

ข้อ ๘ การลงทะเบียนและเงื่อนไขในการใช้งานระบบจดหมายอิเล็กทรอนิกส์ ให้เป็นไปตามแนวทางปฏิบัติการเข้าถึงระบบสารสนเทศของกรมการขนส่งทางบก และข้อกำหนดของการให้บริการ e-mail ภาครัฐ (MailGoThai)

ข้อ ๙ ข้อกำหนดและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของกรมการขนส่งทางบก

๙.๑ ศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบก เป็นผู้ควบคุมดูแลระบบจดหมายอิเล็กทรอนิกส์ของกรมที่ให้บริการแก่ผู้ใช้งาน ภายใต้ข้อกำหนดและเงื่อนไขต่างๆ ที่สามารถปรับปรุงให้ทันสมัยโดยไม่ต้องแจ้งให้ทราบล่วงหน้า ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดและเงื่อนไขตลอดระยะเวลาที่ใช้บริการอย่างเคร่งครัด

๙.๒ เพื่อความปลอดภัยในข้อมูลส่วนบุคคลของผู้ใช้งานและผู้ใช้บริการรายอื่น และเพื่อความเป็นระเบียบเรียบร้อยในการใช้บริการ ผู้ใช้งานต้องไม่กระทำการใดอันเป็นการกระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ การล่วงละเมิดสิทธิส่วนบุคคลหรือสิทธิอื่นใดของบุคคลอื่น และ/หรือสิทธิในทรัพย์สินทางปัญญาของหน่วยงานหรือของบุคคลอื่น รวมทั้งต้องไม่กระทำการ

ใดอันขัดต่อข้อตกลงและเงื่อนไขนี้ ศูนย์เทคโนโลยีสารสนเทศสามารถที่จะลบ ทำให้หยุดชั่วคราว หรือถาวร หรือนำเสนอ และตรวจสอบข้อมูลส่วนบุคคลของผู้ใช้งานได้ตลอดเวลาตามความต้องการของกฎหมาย หรือเพื่อปกป้อง และป้องกันสิทธิ ทรัพย์สิน หรือผลประโยชน์ของกรมและบุคคลภายนอก หรือเพื่อวัตถุประสงค์อื่นใดก็ตาม โดยไม่ต้องบอกกล่าวล่วงหน้า

๙.๓ การให้บริการระบบจดหมายอิเล็กทรอนิกส์กรม มีวัตถุประสงค์เพื่อใช้ในการติดต่อสื่อสารที่เกี่ยวข้องกับการปฏิบัติราชการเท่านั้น ผู้ใช้งานได้ตกลงยินยอมว่าผู้ใช้งานจะเป็นผู้รับผิดชอบในข้อมูล เนื้อหา ข้อความ ซอฟต์แวร์ เสียง เพลง รูปภาพ วิดีโอ หรือข้อมูลอื่นๆ ทั้งหมดแต่ผู้เดียว (ต่อไปนี้จะเรียกว่า “เนื้อหา”) ซึ่งผู้ใช้งานได้ส่งเข้ามาไม่ว่าโดยวิธีใดก็ตาม เนื้อหาทั้งหมดที่ถูกส่งมาจะอยู่ในความรับผิดชอบของบุคคลผู้ริเริ่มนั้น กรมจะไม่รับประกันในความถูกต้องสมบูรณ์และคุณภาพของเนื้อหาดังกล่าว และผู้ใช้งานตกลงยินยอมที่จะไม่กระทำการ ดังต่อไปนี้

(๑) ใช้บริการเพื่อการทำจดหมายลูกโซ่ จดหมายโฆษณา จดหมายที่มีข้อความเป็นที่ต้องการ ทั้งทางด้านการค้าหรืออื่นๆ

(๒) เก็บหรือสะสมข้อมูลเกี่ยวกับผู้อื่นรวมทั้งที่อยู่ของจดหมายอิเล็กทรอนิกส์โดยมิได้รับความยินยอม

(๓) สร้างหลักฐานหรือที่อยู่จดหมายอิเล็กทรอนิกส์ปลอม หรือการกระทำการใดๆ ก็ตาม เพื่อหลอกลวงผู้อื่นให้เข้าใจผิดเกี่ยวกับที่มาของข้อความและผู้ส่งข้อความนั้น

(๔) เนื้อหาผ่านบริการโดยผิดกฎหมายหรือศีลธรรม หมิ่นประมาท กล่าวโทษ ขู่เข็ญ คุกคาม สร้างความเสียหาย ลามก หยาบโลนหรือเป็นที่น่ารังเกียจของผู้อื่น

(๕) ส่งเนื้อหาใดใดที่เป็นการละเมิดทรัพย์สินทางปัญญา หรือสิทธิอื่นของบุคคลหรือสถาบันอื่นรวมทั้งเครื่องหมายการค้า ลิขสิทธิ์ หรือสิทธิในการเผยแพร่ต่างๆ

(๖) ส่งเนื้อหาใดใดที่มีไวรัสหรือโปรแกรมที่เป็นอันตราย

(๗) ขัดขวาง แทรกแซง หรือรบกวนเครือข่ายของบริการ หรือฝ่าฝืนข้อบังคับนโยบาย หรือการปฏิบัติจองเครือข่ายนั้น

(๘) พยายามฝ่าฝืนเข้าสู่บริการของบัญชีผู้อื่น ระบบสารสนเทศหรือเครือข่ายของบริการ โดยมิได้รับอนุญาต หรือรบกวนการใช้งานของผู้ใช้งานอื่น

๙.๔ ศูนย์เทคโนโลยีสารสนเทศอาจเข้าถึงหรือเปิดเผยข้อมูลการสื่อสารของผู้ใช้งานเพื่อปฏิบัติตามกฎหมาย หรือตอบสนองต่อการเรียกร้องที่ชอบด้วยกฎหมาย หรือกระบวนการทางกฎหมาย หรือเพื่อปกป้องสิทธิหรือทรัพย์สินของหน่วยงานหรือของผู้ใช้บริการอื่น

๙.๕ ศูนย์เทคโนโลยีสารสนเทศอาจยุติการให้บริการชั่วคราว เพื่อเพิ่มระบบรักษาความปลอดภัยหรือหยุดยั้งการก่อกวนระบบการให้บริการ

๙.๖ ศูนย์เทคโนโลยีสารสนเทศจะไม่รับประกันความเสียหายหรือสูญหายของข้อมูลที่เก็บไว้ในระบบ

๙.๗ กรณีเกิดความสูญหายหรือเสียหายขึ้นเนื่องจากการใช้บริการ หรือจากการละเมิดระเบียบกฎเกณฑ์และเงื่อนไขนี้ไม่ว่าโดยบุคคลใด การเขียนและเผยแพร่ข้อความที่ต้องห้าม กรมไม่ต้องรับผิดชอบใดๆ ทั้งสิ้นต่อผู้ใช้งาน และ/หรือบุคคลผู้เสียหายนั้น ผู้ใช้งานต้องรับผิดชอบและรับผลเสียหายที่เกิดขึ้นนั้นแต่เพียงผู้เดียว ทั้งนี้ผู้ใช้งานตกลงสละสิทธิเรียกร้องให้กรมรับผิดชอบในความสูญหายและเสียหายใดๆ ที่เกิดขึ้นจากการใช้บริการนี้ทั้งสิ้น นอกจากนี้ ผู้ใช้งานต้องปกป้องมิให้กรมต้องรับผิดชอบหรือฟ้องร้องจากบุคคลอื่นอันเนื่องมาจากบริการนี้ รวมทั้งจะต้องรับผิดชอบและชดใช้ค่าเสียหายต่างๆ ที่เกิดขึ้นเองทั้งสิ้น

ข้อ ๑๐ การลงทะเบียนผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของกรม

๑๐.๑ ระบบจดหมายอิเล็กทรอนิกส์ของกรมบริการสำหรับข้าราชการ ลูกจ้าง และพนักงานราชการ ในสังกัดกรมเท่านั้น

๑๐.๒ ในการลงทะเบียนผู้ใช้งานสำหรับบุคคล ผู้ใช้งานต้องลงทะเบียนด้วยตัวเองผ่านช่องทางที่ศูนย์เทคโนโลยีสารสนเทศเปิดให้ และตกลงที่จะให้ข้อมูลที่เป็นจริง ถูกต้อง ครบถ้วน และล่าสุดเกี่ยวกับตัวของผู้ใช้งานเองในแบบลงทะเบียนคงไว้ซึ่งความถูกต้องและเป็นจริงของข้อมูลของผู้ใช้งาน ในการลงทะเบียนหากผู้ใช้งานได้ให้ข้อมูลดังกล่าวที่ไม่เป็นจริง ไม่ถูกต้อง ไม่ใช่ข้อมูลล่าสุด หรือไม่สมบูรณ์ หรือหากผู้ดูแลมีเหตุผลในการสงสัยว่าข้อมูลดังกล่าวที่ไม่เป็นจริง ไม่ถูกต้อง ไม่ใช่ข้อมูลล่าสุด หรือไม่สมบูรณ์ ศูนย์เทคโนโลยีสารสนเทศมีสิทธิที่จะระงับการให้บริการแก่บัญชีผู้ใช้งาน (Username) โดยไม่ต้องบอกกล่าว

๑๐.๓ ในการลงทะเบียนผู้ใช้งานสำหรับหน่วยงาน ผู้ใช้งานต้องกำหนดชื่อบุคคล และที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (e-mail address) ของผู้รับผิดชอบ โดยผู้ใช้งานต้องลงทะเบียนด้วยตัวเองผ่านช่องทางที่ศูนย์เทคโนโลยีสารสนเทศเปิดให้และตกลงที่จะให้ข้อมูลที่เป็นจริง ถูกต้อง ครบถ้วน

๑๐.๔ ผู้ใช้งานต้องรับผิดชอบในการรักษาความลับของรหัสผ่าน (Password) และบัญชีชื่อผู้ใช้งาน (Username) และรับผิดชอบในกิจกรรมทั้งหมดที่เกิดขึ้นภายใต้บัญชีชื่อผู้ใช้งาน (Username)

๑๐.๕ ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ทุกครั้งก่อนที่จะใช้ระบบจดหมายอิเล็กทรอนิกส์ และหากพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านหรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๑๐.๖ ผู้ใช้งานจะต้องลงทะเบียนขอใช้งานระบบจดหมายอิเล็กทรอนิกส์ โดยหน้าลงทะเบียนจะปรากฏให้เห็นเฉพาะการใช้งานจากเครือข่ายภายในกรมเท่านั้น โดยผู้ใช้งานจะต้องให้ข้อมูลที่เป็นความจริง ถูกต้อง และครบถ้วน โดยชื่อผู้ใช้งานจะมีรูปแบบ คือ ชื่อจริงภาษาอังกฤษตามด้วยเครื่องหมายมหัพภาค “.” และตามด้วยนามสกุลภาษาอังกฤษ ๓ ตัวอักษรแรก ทั้งนี้หากชื่อผู้ใช้งานไม่เป็นไปตามรูปแบบดังกล่าวจะไม่ได้รับการอนุมัติการละทะเบียนเพื่อนใช้งานระบบจดหมายอิเล็กทรอนิกส์

๑๐.๗ หลังจากลงทะเบียนแล้วจะใช้เวลาตรวจสอบและรอการอนุมัติจากผู้ดูแลระบบ (System Administrator) โดยใช้เวลาไม่เกิน ๗ วัน ซึ่งผู้ใช้งานสามารถตรวจสอบกรอนุมัติการใช้งานได้จากหน้าเว็บไซต์อินทราเน็ต

๑๐.๘ หากผู้ใช้งานพบปัญหาในการลงทะเบียน หรือไม่ได้รับการอนุมัติการลงทะเบียนขอให้ติดต่อสอบถามจากผู้ดูแลระบบทันที

๑๐.๙ หลังจากได้รับการอนุมัติการลงทะเบียนแล้ว ผู้ใช้งานสามารถเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์ได้ทันทีโดยใช้ชื่อผู้ใช้งานตามที่ผู้ใช้งานได้ลงทะเบียนไว้ในระบบ

ข้อ ๑๑ การเปลี่ยนแปลงและยกเลิกบริการระบบจดหมายอิเล็กทรอนิกส์ของกรม

๑๑.๑ ศูนย์เทคโนโลยีสารสนเทศขอสงวนสิทธิการพิจารณาแก้ไขเปลี่ยนแปลงข้อตกลงและเงื่อนไขการใช้บริการนี้ได้ตามความเหมาะสม และให้ถือว่าผู้ใช้งานที่ยังคงใช้บริการต่อไปตกลงยอมรับที่จะปฏิบัติตามระเบียบกฎเกณฑ์และเงื่อนไขที่แก้ไขเปลี่ยนแปลงนั้นโดยปริยาย

๑๑.๒ ศูนย์เทคโนโลยีสารสนเทศขอสงวนสิทธิในการเปลี่ยนแปลง ปรับปรุง แก้ไข และระงับบริการไว้ชั่วคราวหรือถาวรได้ตลอดเวลา โดยไม่ต้องบอกกล่าวให้ทราบ

๑๑.๓ ศูนย์เทคโนโลยีสารสนเทศมีสิทธิยกเลิก หรือระงับให้บริการไว้ชั่วคราวหรือถาวรหากผู้ใช้งานฝ่าฝืนหรือพยายามฝ่าฝืนข้อตกลงหรือเงื่อนไขนี้ข้อหนึ่งข้อใด

๑๑.๔ ศูนย์เทคโนโลยีสารสนเทศมีสิทธิลบจดหมายอิเล็กทรอนิกส์ทั้งหมดที่มีอยู่ในบัญชีชื่อผู้ใช้งาน (Username) ออกและปิดการรับจดหมายอิเล็กทรอนิกส์จากบุคคลอื่นที่อาจส่งถึงผู้ใช้งาน หากผู้ใช้งานไม่ได้เข้ามาใช้งานจดหมายอิเล็กทรอนิกส์ของผู้ใช้งานผ่านบริการเป็นเวลา ๓๐ วัน แต่ชื่อบัญชีผู้ใช้งาน (Username) จะยังคงอยู่ โดยผู้ใช้งานกลับสู่สภาวะเดิม (Re-activate) ได้ โดยการกลับเข้ามาใช้บริการอีกครั้ง

๑๑.๕ ศูนย์เทคโนโลยีสารสนเทศสามารถยกเลิกบริการ และลบข้อมูลเนื้อหาในบริการได้ทันที โดยไม่ต้องแจ้งให้ทราบล่วงหน้า หากผู้ใช้งานไม่เข้ามาใช้งานจดหมายอิเล็กทรอนิกส์เป็นเวลาเกินกว่า ๙๐ วัน

๑๑.๖ กรณีผู้ใช้งานลาออก เสียชีวิต หรือถูกไล่ออก ถือว่าหมดสมาชิกภาพ โดย ศูนย์เทคโนโลยีสารสนเทศสงวนสิทธิจะทำการยุติการใช้งานจดหมายอิเล็กทรอนิกส์นั้นโดยไม่ต้องบอกกล่าว

ส่วนที่ ๕
นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต
(Internet Security Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต(Internet) อย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบสารสนเทศแก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบสารสนเทศของบุคคลอื่นโดยปกติสุข ทำให้ระบบสารสนเทศขององค์กรถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. แนวทางปฏิบัติ

ข้อ ๑ จะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายก่อน

ข้อ ๒ ผู้ใช้งานต้องใช้ข้อความที่สุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้งานเครือข่ายเท่านั้น

ข้อ ๓ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๔ ห้ามมิให้ผู้ใช้งานอินเทอร์เน็ตในระหว่างเวลาทำงานเพื่อการรับส่งข้อมูลหรือการใช้งานแฟ้มข้อมูลร่วมกัน (Shared File) หรือที่มิได้เกี่ยวข้องกับการทำงาน เช่น ข้อมูลหนัง ข้อมูลเพลง ข้อมูลเกมส์ เว็บบล็อก เป็นต้น

ข้อ ๕ บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับการใช้งานระบบอินเทอร์เน็ต ให้สิทธิเป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน จำหน่าย หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

ข้อ ๖ ผู้ใช้งานต้องรับผิดชอบในการจัดเก็บและรักษาบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองให้เป็นความลับ และไม่สามารถปฏิเสธความรับผิดชอบได้หากมีผู้อื่นล่วงรู้ข้อมูลและนำไปใช้งานในทางที่ผิด ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีชื่อผู้ใช้งาน (Username) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

ข้อ ๗ ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่นกล่าวคือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีชื่อผู้ใช้งาน (Username) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ของหน่วยงานในหน่วยงาน หรือหน่วยงานอื่นๆ การเผยแพร่ข้อความใดๆ ที่ก่อนให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว หน่วยงานไม่มีส่วนรับผิดชอบความเสียหายดังกล่าว

ข้อ ๘ ห้ามมิให้ผู้ใช้งานปฏิบัติการใดๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของหน่วยงาน

ข้อ ๙ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๑๐ ระมัดระวังการดาวน์โหลด (Download) และการอัพเดท (Update) โปรแกรม ใช้งานจากระบบอินเทอร์เน็ต (Internet) และโปรแกรมต่างๆ โดยจะต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๑๑ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๑๒ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ ๑๓ หลังจากเลิกใช้งานระบบต่างๆ ที่มีการลงบันทึกเข้า (Login) ให้ทำตามขั้นตอนลงบันทึกออก (Logout) ทุกครั้งเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อ ๑๔ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์ทุกครั้งเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อ ๑๕ ข้อกำหนดและเงื่อนไขการใช้บริการระบบอินทราเน็ตของกรมการขนส่งทางบก

๑๕.๑ ศูนย์เทคโนโลยีสารสนเทศกรมการขนส่งทางบก เป็นผู้ควบคุมดูแลระบบอินทราเน็ตของกรมที่ให้บริการแก่ผู้ใช้งาน ภายใต้ข้อกำหนดและเงื่อนไขต่างๆ ที่สามารถปรับปรุงให้ทันสมัยโดยไม่ต้องแจ้งให้ทราบล่วงหน้า ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดและเงื่อนไขตลอดระยะเวลาที่ใช้บริการอย่างเคร่งครัด

๑๕.๒ เพื่อความปลอดภัยในข้อมูลส่วนบุคคลของผู้ใช้งานและผู้ใช้งานรายอื่น และเพื่อความเป็นระเบียบเรียบร้อยในการใช้บริการ ผู้ใช้งานต้องไม่กระทำการใดอันเป็นการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ การล่วงละเมิดสิทธิส่วนบุคคลหรือสิทธิอื่นใดของบุคคลอื่น และ/หรือสิทธิในทรัพย์สินทางปัญญาของหน่วยงานหรือของบุคคลอื่น รวมทั้งต้องไม่กระทำการใดอันขัดต่อข้อตกลงและเงื่อนไขนี้ ศูนย์เทคโนโลยีสารสนเทศสามารถที่จะลบ ทำให้หยุดชั่วคราว หรือถาวร หรือนำเสนอ และตรวจสอบข้อมูลส่วนบุคคลของผู้ใช้งานตลอดเวลาตามความต้องการของกฎหมาย หรือเพื่อปกป้องและป้องกันสิทธิ ทรัพย์สิน หรือผลประโยชน์ของกรมและบุคคลภายนอก หรือเพื่อวัตถุประสงค์อื่นใดก็ตาม โดยไม่ต้องบอกกล่าวล่วงหน้า

๑๕.๓ การให้บริการระบบอินทราเน็ตกรม มีวัตถุประสงค์เพื่อใช้ในการติดต่อสื่อสารที่เกี่ยวข้องกับการปฏิบัติราชการเท่านั้น ผู้ใช้งานได้ตกลงยินยอมว่าผู้ใช้งานจะเป็นผู้รับผิดชอบในข้อมูล เนื้อหา ข้อความ รูปภาพ หรือข้อมูลอื่นๆ ทั้งหมดแต่ผู้เดียว (ต่อไปนี้จะเรียกว่า “เนื้อหา”) ซึ่งผู้ใช้งานได้ส่งเข้ามาไม่ว่าโดยวิธีใดก็ตาม เนื้อหาทั้งหมดที่ถูกส่งมาจะอยู่ในความรับผิดชอบของบุคคลนั้น และผู้ใช้งานตกลงยินยอมที่จะไม่กระทำการดังต่อไปนี้

(๑) ส่งเนื้อหาผ่านบริการโดยผิดกฎหมายหรือศีลธรรม หมิ่นประมาท กล่าวโทษ ขู่เข็ญ คุกคาม สร้างความเสียหาย ลามก หยาบโลนหรือเป็นที่น่ารังเกียจของผู้อื่น

(๒) ส่งเนื้อหาใดใดที่เป็นการละเมิดทรัพย์สินทางปัญญา หรือสิทธิอื่นของบุคคลหรือสถาบันอื่นรวมทั้งเครื่องหมายการค้า ลิขสิทธิ์ หรือสิทธิในการเผยแพร่ต่างๆ

(๓) พยายามฝ่าฝืนเข้าสู่บริการของบัญชีผู้อื่น ระบบสารสนเทศหรือเครือข่ายบริการ โดยมิได้รับอนุญาต หรือ รบกวนการใช้งานของผู้ใช้งานอื่น

๑๕.๔ ผู้ใช้งานต้องเป็นบุคลากรของกรมการขนส่งทางบกเท่านั้น

๑๕.๕ ศูนย์เทคโนโลยีสารสนเทศอาจเข้าถึงหรือเปิดเผยข้อมูลการสื่อสารของผู้ใช้งานเพื่อปฏิบัติตามกฎหมาย หรือตอบสนองต่อการเรียกร้องที่ชอบด้วยกฎหมายหรือกระบวนการทางกฎหมาย หรือเพื่อปกป้องสิทธิหรือทรัพย์สินของหน่วยงานหรือของผู้ใช้งานอื่น

๑๕.๖ ศูนย์เทคโนโลยีสารสนเทศอาจยุติการให้บริการชั่วคราว เพื่อเพิ่มระบบรักษาความปลอดภัยหรือหยุดยั้งการก่อกวนระบบการให้บริการ

๑๕.๗ ศูนย์เทคโนโลยีสารสนเทศจะไม่รับประกันความเสียหายหรือสูญหายของข้อมูลที่เก็บไว้ในระบบ

๑๕.๘ หากเกิดความเสียหายขึ้นเนื่องจากการใช้บริการ หรือจากการละเมิดระเบียบกฎเกณฑ์และเงื่อนไขนี้ไม่ว่าโดยบุคคลใด การเขียนและเผยแพร่ข้อความที่ต้องห้าม กรมไม่ต้องรับผิดชอบใดๆ ทั้งสิ้นต่อผู้ใช้งาน และ/หรือบุคคลผู้เสียหายนั้น ผู้ใช้งานต้องรับผิดชอบและรับผลเสียหายที่เกิดขึ้นนั้นแต่เพียงผู้เดียว ทั้งนี้ ผู้ใช้งานตกลงสละสิทธิเรียกร้องให้กรมรับผิดในความสูญหายและเสียหายใดๆ ที่เกิดขึ้นจากการใช้บริการนี้ทั้งสิ้น นอกจากนี้ ผู้ใช้งานต้องปกป้องมิให้กรมการขนส่งทางบกต้องรับผิดหรือถูกฟ้องร้องจากบุคคลอื่นอันเนื่องมากจากบริการนี้ รวมทั้งจะต้องรับผิดชอบและชดใช้ค่าเสียหายต่างๆ ที่เกิดขึ้นเองทั้งสิ้น

ข้อ ๑๖ การเปลี่ยนแปลงและการยกเลิกบริการระบบอินทราเน็ตของกรม

๑๖.๑ ศูนย์เทคโนโลยีสารสนเทศขอสงวนสิทธิในการพิจารณา แก้ไข เปลี่ยนแปลงข้อตกลงและเงื่อนไขการใช้บริการนี้ได้ตามความเหมาะสม และให้ถือว่าผู้ใช้งานที่ยังคงใช้บริการต่อไปตกลงยอมรับที่จะปฏิบัติตามกฎเกณฑ์และเงื่อนไขที่แก้ไขเปลี่ยนแปลงนั้นโดยปริยาย

๑๖.๒ ศูนย์เทคโนโลยีสารสนเทศขอสงวนสิทธิในการเปลี่ยนแปลง ปรับปรุง แก้ไข และระงับบริการไว้ชั่วคราวหรือถาวรได้ตลอดเวลา โดยไม่ต้องบอกกล่าวให้ทราบ

๑๖.๓ ศูนย์เทคโนโลยีสารสนเทศมีสิทธิยกเลิก หรือระงับการให้บริการไว้ชั่วคราวหรือถาวร หากผู้ใช้งานฝ่าฝืนหรือพยายามฝ่าฝืนข้อตกลงหรือเงื่อนไงข้อหนึ่งข้อใด

๑๖.๔ ศูนย์เทคโนโลยีสารสนเทศสามารถยกเลิกบริการ และลบข้อมูลเนื้อหาของผู้ใช้งานได้ทันที โดยไม่ต้องแจ้งให้ทราบล่วงหน้า หากผู้ใช้งานละเมิดระเบียบกฎเกณฑ์และเงื่อนไขการให้บริการ

๑๖.๕ กรณีผู้ใช้งานลาออก เสียชีวิต หรือถูกไล่ออก ถือว่าสิ้นสุดการเป็นสมาชิกภาพศูนย์เทคโนโลยีสารสนเทศขอสงวนสิทธิในการหยุดการใช้งานอินทราเน็ตของผู้ใช้งานนั้นโดยไม่ต้องแจ้งให้ทราบ

ส่วนที่ ๖

นโยบายความมั่นคงปลอดภัยของการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

(Access control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศและระบบเครือข่ายของกรม และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ยืนยันตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของกรมได้อย่างถูกต้อง โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย ผู้ใช้งานสามารถทำความเข้าใจและปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๒. แนวนโยบาย

ข้อ ๑. ผู้ที่เข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากผู้บังคับบัญชากรม หรือผู้ที่ได้รับมอบหมายในการอนุญาต เป็นลายลักษณ์อักษรเท่านั้น

ข้อ ๒. มีการจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่างๆของผู้ใช้งานตั้งแต่เริ่มเข้าใช้งานจนสิ้นสุดการใช้งานเพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

ข้อ ๓. มีการกำหนดสิทธิการใช้งานและการเข้าถึงตามระดับความสำคัญของผู้ใช้งานซึ่งเห็นชอบโดยผู้บริหารของหน่วยงาน

ข้อ ๔. มีการกำหนดสิทธิในการเข้าใช้งานแก่ผู้ใช้งานให้ตรงตามหน้าที่ความรับผิดชอบ โดยสามารถตรวจสอบสิทธิได้ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

ข้อ ๕. การเข้าถึงระบบด้วยการ Remote User ต้องได้รับการอนุญาตและสิทธิการเข้าใช้งานระบบจากเจ้าหน้าที่ที่ควบคุมดูแลของศูนย์เทคโนโลยีสารสนเทศกรมการขนส่งทางบกเท่านั้น

ข้อ ๖. ผู้ดูแลระบบสามารถควบคุมหรือตัดสิทธิการใช้งานของผู้ใช้งานได้ตามความเหมาะสม หากผู้ใช้งานกระทำการใดๆในทางที่ผิดตามประกาศของกรมการขนส่งทางบก

ข้อ ๗. มีการควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

ข้อ ๘. ผู้ใช้งานที่ผ่านการตรวจสอบสิทธิทุกคนจะต้องทราบถึงข้อตกลงในการใช้งานระบบสารสนเทศนั้นๆด้วย

ข้อ ๙. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สินการจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

ข้อ ๑๐. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

๑๐.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ

๑๐.๒ กำหนดเกณฑ์การระงับสิทธิมอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

๑๐.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓. แนวทางปฏิบัติ

หมวด ๑ การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

ข้อ ๑ กรมการขนส่งทางบกกำหนดมาตรการควบคุมการเข้าใช้งาน ระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของกรมการขนส่งทางบก จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บังคับบัญชากรมการขนส่งทางบก หรือผู้ที่ได้รับมอบหมายให้มีอำนาจในการอนุญาตบุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน ให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูงหรือผู้อำนวยการแล้วแต่กรณี เพื่อให้ความเห็นชอบและอนุญาตก่อน โดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิตามอนุญาตนั้น

ข้อ ๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

ข้อ ๔ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๕ บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศและการสื่อสารของกรมการขนส่งทางบก จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้มีอำนาจในการอนุมติ โดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิตามอนุญาตนั้น ดังนี้

๕.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

๕.๒ กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

ข้อ ๖ หน่วยงานที่ทำงานให้กับกรมทุกหน่วยงานที่ต้องการเชื่อมต่อจากภายนอก ต้องแจ้งต่อศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร เพื่อขออนุมัติก่อนดำเนินการเชื่อมต่อ

ข้อ ๗ กำหนดมาตรฐานในการเข้าใช้ข้อมูล หรือการเชื่อมโยงข้อมูลของหน่วยงานภาครัฐและภาคเอกชนที่ต้องการข้อมูลจากกรมการขนส่งทางบก

ข้อ ๘ ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศ และปฏิบัติงานตามผู้อำนวยการมอบหมาย ดังนี้

๘.๑ อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของหน่วยงานจะกระทำได้ต่อเมื่อได้รับอนุญาตจากผู้อำนวยการเท่านั้น

๘.๒ กำหนดสิทธิของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิการเข้าถึงนั้นอย่างสม่ำเสมอ

๘.๓ จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

๘.๔ ติดตั้งระบบการบันทึกและติดตามการใช้งานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศของหน่วยงานอย่างสม่ำเสมอ

ข้อ ๙ การจัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลระดับชั้น การเข้าถึง เวลาเข้าถึงและช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจน โดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยกำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญ ไว้ดังนี้

๙.๑ การจัดประเภทของข้อมูล แบ่งออกเป็น ๓ ประเภท คือ

๙.๑.๑ ข้อมูลสารสนเทศด้านการบริหาร

- นโยบาย
- ข้อมูลยุทธศาสตร์
- ข้อมูลบุคลากร
- ข้อมูลงบประมาณ การเงินและบัญชี
- ข้อมูลสถิติเชิงวิเคราะห์

๙.๑.๒ ข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน

- ข้อมูลการดำเนินงานตามภารกิจองค์กร
- ข้อมูลติดตามการดำเนินงานตามภารกิจองค์กร
- ข้อมูลกฎ ระเบียบ กฎหมาย
- ข้อมูลการติดต่อสื่อสารภายในองค์กร
- ข้อมูลติดตามการใช้จ่ายงบประมาณ
- ข้อมูลรายงานผลการปฏิบัติงาน

๙.๑.๓ ข้อมูลสารสนเทศด้านการบริการ

๙.๒ การแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภทประเภทผู้เกี่ยวข้องที่สามารถเข้าถึงข้อมูล ได้แก่

๙.๒.๑ ระดับชั้นสำหรับผู้บริหาร คือระดับชั้นการเข้าถึงที่อนุญาตให้ผู้บริหาร หรือผู้ที่ได้รับมอบหมายเข้าถึงข้อมูลสารสนเทศด้านการบริหาร ด้านการจัดการและปฏิบัติงาน และด้านการให้บริการ โดยจะได้รับสิทธิตามความจำเป็นต่อการปฏิบัติหน้าที่ของผู้เข้าถึงในระดับนี้เท่านั้น ระดับชั้นสำหรับผู้บริหารทั่วไป หมายถึง ผู้อำนวยการสำนักฯ ผู้อำนวยการกลุ่ม

๙.๒.๒ ระดับชั้นสำหรับผู้ใช้งานทั่วไป คือระดับชั้นการเข้าถึงที่อนุญาตให้พนักงาน หรือเจ้าหน้าที่ที่ได้รับมอบหมายเข้าถึงข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน และด้านการให้บริการ โดยจะได้รับสิทธิตามความจำเป็นต่อการปฏิบัติหน้าที่ของผู้เข้าถึงในระดับนี้เท่านั้น

๙.๒.๓ ระดับชั้นสำหรับผู้ดูและระบบหรือผู้ที่ได้รับมอบหมาย คือ ระดับชั้นการเข้าถึงที่อนุญาตให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย เข้าถึงข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน และด้านการให้บริการ โดยจะได้รับสิทธิตามความจำเป็นต่อการดูแลระบบ หรือปฏิบัติหน้าที่ของผู้เข้าถึงในระดับนี้เท่านั้น

๙.๓ ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๑๗ ซึ่งกำหนดชั้นความลับของข้อมูลเป็น ๔ ระดับ ได้แก่

๙.๓.๑ ลับที่สุด ได้แก่ ข้อมูลที่มีความสำคัญที่สุดเกี่ยวกับข่าวสาร วัตถุ หรือบุคคล ซึ่งถ้าหากข้อมูลดังกล่าวทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคลผู้ไม่มีหน้าที่ได้รับทราบจะทำให้เกิดความเสียหายหรือเป็นภยันตรายต่อความมั่นคงปลอดภัยของสาธารณชน หรือความสงบเรียบร้อยของประเทศชาติ หรือต่อธุรกิจหรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้อง อย่างร้ายแรงที่สุด

๙.๓.๒ ลับมาก ได้แก่ ข้อมูลที่มีความสำคัญมากเกี่ยวกับข่าวสาร วัตถุ หรือบุคคล ซึ่งถ้าหากข้อมูลดังกล่าวทั้งหมด หรือเพียงบางส่วนรั่วไหลไปถึงบุคคลที่ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายเป็นภยันตรายต่อความมั่นคงปลอดภัยของสาธารณชน หรือความสงบเรียบร้อยของประเทศชาติ หรือต่อธุรกิจหรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้อง อย่างร้ายแรง

๙.๓.๓ ลับ ได้แก่ ข้อมูลที่มีความสำคัญเกี่ยวกับข่าวสาร วัตถุ หรือบุคคล ซึ่งถ้าหากข้อมูลดังกล่าวทั้งหมด หรือเพียงบางส่วนรั่วไหลไปถึงบุคคลที่ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายต่อธุรกิจหรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้อง

๙.๓.๔ ปกปิด ได้แก่ ข้อมูลซึ่งไม่พึงเปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบ โดยสงวนไว้ให้ทราบเฉพาะบุคคลที่มีหน้าที่ต้องทราบเพื่อประโยชน์ในการปฏิบัติภารกิจขององค์กรเท่านั้น

๙.๓.๕ ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๙.๔ การกำหนดช่องทางการเข้าถึง ผู้ใช้งานที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดไว้นั้นจะต้องได้รับสิทธิจากหน่วยงานโดยมีการกำหนดบัญชีผู้ใช้งานตามระดับการเข้าถึงให้สามารถเข้าใช้งานตามประเภทความรับผิดชอบ สิทธิในการเข้าถึงข้อมูล และสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้นโดยมีช่องทางการเข้าถึง ดังนี้

- ระบบเครือข่ายภายใน (Intranet)
- ระบบเครือข่ายอินเทอร์เน็ต (Internet)
- ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)
- เว็บไซต์ (Website)
- ระบบเครือข่าย LAN
- ระบบเครือข่ายไร้สาย (Wireless LAN)
- การประชุมทางไกล (Video Conference)
- โทรศัพท์หรือโทรสาร

๙.๕ การกำหนดเวลาที่สามารถเข้าถึงได้

- การเข้าถึงสารสนเทศในเวลาราชการ (๐๗.๓๐ – ๑๖.๓๐ น.)
- การเข้าถึงสารสนเทศนอกเวลาราชการ (๑๖.๓๐ – ๑๘.๓๐ น.)
- การเข้าถึงสารสนเทศในช่วงวันที่มิได้ทำการ (วันหยุดราชการ และ วันหยุดนักขัตฤกษ์)

- การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง ต้องระบุช่วงเวลาหรือจำนวนระยะเวลาเข้าถึง

(๑) ๑ – ๓ วัน

(๒) ๑ สัปดาห์

(๓) ๑ เดือน

(๔) ตามเวลาที่ร้องขอ

๙.๖ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

๙.๖.๑ ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบ

๙.๖.๒ กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้งานข้อมูลในแต่ละชั้นความลับ

๙.๖.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๙.๖.๔ การกำหนดให้เปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดความสำคัญของข้อมูลแต่ละระดับ

๙.๖.๕ การรับ-ส่งข้อมูลระหว่างต้นทางและปลายทางของกรมผ่านระบบเครือข่ายต้องเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล โดยการรับ-ส่งข้อมูลของกรม ประกอบด้วย ๓ ประเภทได้แก่

(๑) การรับ-ส่งข้อมูลระหว่างส่วนกลางและสำนักงานขนส่งจังหวัดทั่วประเทศ เป็นการรับ-ส่งข้อมูลโดยใช้เทคโนโลยี MPLS (Multi Protocol Switching)

(๒) การรับ-ส่งข้อมูล กรณีออกหน่วยเคลื่อนที่ด้วย SSL VPN ผู้ใช้งานสามารถติดต่อเข้าใช้งานแอปพลิเคชั่นภายในเครือข่ายของกรม โดยใช้ Secure Remote Access และควบคุมความปลอดภัยด้วยบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบ

(๓) การรับ-ส่งข้อมูลระหว่างส่วนกลาง และศูนย์สำรองข้อมูลด้วยเทคโนโลยี SD-WAN

๙.๖.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ของทางราชการออกนอกหน่วยงาน รวมถึงการบำรุงรักษา การตรวจสอบซ่อมแซมให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๙.๖.๗ การกำหนดระยะเวลาการเชื่อมต่อ (Limitation of connection time) สำหรับการใช้งานระบบสารสนเทศบางระบบให้เป็นไปตามช่วงเวลาการทำงานที่หน่วยงานกำหนด ส่วนระบบสารสนเทศที่มีความสำคัญสูงให้ทำการตัดระบบและหมดเวลาการใช้งานรวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีการใช้งานภายในช่วงระยะเวลา ๑๕ นาที

๙.๗ การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงาน ดังนี้

๙.๗.๑ มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน ดังนี้

- ระบบรักษาความปลอดภัย (Security)
- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศและควบคุมความชื้น

๙.๗.๒ ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าทำงานได้ปกติและลดความเสี่ยงจากความล้มเหลวในการทำงาน

๙.๗.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (Data Center) เมื่อมีการทำงานเครื่องผิดปกติหรือหยุดการทำงาน

๙.๗.๔ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอกและให้แยกอุปกรณ์ที่มีความสำคัญเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

๙.๗.๕ ตรวจสอบ ดูแลสภาพแวดล้อมภายในห้องและตรวจสอบระดับอุณหภูมิความชื้นให้อยู่ระดับปกติ เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ภายในห้องศูนย์ข้อมูล (Data Center)

๙.๗.๖ การเดินสายไฟ สายสัญญาณเครือข่ายของหน่วยงานและสายเคเบิ้ลอื่น ที่จำเป็นต้องทำการวางผ่านเข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้นั้น ให้ร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันสัตว์หรือแมลงเข้าทำรังรบกวน หรือกัดแทะทำความเสียหายต่อสายไฟ ป้องกันการดักจับสัญญาณ การตัดสายสัญญาณ อันจะทำให้เกิดความเสียหายต่อระบบเครือข่ายใช้งานไม่ได้

๙.๗.๗ ต้องจัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนถูกต้อง โดยสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน แล้วให้จัดเก็บสายสัญญาณต่างๆ ไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิทเพื่อป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง

๙.๘ จัดทำโครงการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และระบบสารสนเทศ ดังนี้

๙.๘.๑ กำหนดการบำรุงรักษาอุปกรณ์แต่ละประเภทตามรอบระยะเวลาการใช้งานไว้ในแผนการบำรุงรักษาประจำปี

๙.๘.๒ บันทึกรายละเอียดการให้บริการบำรุงรักษาอุปกรณ์ทุกครั้งผ่านระบบ Support Desk และต้องบันทึกรายละเอียดข้อบกพร่องของอุปกรณ์ที่ตรวจพบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ในภายหลัง

๙.๘.๓ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้รับจ้างให้เป็นไปตามขอบเขตและข้อกำหนดของสัญญา

๙.๙ การควบคุมการนำสินทรัพย์ของหน่วยงานออกนอกพื้นที่ ดังนี้

๙.๙.๑ บันทึกและจัดเก็บข้อมูลสินทรัพย์ของหน่วยงานที่นำออกนอกพื้นที่ เพื่อเป็นหลักฐาน ป้องกันการสูญหาย รวมทั้งบันทึกการส่งคืน

๙.๙.๒ ห้ามผู้ใช้งานละทิ้งสินทรัพย์ของหน่วยงานไว้เพียงลำพังในที่สาธารณะ โดยให้ถือเสมือนเป็นทรัพย์สินของตนเอง

๙.๙.๓ กรณีจำเป็นต้องจำหน่ายสินทรัพย์ของหน่วยงาน ให้ลบหรือทำลายข้อมูลสำคัญหรือสื่อบันทึกข้อมูลก่อนที่จะจำหน่ายอุปกรณ์นั้น

๙.๑๐ กำหนดเงื่อนไขในการระงับหรือยกเลิกสิทธิของผู้ใช้งานในการใช้งานระบบสารสนเทศในแต่ละประเภทของข้อมูล

๙.๑๑ ผู้ดูแลระบบต้องมีการทบทวนและปรับปรุงสิทธิให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัยของกรม

หมวด ๒ การบริหารจัดการการเข้าถึงระบบสารสนเทศ

๑. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

แนวนโยบาย

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตจากกรมการขนส่งทางบก และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต จะต้องประกอบด้วย

(๑) การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (user access) ประกอบด้วย

(๑.๑) มีการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

(๑.๒) ให้ความรู้ความเข้าใจกับผู้ใช้งานเพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การอนุญาตให้เข้าถึงระบบสารสนเทศหลัก

(๒.๑) ผู้ดูแลระบบสารสนเทศของหน่วยงาน (Administrator) ไม่เกินหน่วยงานละ ๓ คน และสำนักงานขนส่งกรุงเทพมหานครพื้นที่ ๕ สำนักบริหารการคลังและรายได้ สำนักงานขนส่งผู้โดยสาร สำนักการขนส่งสินค้า และสำนักงานขนส่งในส่วนภูมิภาคต้องกำหนดเจ้าหน้าที่เป็นผู้ดูแลและแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบเป็นหนังสือ เพื่อเพิ่มเติมการเข้าถึงโปรแกรมกำหนดสิทธิการเข้าใช้งานระบบสารสนเทศให้กับผู้ใช้งานระบบของหน่วยงาน

(๒.๒) ผู้ดูแลระบบสารสนเทศของหน่วยงานมีหน้าที่กำหนดสิทธิการเข้าใช้งานระบบสารสนเทศให้กับเจ้าหน้าที่ผู้ใช้งานระบบของหน่วยงาน โดยต้องกำหนดสิทธิในการเข้าถึงให้ตรงตามหน้าที่ความรับผิดชอบของผู้ใช้งานระบบที่ได้รับมอบหมายจากผู้บังคับบัญชา สำหรับหน่วยงานที่ไม่มีผู้ดูแลระบบกรณีต้องการเข้าใช้งานระบบสารสนเทศต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบเป็นหนังสือ

(๒.๓) หน่วยงานด้านทะเบียนรถที่ต้องการดำเนินการใดๆ กับข้อมูลทะเบียนรถที่ไม่เปิดเผยเป็นการทั่วไป ได้แก่ ข้อมูลทะเบียนรถของสำนักพระราชวัง ข้อมูลทะเบียนรถอำพราง ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบเป็นหนังสือ

(๓) การลงทะเบียนผู้ใช้งาน (user registration) ประกอบด้วย

(๓.๑) ต้องกำหนดขั้นตอนการลงทะเบียนผู้ใช้งานระบบตามความเหมาะสมในแต่ละระบบงานที่ได้รับอยู่ในความรับผิดชอบของกรมการขนส่งทางบก

(๓.๒) ต้องจัดทำบัญชีผู้ใช้งานระบบอย่างน้อยต้องประกอบด้วย

- รายชื่อผู้ขออนุญาตเข้าใช้งานระบบ
- รายชื่อผู้ได้รับการอนุมัติเข้าใช้งานระบบ
- กำหนดสิทธิการเข้าใช้งานข้อมูล
- ผู้อนุมัติหรือผู้ดูแลระบบที่ได้รับมอบหมาย
- การยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานระบบ

(๓.๓) ต้องกำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๓.๔) ต้องกำหนดหลักเกณฑ์ในการยกเลิกหรือเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการลาออกเปลี่ยนตำแหน่งโอนย้ายหรือสิ้นสุดการจ้าง เป็นต้น

(๓.๕) ต้องตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าทีและความรับผิดชอบหรือความต้องการของกรม

(๔) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ประกอบด้วย

(๔.๑) มีการแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ซึ่งหมายรวมถึงสิทธิจำเพาะสิทธิพิเศษและสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงข้อมูลสารสนเทศ

(๔.๒) การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูลผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

(๔.๓) ผู้ใช้มีสิทธิเข้าใช้งานผ่านระบบเครือข่ายระบบงานและระบบปฏิบัติการตามที่ผู้ดูแลระบบกำหนด

(๔.๔) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

(๕) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ประกอบด้วย

(๕.๑) มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานให้มีความมั่นคงปลอดภัยอย่างรัดกุม

(๕.๒) มีการกำหนดให้เครื่องแม่ข่ายต้องกำหนดรหัสผ่านของผู้ดูแลระบบของแต่ละระบบโดยเฉพาะและให้ทราบรหัสผ่านเฉพาะผู้เกี่ยวข้องเท่านั้นและไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน

(๕.๓) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๕.๔) ผู้ใช้งานระบบควรทำการแจ้งผู้ดูแลระบบหากต้องการทำกิจกรรมที่อาจมีผลกระทบต่อความปลอดภัยของระบบ และผู้ใช้งานระบบควรจะแจ้งผู้ดูแลระบบความปลอดภัยของระบบทันทีถ้าหากสงสัยว่าได้กระทำกิจกรรมที่มีผลต่อความปลอดภัยของระบบ

(๕.๕) การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูลหรือระบบเครือข่ายผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

(๕.๖) มีการตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคล ผ่าน Proxy เป็นต้น

(๕.๗) กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบ เป็นเวลาอย่างน้อย ๓ เดือน หรือตามที่หน่วยงานกำหนด

(๖) การทบทวนสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน (review of user access rights) ประกอบด้วย

(๖.๑) สิทธิการเข้าถึงข้อมูลของผู้ใช้งานต้องได้รับการพิจารณาทบทวนอย่างสม่ำเสมอโดยผู้ดูแลระบบอย่างน้อยปีละ ๑ ครั้งและทุกครั้งที่มีการปรับเปลี่ยน เช่น การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ การยกเลิกการจ้าง หรือการเกษียณอายุราชการ เป็นต้น

(๖.๒) สิทธิการเข้าถึงข้อมูลควรได้รับการทบทวนและจัดสรรใหม่เมื่อมีการโยกย้ายบุคลากรภายในหน่วยงาน

(๖.๓) การกำหนดสิทธิพิเศษควรได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดเพื่อมั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

(๖.๔) การเปลี่ยนแปลงของผู้ใช้งานที่ได้รับสิทธิพิเศษควรถูกบันทึกเพื่อการทบทวน

(๖.๕) สิทธิในระดับผู้ดูแลระบบต้องทบทวนสิทธิสำหรับผู้มีสิทธิในระดับสูง อย่างน้อยปีละ ๑ ครั้ง

แนวทางปฏิบัติ

(๑) การลงทะเบียนผู้ใช้งาน (user registration) มีดังนี้

(๑.๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ สำหรับระบบสารสนเทศขององค์กร

(๑.๒) ให้ผู้ใช้งานกรอกข้อมูลการขอใช้ระบบงานสารสนเทศลงในแบบฟอร์มลงทะเบียนและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งานระบบ

(๑.๓) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายพิจารณาคำขอลงทะเบียน อนุมัติกำหนดระดับการเข้าใช้งานสารสนเทศเท่าที่จำเป็นในแต่ละระบบงานตามหน้าที่ความรับผิดชอบ และทำการบันทึกจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศทุกครั้ง

(๑.๔) ระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคลและไม่ซ้ำซ้อนกัน

(๑.๕) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุลหากซ้ำให้เพิ่มอักษรตัวที่สองหรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๑.๖) กำหนดบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและกำหนดสิทธิการใช้งานระบบเท่าที่จำเป็นในแต่ละระบบงาน

(๑.๗) ต้องตรวจสอบและมอบหมายสิทธิที่เหมาะสมต่อหน้าที่ความรับผิดชอบหรือความต้องการของศูนย์เทคโนโลยีสารสนเทศให้ผู้มีส่วนเกี่ยวข้องกับระบบงาน

(๑.๘) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนามรับทราบด้วย

(๑.๙) ผู้ดูแลระบบจัดทำการบันทึกการเปลี่ยนแปลงบัญชีผู้ใช้งานแต่ละรายในระบบเมื่อได้รับรายงานบัญชีรายชื่อผู้ใช้งานได้ถูกเพิกถอนสิทธิ หรือลาออก หรือเปลี่ยนแปลงตำแหน่งหรือย้ายหน่วยงาน

(๑.๑๐) ปฏิเสธการเข้าสู่ระบบ หากผู้ใช้งานใส่รหัสเข้าระบบผิดต่อเนื่อง ๓ ครั้ง และให้แจ้งความจำนงพร้อมหลักฐานแสดงความเป็นตัวตนต่อศูนย์เทคโนโลยีสารสนเทศ เพื่อขอรับรหัสผ่านใหม่

(๑.๑๑) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๒) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ โดยผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการดังนี้

(๒.๑) ผู้ดูแลระบบแสดงกระบวนการในการมอบหมายหรือการกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒.๒) ผู้ดูแลระบบสามารถบันทึกการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศตามที่ได้รับอนุมัติหรือตามอำนาจหน้าที่ความรับผิดชอบหรือตามความจำเป็นในการใช้งานระบบเท่านั้น

(๒.๓) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศมอบอำนาจหน้าที่ความรับผิดชอบให้ผู้ดูแลระบบหรือมอบหมายสิทธิการบริหารจัดการบัญชีผู้ใช้งานให้ผู้อื่นที่มีส่วนเกี่ยวข้องกับระบบงานดำเนินการแทนก็ได้

(๒.๔) บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งานระบบ

(๒.๕) บันทึกและจัดเก็บข้อมูลการเปลี่ยนแปลงบัญชีผู้ใช้งานการมอบหมายอำนาจหน้าที่หรือสิทธิการควบคุมการใช้งานทุกครั้ง

(๒.๖) ทำการทบทวนระดับและสิทธิของผู้ใช้งานระบบสารสนเทศอย่างสม่ำเสมอ

(๒.๗) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

(๓) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) มีดังนี้

(๓.๑) การกำหนดรหัสผ่านควรมีความยาวมากกว่า หรือเท่ากับ ๖ ตัวอักษร (โดยมีการผสมผสานตัวอักษรระหว่างตัวอักษรตัวปกติตัวพิมพ์ใหญ่ตัวเลขและสัญลักษณ์เข้าด้วยกัน) และเป็นไปตามระเบียบกรมการขนส่งทางบก ว่าด้วยการใช้งานระบบสารสนเทศ ปี ๒๕๖๐

(๓.๒) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ นามสกุล เบอร์โทรศัพท์ของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตนหรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๓.๓) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(๓.๔) การตั้งรหัสผ่านชั่วคราวต้องยากต่อการเดาและต้องมีความแตกต่างกัน

(๓.๕) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัยโดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่านและผู้ใช้งานควรตอบกลับทันทีหลังจากได้รับรหัสผ่าน

(๓.๖) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราวและควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๓.๗) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๓.๘) ในกรณีระบบงานใดอนุญาตให้เปลี่ยนรหัสผ่านควรเปลี่ยนรหัสผ่านใหม่ทันทีสำหรับการเข้าใช้งานครั้งแรก

(๓.๙) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๓.๑๐) ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

(๓.๑๑) ไม่อนุญาตให้เจ้าหน้าที่หรือผู้ใช้งานระบบใช้รหัสผ่านร่วมกัน

(๓.๑๒) ภายหลังการใช้งานเครื่องแม่ข่ายเสร็จสิ้นจะต้องทำการ log off ทุกครั้ง

(๓.๑๓) กรณีผู้ใช้งานระบบลืมรหัสผ่าน (Password) หรือไม่ได้ใช้รหัสผู้ใช้ (User-ID) และรหัสผ่าน (Password) เป็นเวลา ๒๑๐ วัน ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบกทราบเป็นหนังสือ เพื่อดำเนินการกำหนดรหัสผ่าน (Password) ใหม่

(๓.๑๔) จัดทำขั้นตอนการปฏิบัติสำหรับการตั้งหรือการเปลี่ยนรหัสผ่านให้ผู้ใช้งานทราบ

(๔) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) มีดังนี้

(๔.๑) การทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ

(๔.๒) ปรับปรุงบัญชีผู้ใช้งานและบันทึกการเปลี่ยนแปลงสิทธิบัญชีผู้ใช้งาน

(๔.๓) การทบทวนสิทธิการเข้าใช้งานในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาโดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(๔.๔) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้งหรือเมื่อมีการเปลี่ยนแปลง เช่นมีการลาออก เปลี่ยนตำแหน่ง โอนย้ายหรือสิ้นสุดการจ้าง

๒. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

แนวนโยบาย

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ โดยได้กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานทุกคนในกรมการขนส่งทางบกและผู้ดูแลระบบครอบคลุมเรื่องต่างๆดังนี้

(๑) ต้องกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password) สำหรับผู้ใช้งานเพื่อให้สามารถกำหนดรหัสผ่านการใช้งานรหัสผ่านและการเปลี่ยนหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์เพื่อกำหนดแนวทางในการป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงระบบและอุปกรณ์ต่างๆ ของหน่วยงานในขณะที่ไม่มีผู้ดูแลควรมี ดังนี้

(๒.๑) มีมาตรการป้องกันดูแลอุปกรณ์ที่ไม่มีผู้ใช้งานหรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๒.๒) สร้างความตระหนักและเอาใจใส่ต่อการป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงานตลอดเวลาเพื่อไม่ให้เกิดความเสียหายหรือสูญหาย หรือมีผู้ไม่ประสงค์ดีเข้าถึงระบบและอุปกรณ์ต่างๆ โดยไม่ได้รับอนุญาต

(๒.๓) ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบสารสนเทศเสร็จสิ้นจะต้องทำการ log off ทุกครั้งเสมอ

(๒.๔) ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๒.๕) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่มีการดูแลชั่วคราว

(๒.๖) ผู้บริหารมอบหมายหน่วยงานผู้รับผิดชอบหรือแต่งตั้งผู้มีส่วนเกี่ยวข้องในการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานไม่ให้เกิดความเสียหายหรือสูญหายหรือถูกบุกรุกข้อมูลสารสนเทศ

(๓) การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบสารสนเทศ (Clear desk and Clear screen Policy) ควรมีดังนี้

(๓.๑) มีมาตรการการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานเพื่อไม่ให้เกิดความเสียหายหรือสูญหาย หรือถูกบุกรุกข้อมูลสารสนเทศจากผู้ไม่มีส่วนเกี่ยวข้อง

(๓.๒) หน่วยงานผู้รับผิดชอบจะต้องจัดหาสถานที่ที่ใช้ในการจัดเก็บเอกสารสื่อบันทึกข้อมูลเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆที่เกี่ยวข้องให้มีความเหมาะสมไม่ให้ได้รับความเสี่ยง

(๓.๓) ผู้ที่ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์หรือระบบเครือข่ายหรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงานเท่านั้น

(๓.๔) บุคลากรของกรมการขนส่งทางบกทุกคนอนุญาตให้เข้าใช้พื้นที่และอุปกรณ์ต่างๆได้ตามสิทธิที่หน่วยงานกำหนดเท่านั้น

(๓.๕) ต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่างๆตามลำดับความสำคัญ

(๓.๖) ต้องบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(๓.๗) ต้องจัดเก็บบันทึกเหตุการณ์การเข้า-ออกพื้นที่ของศูนย์เทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

(๓.๘) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่างๆของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งานเพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(๓.๙) บุคคลภายนอกหรือเจ้าหน้าที่บริษัทที่เกี่ยวข้องกับโครงการต่างๆของกรมการขนส่งทางบกจะต้องขออนุญาตเพื่อเข้าใช้พื้นที่และใช้อุปกรณ์ต่างๆของ ศูนย์เทคโนโลยีสารสนเทศ และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารด้าน IT หรือผู้ที่ได้รับมอบอำนาจก่อนเข้าพื้นที่เท่านั้น

(๓.๑๐) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่ายเช่นชื่อผู้ใช้งานและรหัสผ่าน

(๓.๑๑) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่ายเช่นตรวจสอบไวรัสการยืนยันตัวบุคคลผ่าน Proxy อย่างสม่ำเสมอ

(๔) ข้อมูลสารสนเทศใดที่เป็นความลับผู้ดูแลระบบอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

(๕) กำหนดให้ต้องบันทึกการทำงานของระบบสารสนเทศ บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย ๓ เดือนหรือตามที่หน่วยงานกำหนด

แนวทางปฏิบัติ

(๑) วิธีการปฏิบัติการใช้งานรหัสผ่าน (Password use) มีข้อปฏิบัติดังนี้

(๑.๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๑.๒) กำหนดรหัสผ่านต้องมีความยาวมากกว่าหรือเท่ากับ ๖ ตัวอักษร (โดยต้องผสมผสานตัวอักษรระหว่างตัวอักษรตัวปกติตัวพิมพ์ใหญ่ตัวเลขและสัญลักษณ์เข้าด้วยกัน)

(๑.๓) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่ายเช่นชื่อสกุลเบอร์โทรศัพท์ของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตนหรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๑.๔) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกันหรือกลุ่มเหมือนกัน

(๑.๕) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(๑.๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๑.๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๑.๘) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑.๙) ต้องเปลี่ยนรหัสผ่านอย่างสม่ำเสมอทุก ๖ เดือนหรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้ และจะกำหนดรหัสผ่านซ้ำกับที่เคยกำหนดมาแล้วภายใน ๖ เดือนไม่ได้

(๑.๑๐) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันหรือรหัสผ่านเดิมสำหรับระบบงานอื่นๆที่ตนใช้งาน

(๑.๑๑) กรณีผู้ใช้งานระบบลืมรหัสผ่าน (Password) หรือไม่ได้ใช้รหัสผู้ใช้ (User-ID) และรหัสผ่าน (Password) เป็นเวลา ๒๑๐ วัน ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบกทราบเป็นหนังสือ เพื่อดำเนินการกำหนดรหัสผ่าน (Password) ใหม่

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์มีข้อปฏิบัติดังนี้

(๒.๑) ผู้ดูแลระบบหรือผู้รับผิดชอบกำหนดข้อปฏิบัติในการป้องกันอุปกรณ์ระบบคอมพิวเตอร์และระบบสารสนเทศที่ใช้งานเพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒.๒) กำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งานอยู่ เพื่อป้องกันการสูญหายหรือเข้าถึงโดยไม่ได้รับอนุญาต ดังนี้

- ต้องกำหนดรหัสผ่านก่อนเข้าใช้งานเครื่องคอมพิวเตอร์
- ดาวน์โหลดไฟล์จากแหล่งข้อมูลอินเทอร์เน็ตที่ไว้ใจได้เท่านั้น

(๒.๓) สร้างให้ทุกคนต้องตระหนักและเอาใจใส่ต่อการป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงานตลอดเวลาเพื่อไม่ให้เกิดความเสียหายหรือสูญหายหรือมีผู้ไม่พึงประสงค์เข้าถึงระบบและอุปกรณ์ต่างๆโดยไม่ได้รับอนุญาต

(๒.๔) เจ้าพนักงานเครื่องคอมพิวเตอร์หรือผู้รับผิดชอบจะต้องมีมาตรการป้องกันระบบสารสนเทศและอุปกรณ์ที่ไม่มีผู้ใช้งานหรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๒.๕) ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบสารสนเทศเสร็จสิ้นจะต้องทำการ log off ทุกครั้ง

(๒.๖) ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา ๑๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๒.๗) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

(๓) การควบคุมทรัพย์สินและการใช้งานระบบ (Clear desk and Clear screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศที่เป็นเอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๓.๑) ผู้ที่ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์หรือระบบเครือข่ายหรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงานเท่านั้น

(๓.๒) บุคลากรของกรมการขนส่งทางบกทุกคนอนุญาตให้เข้าใช้พื้นที่และอุปกรณ์ต่างๆ ได้ตามสิทธิที่หน่วยงานกำหนดเท่านั้น

(๓.๓) บุคลากรจะต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่างๆตามลำดับความสำคัญ

(๓.๔) กำหนดมาตรการป้องกันสินทรัพย์ของหน่วยงาน และควบคุมไม่ให้ทิ้งหรือปล่อยระบบสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องการจัดบริเวณล้อมรอบ การควบคุมการเข้า-ออก การจัดบริเวณการเข้าถึง การวางอุปกรณ์ ระบบและอุปกรณ์สนับสนุนการทำงาน ดังนี้

- ตระหนักเรื่องความปลอดภัยและการปฏิบัติการใดๆ เพื่อป้องกันสินทรัพย์ของหน่วยงาน
- ลงชื่อออกจากระบบและล็อคเครื่องคอมพิวเตอร์ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ปิดเครื่องโทรสารเมื่อไม่ใช้งาน และป้องกันไม่ให้ผู้อื่นใช้กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร
- ป้องกันเครื่องคอมพิวเตอร์โดยใช้กลไกการพิสูจน์ตัวตนก่อนการใช้งาน
- ไม่ควรเสียบสายไฟค้างไว้ที่เต้าเสียบ อาจจะทำให้เกิดฟ้าผ่าเข้าเครื่องหรือกระแสไฟฟ้าไหลเข้าเครื่องได้

(๓.๕) ต้องบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(๓.๖) ต้องจัดเก็บบันทึกเหตุการณ์การเข้า-ออกพื้นที่ของศูนย์เทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

(๓.๗) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่างๆของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งานเพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(๓.๘) บุคคลภายนอกหรือเจ้าหน้าที่บริษัทที่เกี่ยวข้องกับโครงการต่างๆของกรมการขนส่งทางบกจะต้องขออนุญาตเพื่อเข้าใช้พื้นที่และใช้อุปกรณ์ต่างๆ ของศูนย์เทคโนโลยีสารสนเทศและต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายอำนาจก่อนเข้าพื้นที่ศูนย์เทคโนโลยีสารสนเทศเท่านั้น

(๓.๙) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่ายเช่นหมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

(๓.๑๐) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่ายเช่นตรวจสอบไวรัสการยืนยันตัวบุคคลผ่าน Proxy อย่างสม่ำเสมอ

(๓.๑๑) ผู้ดูแลระบบหรือผู้รับผิดชอบจัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งระบุผู้รับผิดชอบเมื่อต้องให้บริการระบบเครือข่ายคอมพิวเตอร์

(๓.๑๒) ผู้ใช้งานระบบและเครื่องคอมพิวเตอร์ต้องลงทะเบียนการใช้งานทุกครั้งเพื่อเป็นการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบทุกครั้ง

(๓.๑๓) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศต้องกำหนดมาตรการการป้องกันดังนี้

- ให้ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- ต้องลงชื่อออกจากระบบทันทีเมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ต้องจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- Log off เครื่องคอมพิวเตอร์หรือล็อคหน้าจอทุกครั้งเมื่อไม่ได้ใช้งาน
- ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(๓.๑๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการพ.ศ. ๒๕๔๔ โดยผู้ใช้งานต้องทำการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากลเมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

(๓.๑๕) การกระทำใด ๆ ที่เกิดจากการใช้บัญชีผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประกอบพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ผู้ใช้งานจะรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

(๓.๑๖) ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกเครื่องมีหน้าที่ต้องสำรองข้อมูลสำคัญจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ ได้แก่ CD,DVD หรือฮาร์ดดิสก์แบบติดตั้งภายนอก

(๓.๑๗) ผู้ใช้งานมีหน้าที่เก็บสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓.๑๘) คัดเลือกเอกสารที่พ้นระยะเวลาเก็บรักษา หรือไม่มีความจำเป็นต้องใช้งาน ทั้งเอกสารและสื่อบันทึกข้อมูลอื่น เสนอผู้บริหารหน่วยงานเพื่อทำลายเอกสารและสื่อบันทึกข้อมูลดังกล่าวตามรูปแบบเหมาะสม เช่น การเข้าเครื่องทำลายเอกสาร การทุบ บดให้เสียหาย เป็นต้น และเป็นไปตามหลักเกณฑ์ว่าด้วยการบริหารและจัดการสินทรัพย์

๓. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

แนวนโยบาย

เพื่อป้องกันการเข้าถึงระบบเครือข่ายกรมการขนส่งทางบกโดยไม่ได้รับอนุญาต ประกอบด้วย

(๑) การกำหนดขอบเขตและสิทธิของผู้ใช้งานสามารถเข้าถึงบริการต่างๆในระบบเครือข่ายของหน่วยงานกำหนดเท่านั้น

(๒) การกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) มีการทบทวนสิทธิการเข้าถึงบริการระบบเครือข่ายอย่างน้อยปีละ ๑ ครั้งและต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานผู้รับผิดชอบเท่านั้น

(๔) มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีกระบวนการในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้

(๕) มีวิธีการระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) เพื่อใช้ในการตรวจสอบการเข้าถึงอุปกรณ์บนระบบเครือข่ายของหน่วยงาน

(๖) มีการกำหนดหลักเกณฑ์ในการควบคุมและการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๗) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่ายและการตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๘) ทำการแบ่งแยกเครือข่าย (segregation in networks) สำหรับกลุ่มผู้ใช้งาน

(๙) มีการควบคุมการเชื่อมโยงเครือข่าย (network connection control) ของหน่วยงานที่มีการใช้ร่วมกันหรือเชื่อมโยงระหว่างกันให้มีความสอดคล้องกับหน่วยงาน

(๑๐) มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย

(๑๑) มีการกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก (remote access) เพื่อรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายของหน่วยงาน

แนวทางปฏิบัติ

(๑) ผู้ดูแลระบบเครือข่ายจัดทำบันทึกการกำหนดขอบเขตและสิทธิของผู้ใช้งานที่สามารถเข้าถึงบริการต่างๆในระบบเครือข่ายของหน่วยงานตามที่กำหนดเท่านั้น

(๒) ผู้ดูแลระบบเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

(๔) การเข้าใช้งานระบบสารสนเทศที่สำคัญตามข้อปฏิบัติที่หน่วยงานกำหนดขึ้น ได้แก่ ระบบงานโปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

(๕) การเข้าสู่ระบบเครือข่ายภายในของกรม โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายสื่อสารก่อนที่จะสามารถใช้งานได้ในทุกกรณี

(๖) ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีกระบวนการในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้ ดังนี้

(๖.๑) ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ทุกครั้ง

(๖.๒) การอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ในการเข้าใช้งานต้องขึ้นอยู่กับความจำเป็นของการดำเนินงานและด้านเทคนิครวมทั้งต้องได้รับความเห็นชอบจากผู้บังคับบัญชา

(๖.๓) หากหน่วยงานหรือผู้ปฏิบัติงานที่มีความประสงค์ขอใช้ชื่อผู้ใช้งานจะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและศูนย์เทคโนโลยีสารสนเทศก่อนโดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

(๗) ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

(๘) ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรมีการบันทึกและแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๙) ระบบเครือข่ายทั้งหมดของกรมที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกกรม ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering การใช้ Firewall หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

(๑๐) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกรมในลักษณะที่ผิดปกติผ่านระบบเครือข่าย ต้องตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๑๑) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ และต้องสามารถตรวจสอบ IP Address ของต้นทางและปลายทางได้

(๑๒) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๑๓) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการภายใต้การควบคุมโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ เท่านั้น

(๑๔) การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึงดังนี้

(๑๔.๑) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศก่อนจึงจะสามารถดำเนินการได้

(๑๔.๒) ผู้ดูแลระบบเครือข่ายมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามที่ศูนย์เทคโนโลยีสารสนเทศกำหนดและสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

(๑๔.๓) จะต้องมีการจำกัดสิทธิการเข้าใช้อุปกรณ์ได้โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

(๑๕) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่ายดังนี้

(๑๕.๑) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทั้งทางกายภาพและโดยการล๊อกอินเข้ามาใช้งาน

(๑๕.๒) ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการกำหนดค่า (Configuration) ไว้ในห้องคอมพิวเตอร์แม่ข่ายที่มีระบบควบคุมการเข้าออกเพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(๑๕.๓) ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

(๑๕.๔) เปิดพอร์ตที่มีความจำเป็นในการใช้งานและยกเลิกหรือปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๑๕.๕) ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมออย่างน้อยเดือนละ ๑ ครั้ง

(๑๕.๖) กำหนดสิทธิบุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

(๑๕.๗) บันทึกการเข้า-ออกพื้นที่บริเวณห้องคอมพิวเตอร์แม่ข่ายกลางได้แก่เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้องและเจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

(๑๕.๘) ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่ายหากจำเป็นให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป

(๑๕.๙) ติดตั้งเครื่องควบคุมบันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางที่ประตูเข้าออกและติดตั้งกล้องโทรทัศน์วงจรปิดกันการโจรกรรม

(๑๖) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่ายและการตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๑๗) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

(๑๘) การแบ่งแยกเครือข่าย (segregation in network) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศ ดังต่อไปนี้

(๑๘.๑) ระบบเครือข่ายอินเทอร์เน็ต (Internet) เพื่อควบคุมการเข้าถึงระบบเครือข่ายจากบุคคลภายนอกโดยไม่ได้รับอนุญาต

(๑๘.๒) ระบบเครือข่ายภายใน (Intranet) ผู้ใช้งานสามารถใช้งานผ่านสายสัญญาณเครือข่าย (LAN) ผ่านจุดเชื่อมต่อ (Outlets) และระบบเครือข่ายไร้สาย (Wireless LAN) ภายในหน่วยงานเท่านั้น

(๑๘.๓) DMZ (Demilitarized Zone) เป็นเขตพิเศษที่เชื่อมต่อทั้งเครือข่ายภายใน (Intranet) และเครือข่ายภายนอก (Internet) สำหรับแยกเครื่องแม่ข่ายที่ให้บริการทั้งบนเครือข่ายภายนอกและเครือข่ายภายใน เพื่อป้องกันการเข้าถึงระบบเครือข่ายภายในหน่วยงานโดยไม่ได้รับอนุญาต

(๑๙) มีการควบคุมการเชื่อมโยงเครือข่าย (network connection control) ศูนย์เทคโนโลยีสารสนเทศต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมโยงระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติอย่างน้อยดังนี้

(๑๙.๑) การจำกัดสิทธิการเข้าถึงเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตน

(๑๙.๒) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๑๙.๓) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

(๑๙.๔) การเข้าใช้งานเชื่อมต่อเครือข่ายต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

(๑๙.๕) ควบคุมไม่ให้เปิดเผยข้อมูลระบบเครือข่ายที่สำคัญในการเชื่อมต่อเข้าสู่ระบบ ได้แก่ หมายเลข IP Address Username และ Password เป็นต้น

(๑๙.๖) ผู้ใช้งานห้ามนำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

(๒๐) มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผยดังนี้

(๒๐.๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) ของหน่วยงาน

(๒๐.๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย (Network Address Translation) เพื่อแยกระบบเครือข่ายย่อย

(๒๐.๓) กำหนดมาตรการบังคับใช้เส้นทางเครือข่ายหรือจำกัดสิทธิในการใช้บริการเครือข่ายของหน่วยงาน

(๒๑) ผู้ดูแลระบบเครือข่ายกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก (remote access) เพื่อรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายของหน่วยงานที่ต้องผ่านการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานและต้องได้รับอนุญาตจากหน่วยงานหรือผู้ดูแลระบบ โดยต้องระบุเหตุผลหรือความจำเป็นในการดำเนินงานอย่างเพียงพอเป็นลายลักษณ์อักษรและได้รับกาอนุมัติจากผู้ที่มีอำนาจอย่างเป็นทางการเท่านั้น และผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดของหน่วยงานอย่างเคร่งครัดโดยดำเนินการ ดังนี้

(๒๑.๑) การควบคุมบุคคลที่เข้าสู่ระบบของกรมจากระยะไกล ต้องกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน โดยต้องกระทำผ่าน VPN เท่านั้น

(๒๑.๒) ผู้ดูแลระบบเครือข่ายต้องไม่เปิด port และ modem ทิ้งเอาไว้โดยไม่จำเป็น

(๒๑.๓) ปิดช่องทางการเชื่อมต่อเมื่อไม่ใช้งานแล้วและเปิดใช้งานเมื่อมีการร้องขอเท่าที่จำเป็นเท่านั้น

(๒๑.๔) มีการควบคุมพอร์ต (port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมตามความเหมาะสม

(๒๑.๕) วิธีการใดๆก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากภายนอก (remote access) ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

(๒๒) การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก จะต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร โดยต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้มีอำนาจในการอนุมัติ และปฏิบัติตามวิธีการที่กรมกำหนด อย่างน้อย ๑ วิธี ดังนี้

(๒๒.๑) การใช้งานคอมพิวเตอร์และคอมพิวเตอร์พกพาทั้งที่เป็นทรัพย์สินของกรม ส่วนตัว หรือของบุคคลภายนอกต้องทำการพิสูจน์ตนผ่านระบบ MAC Authentication ของกรม และแสดงตัวตนโดยป้อนชื่อผู้ใช้ (Username) และการพิสูจน์ยืนยันตัวตน (Authentication) ป้อนรหัสผ่าน (Password) ก่อนใช้งานทุกครั้ง

(๒๒.๒) การติดต่อเข้าใช้งานระบบต่างๆ ของกรมผ่านระบบอินเทอร์เน็ต (Internet) จากภายนอก ต้องทำการเชื่อมต่อผ่านระบบ SSL VPN ของกรม และป้อน Username และ Password ก่อนใช้งานทุกครั้ง

(๒๒.๓) ระบบ GFMIS ให้ใช้ GFMIS Token Key เสียบที่เครื่องที่ต้องการจะใช้งาน และกรอกข้อมูลผู้ใช้งานตามที่กรมบัญชีกลางกำหนด และเมื่อปฏิบัติตามขั้นตอนต่างๆ และได้รับอนุญาตจากระบบของกรมบัญชีกลาง จึงจะสามารถใช้งานได้ โดยเข้าเว็บไซต์ https://webonlineinter.gfmis.go.th โดยระบุดังนี้ Username : AAAAAAAAAA+๑๐ A คือ รหัสหน่วยเบิกจ่ายจำนวน ๑๐ หลัก ๑๐ คือ ค่าคงที่ Password : รหัสเดิมที่หน่วยงานใช้บันทึกข้อมูลผ่านอินเทอร์เน็ต และต้องมีการลงไดรเวอร์ เครื่องที่ต้องการใช้งานด้วย

(๒๓) ผู้ใช้งานต้องไม่กระทำการใดอันเป็นการล่วงละเมิดสิทธิส่วนบุคคลหรือสิทธิอื่นใดของบุคคลอื่น และ/หรือสิทธิในทรัพย์สินทางปัญญาของหน่วยงานหรือของบุคคลอื่น โดยอาศัยระบบเครือข่ายสื่อสารของกรม รวมทั้งต้องไม่กระทำการอันใดขัดต่อข้อตกลงและเงื่อนไขที่ศูนย์เทคโนโลยีสารสนเทศ และกรมกำหนด

(๒๔) ศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบกอาจเข้าถึงหรือเปิดเผยข้อมูลผู้ใช้งาน เพื่อปฏิบัติตามกฎหมาย หรือกระบวนการทางกฎหมาย หรือเพื่อปกป้องสิทธิหรือทรัพย์สินของหน่วยงานหรือของผู้ใช้งานบริการอื่น

(๒๕) ศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบกอาจยุติการให้บริการชั่วคราว เพื่อเพิ่มระบบรักษาความปลอดภัยหรือหยุดยั้งการก่อกวนระบบเครือข่ายสื่อสารของกรม

(๒๖) กรมไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย ได้แก่ การประกาศแจ้งความ การซื้อ หรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

(๒๗) ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าบัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว กรมไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

แนวนโยบาย

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาตควรดำเนินการดังนี้

(๑) การกำหนดขั้นตอนการเข้าถึงระบบปฏิบัติการจะต้องมีการควบคุมโดยการยืนยันตัวตนตามระบบรักษาความมั่นคงปลอดภัยของหน่วยงาน

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งานสามารถตรวจสอบได้

(๓) การระบุและยืนยันตัวตนของผู้ใช้งานสามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติมได้แก่ Token key Hand Scan หรือ finger print เป็นต้นตามความเหมาะสมของแต่ละระบบงานของหน่วยงานได้

(๔) การบริหารจัดการรหัสผ่าน (password management system) มีการแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะอัตโนมัติเพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพเมื่อได้ดำเนินการติดตั้งระบบแล้วให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(๕) มีการจำกัดการใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญเพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้

(๖) มีการกำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (session time-out) เมื่อว่างเว้นจากการใช้งานตามความเหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๗) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) สำหรับระบบสารสนเทศหรือแอปพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

แนวทางปฏิบัติ

(๑) ผู้ดูแลระบบ (system administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (domain controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

(๒) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยการเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้

(๒.๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒.๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๒.๓) จำกัดการป้อนรหัสผ่านในกรณีป้อนรหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๒.๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

(๓) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) กำหนดให้ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งานสามารถตรวจสอบได้ดังนี้

(๓.๑) ผู้ใช้งานต้องระบุชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(๓.๒) การอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นของหน่วยงานทางด้านธุรกิจหรือด้านเทคนิค

(๓.๓) สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key Hand Scan หรือ finger print เป็นต้น ตามความเหมาะสมของแต่ละระบบงานของหน่วยงานได้

(๔) การบริหารจัดการรหัสผ่าน (password management system) ต้องแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะเชิงโต้ตอบ (interactive) หรือต้องทำงานในลักษณะอัตโนมัติเพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพเมื่อได้ดำเนินการติดตั้งระบบแล้วให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(๕) ต้องจำกัดการใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญเพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้ให้ดำเนินการดังนี้

(๕.๑) ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาตและยังไม่ผ่านการตรวจสอบ

(๕.๒) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อหน่วยงาน

(๕.๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ

(๕.๔) ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕.๕) กำหนดให้ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) การใช้งานโปรแกรมอรรถประโยชน์ (Utilities Program) เพื่อการบำรุงรักษาเครื่องคอมพิวเตอร์ที่ติดตั้งอยู่ในระบบสารสนเทศอย่างสม่ำเสมอ ผู้ใช้งานต้องหมั่นใช้โปรแกรม Scandisk เพื่อทำการตรวจสอบการทำงานของหน่วยสำรองข้อมูล ฮาร์ดดิสก์ และ Floppy Disk ว่าส่วนไหนไม่สามารถบันทึกได้ รวมถึงตรวจสอบโครงสร้างของแฟ้มข้อมูลให้มีความถูกต้อง หากพบปัญหาก็จะทำการแก้ไขให้โดยอัตโนมัติ

(๖.๑) Disk defragmenter โปรแกรมช่วยจัดระเบียบข้อมูลในดิสก์

(๖.๒) Disk cleanup โปรแกรมกำจัดข้อมูลที่ซ้ำซ้อนหรือไม่ได้ใช้งานในระบบ

(๗) มีการกำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (session time-out) เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๑๕ นาทีเป็นอย่างน้อยหากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๐ นาทีตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๘) ถ้าไม่มีการใช้งานระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๙) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

(๑๐) กำหนดระยะเวลาในการจำกัดการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูงเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา ๒ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง

๕. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

แนวนโยบาย

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศดำเนินการ ดังนี้

(๑) กำหนดมาตรการการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

(๒) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชั่นโดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๓) ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงต่อหน่วยงานจะได้รับการแยกจากระบบอื่นๆและมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะได้แก่ระบบคลังข้อมูลเศรษฐกิจการคลัง

(๔) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

แนวทางปฏิบัติ

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องดำเนินการดังนี้

(๑.๑) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งานพร้อมทั้งกำหนดสิทธิตามอำนาจหน้าที่ที่ควรได้รับ และต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอำนาจหน้าที่ของผู้ใช้งาน

(๑.๒) ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา ๑๕ นาทีต้องทำการยุติการใช้งานทันที

(๑.๓) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

• กำหนดสิทธิให้กับผู้เข้าใช้งานระบบโดยการกำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลในแต่ละระดับชั้น

• การรับ-ส่งข้อมูลใช้เทคโนโลยี MPLS สำหรับการเข้าใช้ระบบงานภายในที่ตั้ง และเมื่อต้องมีการใช้เครือข่ายสาธารณะเพื่อเข้าถึงระบบงานของกรมต้องมีการเข้ารหัสอย่างปลอดภัย

• การนำอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงานกรณีข้อมูลที่เป็นความลับของหน่วยงานต้องมีการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล

(๑.๔) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใดๆจะต้องได้รับสิทธิและอนุญาตในการเข้าดำเนินการและจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้วผู้ดูแลระบบจะต้องยกเลิกสิทธิที่ให้กับหน่วยงานนั้นๆซึ่งหากหน่วยงานภายนอกดำเนินการใดๆที่มีผลกระทบต่อระบบจะต้องเป็นผู้รับผิดชอบ

(๒) ระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

(๒.๑) การแยกระบบสารสนเทศที่มีความสำคัญสูงและจำเป็นต้องได้รับการดูแลเป็นพิเศษศูนย์เทคโนโลยีสารสนเทศต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ ให้ทำงานอยู่บนเครื่องเซิร์ฟเวอร์หรือคอมพิวเตอร์ไม่ใช้ปะปนกับระบบอื่นเพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องเดียวกันซึ่งจำเป็นต้องติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายกลางที่มีสภาพแวดล้อมเหมาะสม

(๒.๒) ให้มีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะได้แก่ห้องคอมพิวเตอร์แม่ข่ายกลาง ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่ายกลางและอื่นๆ เป็นต้นเพื่อป้องกันการหยุดชะงักการทำงานของระบบ

(๒.๓) ควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกกำหนดสิทธิการเข้าใช้งานโดยกำหนดค่าที่ Firewall

(๒.๔) มีการควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

(๓) การใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

(๓.๑) ต้องตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๓.๒) ต้องระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจกคอมพิวเตอร์ที่นำไปใช้ได้ ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบ

(๓.๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบ

(๓.๔) เจ้าหน้าที่ที่รับผิดชอบในการรับคืนต้องตรวจสภาพความพร้อมใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่รับคืนก่อนเสมอ

(๓.๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

(๔.๑) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอกรวมถึงการเตรียมการระบบสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

(๔.๒) ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆภายในสำนักงานก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าถึง

(๔.๓) ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงานไม่อนุญาตให้ครอบครัวหรือบุคคลอื่นใดเข้าถึงระบบสารสนเทศของสำนักงาน

(๔.๔) การขออนุมัติหรือยกเลิกการปฏิบัติงานจากระยะไกลการกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงานต้องปฏิบัติตามการควบคุมการเข้าถึงเครือข่าย

(๕) การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)

(๕.๑) ต้องมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ

(๕.๒) ต้องมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน

(๕.๓) เจ้าหน้าที่พัฒนาซอฟต์แวร์ของหน่วยงานภายนอกทุกคน ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ตามรูปแบบที่กรมกำหนด

(๕.๔) จัดให้มีคณะกรรมการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๕.๕) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด (Source Code) ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๕.๖) พิจารณากำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการจากภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๕.๗) ต้องมีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่างๆ ที่จะทำให้การติดตั้งก่อนดำเนินการติดตั้ง

(๕.๘) หลังการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอกหน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่างๆ

๖. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

แนวนโยบาย

หน่วยงานต้องมีการกำหนดมาตรการในการควบคุมและป้องกันการรักษาความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) และหลักเกณฑ์การนำอุปกรณ์สื่อสารเคลื่อนที่เข้ามาใช้งานในระบบเครือข่ายไร้สายเพื่อป้องกันและรักษาความปลอดภัยของข้อมูลสารสนเทศของหน่วยงาน

แนวทางปฏิบัติ

(๑) การใช้งานเครือข่ายไร้สาย (Wireless Policy)

(๑.๑) ไม่อนุญาตให้ผู้ใช้งานเปิด ad-hoc หรือ peer-to-peer network

(๑.๒) การเข้าใช้ wireless จะต้องเข้าใช้ผ่าน username และ password ที่หน่วยงานกำหนด

(๑.๓) เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้

(๑.๔) ห้ามมิให้ผู้ใดนำอุปกรณ์ wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็นอุปกรณ์กระจายสัญญาณ (access point), wireless routers, wireless USB client, หรือ wireless card ภายในหน่วยงาน ยกเว้นจะได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้รับผิดชอบของหน่วยงาน

(๒) การใช้งานระบบไฟร์วอลล์ (Firewall) และระบบตรวจจับและป้องกันการบุกรุก(IDS/IPS

(๒.๑) มีการระบุขอบเขต (Trust Zones) ของเครือข่ายเช่นเครือข่าย Internet, web servers, โซนการเชื่อมต่อภายนอกเครือข่ายภายในองค์กรและโซน remote access และออกแบบการควบคุมการจราจรด้วยระบบ firewall ในแต่ละโซน

(๒.๒) มีการระบุการควบคุมระบบไฟร์วอลล์ ในรูปแบบของเอกสารเพื่อใช้ในกรณีที่มีการเปลี่ยนแปลงหรือเคลื่อนย้ายระบบ

(๒.๓) มีการจัดเก็บ Log file และการจราจรของเครือข่ายเป็นประจำและสม่ำเสมอ

(๒.๔) มีการตรวจจับเหตุการณ์ต่างๆที่เกิดขึ้นใน Host หรือเครือข่ายข้อมูล

(๓) การใช้งานเครือข่าย (Internet Security Policy)

(๓.๑) มีการตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่ายเช่นหมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

(๓.๒) มีการตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่างๆตามลำดับความสำคัญ

(๓.๓) มีการบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(๓.๔) มีการจัดเก็บบันทึกเหตุการณ์การเข้าถึงของระบบอย่างสม่ำเสมอ

(๓.๕) จัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งผู้รับผิดชอบเมื่อมีการให้บริการระบบเครือข่ายคอมพิวเตอร์

(๔) การเชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่างๆกับเครือข่าย

(๔.๑) ผู้ใช้ต้องไม่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่างๆกับเครือข่ายอื่นนอกเหนือจากเครือข่ายขององค์กรการติดต่อกับหน่วยงานภายนอกต้องผ่านระบบ Proxy Firewall ขององค์กรก่อน

(๔.๒) ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายขององค์กรต้องได้รับอนุญาตจากผู้ดูแลระบบ

(๕) ผู้ดูแลระบบ (system administrator) ต้องดำเนินการดังต่อไปนี้

(๕.๑) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๕.๒) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๕.๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๕.๔) ควรทำการเปลี่ยนค่า SSID (service set identifier) ที่ถูกกำหนดเป็นค่าDefault มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน

๗. การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ (Outsource Access Control)

แนวนโยบาย

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบสารสนเทศของหน่วยงานให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอกควรประกอบด้วย

(๑) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของหน่วยงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรโดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบสารสนเทศเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย

(๒) หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในหน่วยงานหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงานโดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

(๓) สำหรับงานลักษณะโครงการผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของหน่วยงานให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้านคือการรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล(Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(๔) ผู้ให้บริการหน่วยงานภายนอกต้องจัดทำแผนการดำเนินงานคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวดและให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

แนวทางปฏิบัติ

(๑) ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศขององค์กร

(๒) หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศขององค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๓) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบสารสนเทศซึ่งต้องมีรายละเอียดดังนี้

(๓.๑) เหตุผลในการขอใช้

(๓.๒) ระยะเวลาในการใช้

(๓.๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๓.๔) การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

(๓.๕) กำหนดข้อตกลงการใช้งานข้อมูลเพื่อเป็นการป้องกันการเปิดเผยข้อมูล

(๔) หน่วยงานภายนอกที่ทำงานให้กับหน่วยงานไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กรโดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

(๕) หน่วยงานภายนอกซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

(๖) สำหรับโครงการขนาดใหญ่หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กรผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้านคือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(๗) องค์กรมีสิทธิในการตรวจสอบตามสัญญาหรือข้อตกลงการใช้งานระบบสารสนเทศเพื่อให้มั่นใจได้ว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(๘) ต้องกำหนดให้หน่วยงานภายนอกหรือผู้ให้บริการจัดทำแผนการดำเนินงานคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของหน่วยงานภายนอกหรือผู้ให้บริการเพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดหรือตกลงไว้

ส่วนที่ ๗
นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก
(Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

๑. วัตถุประสงค์

เพื่อป้องกันการบุกรุก โจมตีจากภายนอกกรม โดยต้องมีการตรวจสอบการใช้งานบนระบบเครือข่ายภายในกรม รวมไปถึงพฤติกรรมต่างๆ ที่เกิดขึ้นบนเครือข่ายสื่อสารของกรม และจะต้องมีการบันทึกเป็นลายลักษณ์อักษร สามารถตรวจสอบย้อนหลังได้

๒. แนวทางปฏิบัติ

ข้อ ๑ ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ (IPS) เหตุการณ์ผิดปกติและการแจ้งเตือนต่างๆ ที่อุปกรณ์ตรวจพบ โดยต้องวิเคราะห์และหาสาเหตุของการบุกรุกในระบบสารสนเทศของกรม เพื่อเป็นเครื่องมือสำหรับการสืบสวนหาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด ป้องกันก่อนที่จะเกิดการโจมตี

ข้อ ๒ ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามที่บุกรุกหรือโจมตีกรมเป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยและระบบรักษาความปลอดภัยอื่น ๆ เพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตรายที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือ Hacker รวมทั้งไวรัสประเภทต่างๆ

ข้อ ๓ ผู้ดูแลระบบต้องมีการบริหารจัดการเหตุการณ์บุกรุกระบบ (Incident Management) เป็นการตอบสนองต่อเหตุการณ์บุกรุกทางเครือข่าย สามารถวิเคราะห์ลักษณะการบุกรุกทางเครือข่าย และนำมาแก้ไขสถานการณ์ได้อย่างถูกต้อง ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการบุกรุก โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับกรม และจัดหาวิธีปฏิบัติที่ถูกต้องให้กับกรมเพื่อป้องกันเหตุการณ์เกิดซ้ำ การตอบสนองต่อเหตุการณ์การบุกรุกแบ่งออกเป็น ๔ ขั้นตอน คือ

(๓.๑) จำกัดขอบเขต (Containment) จำกัดพื้นที่ที่เสี่ยงต่อการบุกรุกและจำกัดความรุนแรงของการบุกรุก

(๓.๒) จำกัดต้นเหตุ (Eradication) กำจัดต้นเหตุของการบุกรุก รวมถึงปิดกั้นช่องทางการบุกรุก

(๓.๓) กู้คืนระบบ (Recovery) แก้ไขระบบที่ถูกบุกรุกให้สามารถกลับมาทำงานได้ตามปกติ

(๓.๔) ติดตามผล (Follow–Up) บันทึกผลกระทบของเหตุการณ์และแนะนำวิธีปฏิบัติเพื่อป้องกันเหตุการณ์เกิดซ้ำ

ข้อ ๔ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ ๕ ผู้ดูแลระบบต้องทำการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ และประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง

ข้อ ๖ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของกรมและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลเดินทางในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๗ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IPS

ข้อ ๘ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๙ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๑๐ มีการตรวจสอบและ Update Patch/Signature ของ IPS เป็นประจำ

ข้อ ๑๑ ผู้ดูแลระบบต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำ

ข้อ ๑๒ IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๑๓ เครื่องแม่ข่ายที่มีการติดตั้ง host-based IPS จะต้องมีการตรวจสอบข้อมูลเป็นประจำ

ข้อ ๑๔ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ผู้ดูแลระบบต้องรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

ข้อ ๑๕ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ ผู้ดูแลระบบต้องรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๖ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน หรือตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือตามที่กฎหมายกำหนด

ข้อ ๑๗ การบริหารจัดการการบุกรุกเครือข่ายต้องมีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหายลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๘ ผู้ดูแลระบบมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๙ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของกรม การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศจะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของกรม จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๘

นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery)

๑. วัตถุประสงค์

เพื่อจัดให้มีระบบสารสนเทศของกรมการขนส่งทางบก ระบบสำรองของระบบสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้สามารถใช้งานสารสนเทศได้อย่างต่อเนื่องและให้บริการได้ตามปกติ มีมาตรการในการสำรองข้อมูลที่เป็นมาตรฐาน แนวทางปฏิบัติของผู้ดูแลระบบ และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินหรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๒. แนวทางปฏิบัติ

ส่วนที่ ๑ ระบบสำรองข้อมูลสารสนเทศและการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

ข้อ ๑ ผู้ดูแลระบบหรือผู้รับผิดชอบต้องทำการสำรองข้อมูลระบบงานหลักของกรม ได้แก่

- ระบบงานควบคุมบัญชีรถและเครื่องยนต์
- ระบบงานทะเบียนตรวจสภาพรถภาษีรถยนต์และรถขนส่ง
- ระบบงานใบอนุญาตขับรถและผู้ประจำรถ
- ระบบงานใบอนุญาตประกอบการขนส่ง
- ระบบงานใบอนุญาตประกอบการรถยนต์รับจ้างและบริการ
- ระบบงานโครงข่ายเส้นทางและเงื่อนไขการเดินรถ
- ระบบงานทรัพยากรบุคคล
- ระบบงานการเงิน บัญชี และงบประมาณ ระบบงานควบคุมพัสดุและครุภัณฑ์
- ระบบงานสารบรรณ ระบบงานเพื่อการสื่อสารในองค์กร
- ระบบงานเพื่อให้บริการระบบ e-Service
- ระบบงานแผนที่ข้อมูล
- ระบบการให้บริการผ่าน web application และ mobile application

รวมถึงโปรแกรมระบบปฏิบัติการ (Operation System) โปรแกรมระบบงานคอมพิวเตอร์ (Application) และชุดคำสั่งที่ใช้งานให้ครบถ้วน ตรวจสอบข้อมูลทั้งหมดว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และทดลองกู้คืนข้อมูลพร้อมทดสอบการใช้งานข้อมูลให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

ข้อ ๒ ผู้ดูแลระบบหรือผู้รับผิดชอบต้องจัดทำแผนในการรองรับสถานการณ์ฉุกเฉินหากเกิดปัญหาไม่สามารถใช้งานข้อมูลที่ทำการสำรอง และมีวิธีปฏิบัติการกู้คืนข้อมูล

ข้อ ๓ ต้องมีขั้นตอนและวิธีการปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยมีรายละเอียด ดังนี้

(๑) ข้อมูลที่ต้องสำรอง และความถี่ในการสำรองข้อมูล

(๒) ประเภทสื่อบันทึก (Media)

(๓) จำนวนที่ต้องสำรอง (Copy)

(๔) ขั้นตอนและวิธีการเก็บรักษาสื่อบันทึก

(๕) สถานที่และวิธีการเก็บรักษาสื่อบันทึก

ข้อ ๔ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของกรมการขนส่งทางบก พร้อมทั้งกำหนดระบบสารสนเทศที่ต้องสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรองข้อมูล

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง ได้แก่ การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

ข้อ ๖ ต้องบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน เวลา ชื่อข้อมูลที่สำรองสำเร็จและไม่สำเร็จ

ข้อ ๗ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

ข้อ ๘ จัดเก็บข้อมูลสำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องอยู่ห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

ข้อ ๙ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่จัดเก็บข้อมูลนอกสถานที่

ข้อ ๑๐ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

ข้อ ๑๑ ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย

ข้อ ๑๒ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่สำรองเก็บไว้ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

ข้อ ๑๓ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ ๑๔ ผู้ดูแลระบบหรือผู้รับผิดชอบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้ในการแก้ไขเป็นลายลักษณ์อักษร

ข้อ ๑๕ ผู้ดูแลระบบหรือผู้รับผิดชอบต้องมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ไม่สามารถปฏิบัติงานได้

ข้อ ๑๖ หากพบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาเป็นลายลักษณ์อักษร

ข้อ ๑๗ ผู้ดูแลระบบหรือผู้รับผิดชอบต้องกำหนดช่วงเวลาการสำรองข้อมูล พร้อมทั้งสื่อที่ใช้ในการเก็บข้อมูล

ข้อ ๑๘ ผู้ดูแลระบบหรือผู้รับผิดชอบต้องทบทวนคู่มือการปฏิบัติงานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับสถานการณ์ปัจจุบัน

ข้อ ๑๙ นโยบายที่เกี่ยวข้องกับการสำรองข้อมูลและกู้คืนข้อมูล ผู้ดูแลระบบหรือผู้รับผิดชอบต้องปฏิบัติตามขั้นตอนการปฏิบัติอย่างเคร่งครัด

ส่วนที่ ๒ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

๒.๑ การแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย

(๑) ให้ผู้ใช้งานต้องแจ้งไปศูนย์เทคโนโลยีสารสนเทศทันทีที่มีเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบสนเทศของหน่วยงาน ดังนี้

(ก) มีไวรัสหรือชุดคำสั่งไม่พึงประสงค์เข้ามาในระบบ

(ข) มีการบุกรุกเข้ามาในเครือข่าย

(ค) ข้อมูลสำคัญมีการเปลี่ยนแปลงหรือสูญหาย

(ง) มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(จ) มีการนำข้อมูลที่สำคัญไปใช้ผิดวัตถุประสงค์

(ฉ) มีการใช้ระบบสารสนเทศผิดวัตถุประสงค์

(ช) พบจุดอ่อนในระบบงาน ซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้งาน

(ซ) มีการโจมตีเข้ามาในระบบจนไม่สามารถให้บริการได้

(ฌ) ระบบสารสนเทศชำรุดหรือสูญหาย

(ญ) บุคคลภายนอกเข้าใช้ระบบสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต

(ฎ) มีการติดตั้งซอฟต์แวร์เพื่อขโมยข้อมูล เข้าถึงข้อมูลหรือเหตุการณ์อื่นที่เป็นการละเมิดต่อความมั่นคงปลอดภัยของหน่วยงาน

๒.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเมื่อได้รับแจ้งเหตุตามข้อ ๒.๑ จากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่พบ ให้ปฏิบัติดังนี้

(๑) ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบระดับใด

(๒) แจ้งผู้บริหารระดับสูง และผู้บริหารระดับสูงสุดทราบทันที

(๓) ต้องทำการวิเคราะห์ปัญหาและแก้ไขปัญหาตามความจำเป็น โดยดำเนินการร่วมกับทีมที่ปรึกษาด้านเทคโนโลยีสารสนเทศ แล้วแต่กรณี

(๔) กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ มีผู้เชี่ยวชาญหรือผู้ที่ผ่านการอบรมหรือได้รับการฝึกฝนเป็นผู้ดำเนินการ เพื่อป้องกันไม่ให้หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัยและจำกัดการเข้าถึงหลักฐานนั้น

(๕) จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลางขึ้นไป และแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีรายละเอียดข้อมูลดังนี้

- รายละเอียดเหตุการณ์
- วันเวลา สถานที่เกิดเหตุ
- ชื่อผู้แจ้ง/หน่วยงาน
- สถานะของเหตุการณ์ในแต่ละช่วงเวลา
- ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา
- สาเหตุและวิธีการแก้ไข
- ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

๒.๓ ความรับผิดชอบของผู้อำนวยการกรณีที่มีการละเมิดการปฏิบัติ ต้องปฏิบัติดังนี้

(๑) ให้รายงานต่อผู้บริหารระดับสูง และผู้บริหารระดับสูงสุดทราบ

(๒) สั่งการสอบสวนหาตัวผู้กระทำความผิดและผู้รับผิดชอบให้เร็วที่สุด

(๓) พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เกิดเหตุการณ์ซ้ำได้อีก

(๔) ต้องพิจารณาบทลงโทษ เสนอผู้บริหารระดับสูงและผู้บริหารระดับสูงสุด เพื่อสั่งการลงโทษทางวินัย หรือดำเนินคดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ต่อผู้ละเมิด ผู้เกี่ยวข้องและผู้รับผิดชอบเมื่อมีการละเมิดตามระเบียบนี้จะโดยเจตนาหรือไม่เจตนาก็ดี และการละเมิดนั้นจะเกิดความเสียหายหรือยังไม่เกิดความเสียหายต่อราชการก็ตาม

๒.๔ ความรับผิดชอบของผู้ดูแลระบบ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัยให้ดำเนินการ ดังนี้

(๑) พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่าง ๆ หรือรหัสผ่านที่จำเป็นในการใช้เครือข่ายสื่อสารข้อมูลสารสนเทศ มีผลกระทบหรือสร้างความเสียหายต่อราชการอย่างไรบ้าง

(๒) ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดทันที ในการนี้ต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงาน และวิธีปฏิบัติพร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นสมควร

๒.๕ ความรับผิดชอบของผู้ใช้งานต่อประกาศ

(๑) ปฏิบัติตามประกาศนี้อย่างเคร่งครัด และต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

(๒) ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไขหรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบสารสนเทศและเครือข่ายของหน่วยงาน

(๓) ไม่รบกวน หรือแทรกแซงการสื่อสารข้อมูลในระบบอินเทอร์เน็ตและเครือข่ายของหน่วยงาน

(๔) รายงานความเสี่ยง จุดอ่อน จุดแข็ง หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังศูนย์เทคโนโลยีสารสนเทศโดยเร็วที่สุด

ส่วนที่ ๙

นโยบายการใช้เครื่องคอมพิวเตอร์และอุปกรณ์พกพา

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกกรม เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ของกรมให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยง ในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

๒. แนวทางปฏิบัติ

การใช้งานทั่วไป

ข้อ ๑ เครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาที่กรมอนุญาตให้ผู้ใช้งานเป็นทรัพย์สินของหน่วยงาน ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่อภารกิจของหน่วยงาน

ข้อ ๒ โปรแกรมที่ได้ถูกติดตั้งบนเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาต้องเป็นโปรแกรมมีลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

ข้อ ๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) และอุปกรณ์แบบพกพาจะต้องอยู่ภายใต้การควบคุมของเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศเท่านั้น

ข้อ ๔ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาเพื่อตรวจซ่อมจะต้องดำเนินการภายใต้การควบคุม ของเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่รับผิดชอบเท่านั้น

ข้อ ๕ ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

ข้อ ๖ ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพการใช้งานคงเดิม

ข้อ ๗ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

ข้อ ๘ ไม่ควรใส่เครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาไปในกระเป๋าเดินทางที่เสียงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรือการถูกกระแทกหรือโยนจากการเคลื่อนย้าย

ข้อ ๙ การใช้เครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

ข้อ ๑๐ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง กดสัมผัสหน้าจอให้เป็นรอยขีดข่วนหรือทำให้จอของเครื่องคอมพิวเตอร์แบบพกพาเป็นแตกชำรุดหรือเสียหายได้

ข้อ ๑๑ ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์

ข้อ ๑๒ การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อ ๑๓ ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส

ข้อ ๑๔ ห้ามวางเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

ข้อ ๑๕ การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างระมัดระวัง และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

ความปลอดภัยทางด้านกายภาพ

ข้อ ๑ ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

ข้อ ๒ ผู้ใช้งานห้ามเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อ ๓ ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

การควบคุมการเข้าถึงระบบปฏิบัติการ

ข้อ ๑ การปฏิบัติเพื่อการใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๑.๑) ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

(๑.๒) ก่อนเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง

(๑.๓) ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

(๑.๔) ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ ๒ การระบุและยืนยันตัวตนของผู้ใช้งาน

(๒.๑) การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง มีข้อพึงปฏิบัติ ดังนี้

๒.๑.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (User Name) และแสดงตัวตนก่อนเข้าใช้งานด้วยชื่อผู้ใช้ (Username) หรือ รหัสผู้ใช้งานที่กำหนด (ID)

๒.๑.๒ การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password) โดยระบบมีการจำกัดระยะเวลาในการป้อนรหัสผ่าน และสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสจากเครื่องปลายทาง

๒.๑.๓ สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Smart Card ร่วมได้

(๒.๒) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๒.๒.๑ ผู้ใช้งานที่เป็นเจ้าของบัญชีบริการ (Account) ต้องเป็นผู้รับผิดชอบในผลอันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๒.๒ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับ ห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่ายหรือแจกจ่ายให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๒.๒.๓ ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบัญชีออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งาน

ข้อ ๓ การบริหารจัดการรหัสผ่าน

(๓.๑) ผู้ดูแลระบบต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย โดยการกำหนดรหัสผ่านเป็นไปตามเงื่อนไขที่กำหนด ซึ่งประกอบด้วยตัวอักษร ตัวเลข และอักขระพิเศษ ความยาวรวมไม่ต่ำกว่า ๖ อักขระ

(๓.๒) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๖ เดือน

(๓.๓) การเปลี่ยนรหัสผ่านต้องไม่กำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมในครั้งสุดท้าย

(๓.๔) ระบบบริหารจัดการรหัสผ่านต้องป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้ หรือที่จำเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

ข้อ ๔ การใช้งานโปรแกรมอรรถประโยชน์

(๔.๑) กำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมอรรถประโยชน์ ระดับสิทธิของผู้ขออนุมัติ การระบุและพิสูจน์ตัวตนสำหรับการเข้าใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

(๔.๒) ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมบางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๔.๓) โปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน

(๔.๔) ต้องจัดเก็บโปรแกรมอรรถประโยชน์และซอฟต์แวร์สำหรับระบบงาน

(๔.๕) ต้องยกเลิก ลบทิ้งโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่ไม่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงและใช้งานโปรแกรมอรรถประโยชน์ได้

ข้อ ๕ การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-out) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้นตามระยะเวลาที่กำหนด ดังนี้

(๕.๑) ต้องกำหนดให้ระบบสารสนเทศ ได้แก่ ระบบงานต่างๆ ของกรม อุปกรณ์เครือข่าย มีการตัดและหมดเวลาการใช้งาน รวมถึงการปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๑๐ นาที

(๕.๒) ต้องกำหนดให้ระบบสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๑๐ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

(๕.๓) ต้องกำหนดให้ระบบสารสนเทศที่มีความสำคัญและมีความเสี่ยงสูง ได้แก่ ระบบงานการเงิน บัญชีและงบประมาณ ระบบบริหารทรัพยากรบุคคล และระบบที่มีความสำคัญต่อกรม มีการตัดและหมดเวลาการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

(๖.๑) ต้องกำหนดให้ระบบสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาทำงานราชการตามปกติเท่านั้น

(๖.๒) ต้องกำหนดให้ระบบสารสนเทศที่มีความสำคัญและมีความเสี่ยงสูงมาก ได้แก่ ระบบงานการเงิน บัญชีและงบประมาณ ระบบบริหารทรัพยากรบุคคล และระบบที่มีความสำคัญต่อกรม กำหนดให้ใช้งานได้ ๒ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง มีการตัดและหมดเวลาการใช้งานหลังจากไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๖.๓) ต้องกำหนดให้ระบบสารสนเทศมีการจำกัดช่วงเวลาการใช้งาน มีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานตามระยะเวลาที่กำหนดไว้

การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์(Malware)

ข้อ ๑ ผู้ใช้ ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่(Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ โดยไม่ส่งผลกระทบต่อการใช้งาน

ข้อ ๒ ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

ข้อ ๓ หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์(Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

การสำรองข้อมูลและการกู้คืน

ข้อ ๑ ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

ข้อ ๒ ผู้ใช้ควรจะเก็บรักษาสื่อสำรองข้อมูล(Backup media)ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

ข้อ ๓ สื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

ข้อ ๔ สื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก ด้วยวิธีการทำลายที่เหมาะสม

ส่วนที่ ๑๐

การควบคุมการเข้าถึงห้องเครื่องคอมพิวเตอร์และห้องเครือข่ายสื่อสารข้อมูล

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงศูนย์ข้อมูลหลัก (Data Center) และระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบสารสนเทศ

๒. แนวทางปฏิบัติ

ข้อ ๑ แบ่งแยกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารและสถานที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายสื่อสารข้อมูลให้ชัดเจนและเป็นลายลักษณ์อักษร

ข้อ ๒ กำหนดสิทธิให้กับเจ้าหน้าที่ให้มีสิทธิสามารถเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

ข้อ ๓ ทำความเข้าใจและประชาสัมพันธ์ให้แก่ผู้ใช้งาน (Users) และบุคคลภายนอกเพื่อให้เข้าใจกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ในระหว่างที่ปฏิบัติงานอยู่ในห้องศูนย์ข้อมูลและบริเวณที่มีความสำคัญ และต้องไม่นำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณห้องศูนย์ข้อมูลหลัก (Data Center)

ข้อ ๔ กำหนดผู้รับผิดชอบในการบันทึกการเข้า-ออก และจัดทำรายงานการเข้า-ออกพื้นที่เสนอผู้บังคับบัญชา

ข้อ ๕ ไม่อนุญาตให้ผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูลและบริเวณที่มีความสำคัญ เว้นแต่ได้รับการอนุญาต กรณีมีความจำเป็นให้ผู้ดูแลระบบตรวจสอบเหตุผล วัตถุประสงค์และความจำเป็นโดยละเอียดก่อนเสนอขออนุญาตจากผู้อำนวยการทุกครั้ง

ข้อ ๖ บุคคลภายนอกเข้ามาติดต่อต้องลงชื่อ เพื่ออนุญาตเข้าออกในแบบฟอร์มการเข้า-ออก ที่ศูนย์เทคโนโลยีสารสนเทศกำหนด ตามความจำเป็น โดยจัดทำเป็นเอกสาร “บันทึกการเข้า-ออกพื้นที่” ไว้ให้ชัดเจนและให้ปรับปรุงรายการผู้มีสิทธิเข้า-ออกพื้นที่ใช้งานห้องศูนย์ข้อมูลหลัก (Data Center) อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗ ผู้ใช้งานหรือบุคคลภายนอกที่เข้ามาปฏิบัติงานในหน่วยงาน ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่ปฏิบัติงาน และต้องให้ลงชื่อขออนุญาตการเข้า-ออกในแบบฟอร์มที่กำหนดไว้ โดยมีผู้ดูแลระบบควบคุมการปฏิบัติงานของผู้ใช้งานหรือบุคคลภายนอกตลอดเวลา

ข้อ ๘ บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอใช้พื้นที่ หน่วยงานผู้รับผิดชอบพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

ข้อ ๙ จัดทำประกาศ และประกาศให้บุคคลภายนอกได้รับทราบถึงข้อปฏิบัติในการเข้าในงานพื้นที่ห้องเครื่องคอมพิวเตอร์และห้องเครือข่ายสื่อสารข้อมูล

ข้อ ๑๐ บุคคลภายนอกที่ต้องการเข้าใช้งานห้องเครื่องคอมพิวเตอร์และห้องเครือข่ายสื่อสารข้อมูลจะต้องแจ้งเป็นลายลักษณ์อักษร ประกอบด้วยรายชื่อ วันเวลา และวัตถุประสงค์ที่จะเข้ามาดำเนินงาน และต้องเป็นตามประกาศที่ศูนย์เทคโนโลยีสารสนเทศกำหนด

ข้อ ๑๑ ทบทวนข้อกำหนดในการเข้าใช้งานพื้นที่ห้อง Data Center อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๑

นโยบายด้านการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการตรวจสอบ การควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศรวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้องส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจนและสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๒. แนวทางปฏิบัติ

ข้อ ๑ หน่วยงานจะต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศโดยผู้ตรวจสอบภายในหรือผู้ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ ตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยกลุ่มตรวจสอบภายในของกรม (Internal audit) หรือ โดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External audit) ปีละ ๑ ครั้ง เพื่อตรวจสอบและประเมินความเสี่ยงในภาพรวมการใช้งานด้านระบบสารสนเทศ และให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ และดำเนินการเพื่อป้องกันและแก้ไขปัญหาที่ตรวจพบ

ข้อ ๓ จัดลำดับความสำคัญของความเสี่ยง และระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของกรม

ข้อ ๔ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานเพื่อการประเมินความเสี่ยงนั้นๆ

ข้อ ๕ กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

ข้อ ๖ ติดตามการดำเนินการตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานที่ได้กำหนดไว้

ข้อ ๗ ทบทวนและปรับปรุงแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานในด้านต่างๆ อย่างน้อยปีละ ๑ ครั้งให้สอดคล้องกับสถานการณ์

ส่วนที่ ๑๒

นโยบายการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๑. วัตถุประสงค์

เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศให้กับผู้ใช้งานของหน่วยงาน ป้องกันการกระทำความผิดทางคอมพิวเตอร์อันอาจเกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน และเพื่อให้การใช้งานเครือข่ายและระบบสารสนเทศมีความมั่นคงปลอดภัย

๒. แนวปฏิบัติ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

ข้อ ๑ จัดทำหลักสูตรฝึกอบรม และจัดทำคู่มือการใช้งานระบบสารสนเทศและเผยแพร่ทางเว็บไซต์ของหน่วยงาน

ข้อ ๒ จัดประชุมสัมมนา อบรมหรือมีหนังสือเวียนแจ้งหน่วยงาน ในการเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งานได้ทราบ โดยสอดแทรกเนื้อหาไปกับหลักสูตรอื่น ๆ ของหน่วยงานที่จัดอยู่ได้ และอาจเชิญวิทยากรจากหน่วยงานภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดองค์ความรู้

ข้อ ๓ ติดประกาศ ประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวนโยบายและแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย และต้องปรับปรุงความรู้ให้ทันสมัยและง่ายต่อการจดจำอยู่เสมอ โดยต้องทบทวน ปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางบกให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผลและสำรวจความต้องการของผู้ใช้งาน

ข้อ ๕ สร้างความตระหนักเกี่ยวกับไวรัสหรือชุดคำสั่งไม่พึงประสงค์ เพื่อให้บุคลากรของหน่วยงานมีความรู้ ความเข้าใจ ป้องกันตนเองได้ และรับทราบขั้นตอนปฏิบัติเมื่อพบเหตุว่าต้องดำเนินการในเบื้องต้นอย่างไร

ข้อ ๖ สร้างความเข้าใจให้แก่ผู้ใช้งาน ให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรืออาจเกิดขึ้นอย่างไม่คาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของสำนักงานอัยการสูงสุด

ข้อ ๗ ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบต่างๆ ของหน่วยงานอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ส่วนที่ ๑๓

นโยบายการปฏิบัติงานภายนอกสำนักงาน (Teleworking)

๑. วัตถุประสงค์

เพื่อรองรับการปฏิบัติงานในสถานการณ์ที่อาจเป็นอุปสรรคทำให้ไม่สามารถปฏิบัติงานในอาคารสำนักงานได้ และมีความจำเป็นต้องปฏิบัติงานภายนอกสำนักงาน โดยที่การปฏิบัติงานไม่สะดุดหยุดชะงัก และการเข้าถึงระบบสารสนเทศของกรมได้อย่างมีประสิทธิภาพและปลอดภัย

๒. แนวปฏิบัติ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะเจ้าหน้าที่ผู้ปฏิบัติงาน หรือผู้ที่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศตามภาระหน้าที่ โดยให้สามารถเข้าถึงระบบสารสนเทศเพื่อปฏิบัติงานได้ โดยมีข้อปฏิบัติอย่างน้อย ดังนี้

ข้อ ๑ มีการตรวจสอบว่าอุปกรณ์ที่ใช้ปฏิบัติงานนั้นเป็นของส่วนตัวหรือของหน่วยงานที่อนุญาตให้ใช้เพื่อการปฏิบัติงานนอกสำนักงานที่มีการป้องกันไวรัส โปรแกรมไม่พึงประสงค์และการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด หากจำเป็นต้องการเข้าถึงระบบสารสนเทศของกรม

ข้อ ๒ ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัตินอกสำนักงาน การจัดเก็บข้อมูล และอุปกรณ์สื่อสารสำหรับผู้ใช้งานนอกสำนักงาน

ข้อ ๓ ผู้ใช้งานนอกสำนักงานต้องผ่านการพิสูจน์ตัวตนก่อนการใช้งาน เพื่อความปลอดภัยในการเข้าถึงระบบสารสนเทศ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ ๔ ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบสารสนเทศของหน่วยงานจากภายนอกสำนักงาน หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมเพื่อเข้าถึงระบบสารสนเทศของกรมการขนส่งทางบก

ข้อ ๕ ต้องกำหนดประเภทของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและระบบบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากภายนอกสำนักงาน

ข้อ ๖ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบสารสนเทศและการกู้คืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ข้อ ๗ กำหนดมาตรการป้องกันการรั่วไหลของข้อมูลสารสนเทศ หรือการเข้าถึงระบบสารสนเทศจากผู้ที่ไม่เกี่ยวข้อง

ข้อ ๘ กรณีที่เป็นการประชุมทางไกลให้มีการใช้โปรแกรมหรือช่องทางที่หน่วยงานจัดหาไว้ โดยมีรหัสผู้เข้าร่วมประชุมและรหัสผ่านตามที่กำหนด

ส่วนที่ ๑๔

การกำหนดหน้าที่ความรับผิดชอบ

การกำหนดหน้าที่ความรับผิดชอบ มีวัตถุประสงค์เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้น ซึ่งมีแนวทางปฏิบัติดังนี้ คือ ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ ในส่วนการพัฒนาระบบงานออกจากบุคลากรที่ทำหน้าที่บริหารระบบ ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริงและต้องจัดให้มีการระบุหน้าที่ความรับผิดชอบของแต่ละหน้าที่ความรับผิดชอบของบุคลากรแต่ละคน ภายในศูนย์เทคโนโลยีสารสนเทศ อย่างชัดเจนเป็นลายลักษณ์อักษร ซึ่งมีการจัดให้มีบุคลากรสำรองในกรณีที่ผู้รับผิดชอบไม่สามารถดำเนินการได้ เพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น โดยกำหนดหน้าที่ ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบสารสนเทศ รายละเอียดดังนี้

๑. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย คำปรึกษา ให้ข้อเสนอแนะ ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบสารสนเทศของกรมการขนส่งทางบก หรืออันตรายใดๆ ซึ่งเกิดจากผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

อธิบดีกรมการขนส่งทางบก ในฐานะผู้บริหารระดับสูงสุดของกรม (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีที่ระบบสารสนเทศหรือข้อมูลสารสนเทศที่มีความสำคัญเกิดความเสียหายหรืออันตรายใดๆ แก่กรม หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

รองอธิบดีกรมการขนส่งทางบก (ฝ่ายวิชาการ) ในฐานะผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบ ติดตาม กำกับ ควบคุม ดูแล ตรวจสอบ รวมทั้งให้ข้อเสนอแนะและคำปรึกษากับผู้ใช้งานในการปฏิบัติงาน

๒. ระดับปฏิบัติ

๒.๑ รับผิดชอบในการทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ	นายนุตนันทน์ นุตาลัย	โทร. ๐๘-๙๑๓๖-๑๑๕๕
หัวหน้ากลุ่มนโยบายและมาตรฐานเทคโนโลยีสารสนเทศ	นางสาวพนิดา อุตสาหภูมิ	โทร. ๐๘-๗๑๑๓-๗๒๒๓
หัวหน้ากลุ่มบริหารข้อมูลและระบบสารสนเทศ	นางสาวเพลินพิศ แซ่เตีย	โทร. ๐๘-๖๙๐๖-๗๘๙๖
หัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย	นายธนู ชมภูงาม	โทร. ๐๘-๖๓๑๐-๕๗๒๙
หัวหน้ากลุ่มเทคโนโลยีการขนส่งทางถนน	นายอิษฎา วิทูรากร	โทร. ๐๘-๒๐๙๔-๓๗๗๗

๒.๒ รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัยในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายระบบเครือข่าย ห้องเครื่องคอมพิวเตอร์ห้องเครือข่ายสื่อสารข้อมูล ระบบสนับสนุนต่างๆ ควบคุมการสำรองข้อมูลและการกู้คืนข้อมูลระบบคอมพิวเตอร์แม่ข่ายระบบเครือข่ายสื่อสารข้อมูล รวมไปถึงการสำรองข้อมูลของระบบสารสนเทศหลักของกรม ผู้รับผิดชอบ ได้แก่

หัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย	นายธนู ชมภูงาม	โทร. ๐๘-๖๓๑๐-๕๗๒๙
หัวหน้างานระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย	นายกิตติพล วิมุกติพันธุ์	โทร. ๐๘-๙๗๑๓-๘๒๕๕
นักวิชาการคอมพิวเตอร์ชำนาญการ	นายศุภชัย พลโก	โทร. ๐๘-๖๕๔๒-๔๒๔๑
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายโชคอำนวย เถื่อนสันเทียะ	โทร.๐๘-๕๖๓๙-๙๘๕๖
เจ้าหน้าที่ระบบงานคอมพิวเตอร์	นายจักริน ไอศุริยสมบัติ	โทร.๐๘-๖๕๕๘-๘๗๒๙

มีหน้าที่รับผิดชอบ ดังนี้

(๑) ควบคุมการเข้า – ออก ห้องควบคุมระบบคอมพิวเตอร์ตามการกำหนดสิทธิการเข้าถึงห้องเครื่องคอมพิวเตอร์แม่ข่ายและห้องเครือข่ายสื่อสารข้อมูล

(๒) ดูแลตรวจสอบการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์อื่นๆ ที่เกี่ยวข้อง ที่อยู่ในห้องเครื่องคอมพิวเตอร์แม่ข่าย

(๓) ควบคุมตรวจสอบการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่เกี่ยวข้อง ที่ติดตั้ง ณ อาคารระบบข้อมูลกลางและสำรองข้อมูล ณ สำนักงานขนส่งจังหวัดนนทบุรี

(๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล ตามขั้นตอนและระยะเวลาที่กำหนด

(๕) ตรวจสอบการใช้งานระบบเครือข่ายสื่อสารหลัก และเครือข่ายสำรองของกรม

(๖) กำกับ ดูแล การบำรุงรักษาอุปกรณ์เครือข่ายสื่อสารและอุปกรณ์อื่นๆ ที่เกี่ยวข้อง ให้สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ

๒.๓ รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัยในการเข้าถึงเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบประชุมทางไกล ระบบสื่อสารภายในองค์กร เว็บไซต์และการเผยแพร่ข้อมูล ข่าวสาร และสื่อการเรียนรู้ทางวิชาการ ควบคุมการสำรองและการกู้คืนข้อมูลของระบบสื่อสารภายในองค์กร เครื่องคอมพิวเตอร์ลูกข่าย ระบบอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ การแก้ไขปัญหา ติดตามและประเมินผลการใช้งานระบบสารสนเทศ การแก้ไขซ่อมแซม การติดตั้งเครื่องคอมพิวเตอร์ และการติดตั้งซอฟต์แวร์ต่างๆ การจัดทำทะเบียนครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง ผู้รับผิดชอบ ได้แก่

หัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย	นายธนู ชมภูงาม	โทร. ๐๘-๖๓๑๐-๕๗๒๙
หัวหน้างานสนับสนุนระบบสารสนเทศ	นายอภินันท์ สุวรรณนุรักษ์	โทร. ๐๘-๑๘๗๕-๔๓๙๙
นักวิชาการคอมพิวเตอร์ชำนาญการ	นางสาวชนิดา เจริญสมบัติอมร	โทร. ๐๘-๑๖๔๓-๙๙๙๙
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายทวีป นาคงาม	โทร. ๐๘-๘๔๒๔-๘๑๔๓
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายกิตติชัย เกษลา	โทร. ๐๘-๘๐๕๔-๖๑๔๓
เจ้าหน้าที่บันทึกข้อมูล	นายณัฐพล นกดี	โทร. ๐๘-๗๙๘๐-๙๒๓๓
เจ้าหน้าที่บันทึกข้อมูล	นายทรงสวัสดิ์ พูลสวัสดิ์	โทร. ๐๘-๙๐๗๕-๙๗๙๐
เจ้าหน้าที่บันทึกข้อมูล	นางสาวกัญญาพัชร ภูมูลเมือง	โทร. ๐๖-๔๔๑๓-๓๖๓๕

มีหน้าที่รับผิดชอบ ดังนี้

(๑) ตรวจสอบ ดูแล การใช้งานเครื่องคอมพิวเตอร์ลูกข่ายทั้งหมดในส่วนกลางและส่วนภูมิภาค ระบบอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ของกรม

(๒) กำกับ ดูแล ตรวจสอบการบำรุงรักษาเครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์ต่างๆ ที่เกี่ยวข้อง ทั้งในส่วนกลางและส่วนภูมิภาค

(๓) รักษาความปลอดภัยในการเข้าถึงเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

(๔) จัดระบบประชุมทางไกล (Video- Conference) ระหว่างหน่วยงานส่วนกลางกับส่วนภูมิภาค

(๕) ปรับปรุง ดูแลเรื่องระบบสื่อสารภายในองค์กร เว็บไซต์และการเผยแพร่ข้อมูลข่าวสาร และสื่อการเรียนรู้ทางวิชาการของกรม ตลอดจนควบคุมการสำรองและการกู้คืนข้อมูลของระบบสื่อสารภายในองค์กร เครื่องคอมพิวเตอร์ลูกข่าย

(๖) กำหนดสิทธิและตรวจสอบจำนวนผู้ใช้งานระบบอินทราเน็ตและจดหมายอิเล็กทรอนิกส์ของกรม

(๗) บริหารจัดการ การใช้งานพื้นที่ของเว็บไซต์ของหน่วยงานทั้งส่วนกลางและส่วนภูมิภาค

(๘) แก้ไขปัญหา ติดตามและประเมินผลการใช้งานระบบสารสนเทศ การแก้ไขซ่อมแซม การติดตั้งเครื่องคอมพิวเตอร์ และการติดตั้งซอฟต์แวร์ต่างๆ การจัดทำทะเบียนครุภัณฑ์เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

๒.๔ รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย บริหารจัดการ และบำรุงรักษาระบบฐานข้อมูลและคลังข้อมูล ระบบสารสนเทศ และระบบเชื่อมโยงข้อมูล ตรวจสอบและกำหนดสิทธิในการใช้งานระบบฐานข้อมูล ระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

หัวหน้ากลุ่มบริหารข้อมูลและระบบสารสนเทศ	นางสาวเพลินพิศ แซ่เตีย	โทร. ๐๘-๖๙๐๖-๗๘๙๖
หัวหน้างานบริหารฐานข้อมูล	นางสาวศศิธร คำพันยิ้ม	โทร. ๐๘-๖๖๒๖-๙๑๑๓
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นางสาวรัชชาภรณ์ สุกลพราหมณ์	โทร. ๐๙-๑๘๘๗-๑๓๗๓
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายวีระพงษ์ จันทร์วงศ์	โทร. ๐๘-๖๗๓๔-๒๗๙๘
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายวโรภาส วุ่นศรี	โทร. ๐๘-๖๕๖๘-๖๔๕๒
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นางสาวธนพร แสงอินทร์	โทร. ๐๘-๖๓๘๘-๐๒๗๑

มีหน้าที่รับผิดชอบ ดังนี้

(๑) กำหนดสิทธิ และตรวจสอบจำนวนผู้ใช้งานระบบสารสนเทศหลักของกรม

(๒) กำหนดสิทธิ และตรวจสอบ หน่วยงานภายนอกทั้งภาครัฐและภาคเอกชน ที่มีการเชื่อมโยงข้อมูลจากระบบสารสนเทศหลักของกรม

(๓) บำรุงรักษาฐานข้อมูล การแลกเปลี่ยนข้อมูล กำหนดมาตรฐานโครงสร้างฐานข้อมูลและคลังข้อมูล ตรวจสอบการใช้งานฐานข้อมูล บริหารจัดการชุดคำสั่งและประมวลผลข้อมูล

(๔) ตรวจสอบและประมวลผลข้อมูลให้แก่หน่วยงานที่ร้องขอ

๒.๕ รับผิดชอบในการศึกษา วิเคราะห์ ออกแบบ พัฒนา ปรับปรุง ควบคุมและบำรุงรักษาระบบสารสนเทศที่สนับสนุนการให้บริการประชาชนและผู้ประกอบการขนส่งทางถนน ระบบสารสนเทศที่สนับสนุนการปฏิบัติของเจ้าหน้าที่กรม กำหนดวิธีรักษาความปลอดภัยของการพัฒนาระบบสารสนเทศ ผู้รับผิดชอบ ดังนี้

หัวหน้ากลุ่มบริหารข้อมูลและระบบสารสนเทศ	นางสาวเพลินพิศ แซ่เตีย	โทร.๐๘-๖๙๐๖-๗๘๙๖
หัวหน้างานพัฒนาระบบสารสนเทศบริการ	นางสาวนภาพร โพธิ์ฉิม	โทร.๐๘-๗๗๐๔-๒๖๒๖
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายเอกพันธุ์ ศรีวงษ์	โทร.๐๙-๓๓๒๐-๖๗๐๗
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายนันทัช กวีวุฒิพันธุ์	โทร.๐๘-๓๔๔๙-๔๓๘๙
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายพิชญ์พิศุทธิ์ เรืองสว่าง	โทร.๐๘-๗๖๗๒-๑๘๒๖
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายกันตธร พูลสวัสดิ์	โทร.๐๘-๘๒๒๖-๕๒๘๒
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายยุรนันท์ สุภาวิตา	โทร.๐๘-๖๐๒๖-๘๗๕๕

มีหน้าที่รับผิดชอบ ดังนี้

(๑) ศึกษา วิเคราะห์ ออกแบบ พัฒนา ปรับปรุง ควบคุมและบำรุงรักษาระบบสารสนเทศที่สนับสนุนการดำเนินงานด้านทะเบียนและภาษีรถ ด้านใบอนุญาตขับรถและผู้ประจำรถ ด้านประกอบการขนส่ง และอื่นๆ ที่เกี่ยวข้อง กับการให้บริการประชาชนและผู้ประกอบการขนส่งทางถนน

(๒) ตรวจสอบ พัฒนาปรับปรุงโปรแกรมให้มีประสิทธิภาพและตรงตามความต้องการของหน่วยงานและผู้ใช้

(๓) กำหนดวิธีการรักษาความปลอดภัยของการพัฒนาระบบสารสนเทศ

๒.๖ รับผิดชอบในการศึกษา วิเคราะห์ออกแบบ พัฒนา ปรับปรุง ควบคุมและบำรุงรักษาระบบสารสนเทศต่างๆ ที่สนับสนุนการดำเนินงานของเจ้าหน้าที่ และผู้บริหารกรมการขนส่งทางบก และกำหนดวิธีการรักษาความปลอดภัยของการพัฒนาระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

หัวหน้ากลุ่มบริหารข้อมูลและระบบสารสนเทศ	นางสาวเพลินพิศ แซ่เตีย	โทร. ๐๘-๖๙๐๖-๗๘๙๖
หัวหน้างานพัฒนาระบบสารสนเทศบริหาร	นายพฤฒิ บุญชูวงศ์	โทร.๐๘-๖๖๙๓-๕๓๑๑
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายวลัญชน์ บุญแก้วขวัญ	โทร.๐๘-๑๔๔๖-๙๕๖๙
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายธิรเดช แสงแก้ว	โทร.๐๘-๘๘๔๑-๑๙๘๙
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นางสาวกาญจนา กิจส่งเสริมกุล	โทร.๐๘-๘๖๔๙-๕๓๖๕

มีหน้าที่รับผิดชอบ ดังนี้

(๑) ศึกษา วิเคราะห์ ออกแบบ พัฒนา ปรับปรุง ควบคุมและบำรุงรักษาระบบสารสนเทศต่างๆ ที่สนับสนุนการดำเนินงานของเจ้าหน้าที่กรม และสนับสนุนข้อมูลประกอบการตัดสินใจของผู้บริหาร

(๒) ตรวจสอบ/พัฒนา/ปรับปรุงโปรแกรมให้มีประสิทธิภาพและตรงตามความต้องการของหน่วยงาน

(๓) กำหนดวิธีรักษาความปลอดภัยของการพัฒนาระบบสารสนเทศ

๒.๗ รับผิดชอบในการศึกษา วิเคราะห์ และจัดทำแผนในการพัฒนา ปรับปรุง บำรุงรักษา และจัดทำแผนในการนำระบบภูมิสารสนเทศมาประยุกต์ใช้กับการกำหนดเส้นทางการเดินรถ การกำกับ ติดตามการประกอบการขนส่งทางถนน ระบบนำเสนอข้อมูลการดำเนินงานผ่านระบบภูมิสารสนเทศ เพื่อส่งเสริมให้การขนส่งและการจราจรทางถนนเกิดความปลอดภัยและอำนวยความสะดวกในการขนส่งทางถนน ผู้รับผิดชอบ ดังนี้

หัวหน้ากลุ่มเทคโนโลยีการขนส่งทางถนน	นายอิษฎา วิทูรากร	โทร. ๐๘-๒๐๙๔-๓๗๗๗
หัวหน้างานพัฒนาระบบภูมิสารสนเทศ	นายอัตถวิชญ์ คิมสกุลเวช	โทร. ๐๖-๑๙๕๙-๗๙๙๘
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายกฤติเดช เจิมศิริ	โทร. ๐๙-๘๕๙๗-๙๖๖๖
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นางสาวปาณิสรา ตันติกุลชาติ	โทร. ๐๙-๑๘๘๗-๐๑๒๘

มีหน้าที่รับผิดชอบ ดังนี้

(๑) การศึกษา วิเคราะห์ และจัดทำแผนในการพัฒนา ปรับปรุง บำรุงรักษา และจัดทำแผนในการนำระบบภูมิสารสนเทศมาประยุกต์ใช้กับการกำหนดเส้นทางการเดินรถ การกำกับติดตามการประกอบการขนส่งทางถนน ระบบนำเสนอข้อมูลการดำเนินงานผ่านระบบภูมิสารสนเทศ ภายใต้การกำกับ แนะนำ ตรวจสอบของผู้บังคับบัญชาในศูนย์เทคโนโลยีสารสนเทศ

(๒) นำเทคโนโลยีมาประยุกต์ใช้กับการกำกับดูแลสถานีขนส่งผู้โดยสาร สถานีขนส่งสินค้า สถานตรวจสภาพเอกชน และหน่วยงานอื่นที่เกี่ยวข้อง

(๓) กำหนดมาตรฐาน และส่งเสริมให้การขนส่งและการจราจรทางถนนเกิดความปลอดภัยและอำนวยความสะดวกในการขนส่งทางถนน

๒.๘ รับผิดชอบในการศึกษา วิเคราะห์ จัดทำแผนในการพัฒนา ปรับปรุง และบำรุงรักษา และการจัดทำแผนในการนำเทคโนโลยี RFID, GPS, Image Processing หรือเทคโนโลยีอื่นมาประยุกต์ใช้ในการปรับปรุงการขนส่งและการจราจรให้มีประสิทธิภาพ หรือที่เรียกว่าระบบการขนส่งและจราจรอัจฉริยะ (ITS) เพื่อส่งเสริมให้การขนส่งและการจราจรทางถนนเกิดความปลอดภัยและอำนวยความสะดวกในการขนส่งทางถนน ผู้รับผิดชอบ ดังนี้

หัวหน้ากลุ่มเทคโนโลยีการขนส่งทางถนน	นายอิษฎา วิทูรากร	โทร. ๐๘-๒๐๙๔-๓๗๗๗
หัวหน้างานเทคโนโลยีระบบความปลอดภัยการขนส่งทางถนน	นายศิวัช โกยทอง	โทร. ๐๘-๙๖๗๐-๙๕๒๒
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายจิรัณ บุรพรัตน์	โทร. ๐๙-๐๙๓๑-๒๕๖๐
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายแทนชนก กลั่นทิพย์	โทร. ๐๘-๗๑๖๑-๘๖๕๖

มีหน้าที่รับผิดชอบ ดังนี้

(๑) ศึกษา วิเคราะห์ จัดทำแผนในการพัฒนา ปรับปรุง และบำรุงรักษา และการจัดทำแผนในการระบุตัวตนด้วยคลื่นความถี่ (RFID) พิกัดตำแหน่ง (GPS) การประมวลผลด้วยภาพ (Image Processing) หรือเทคโนโลยีอื่นมาประยุกต์ใช้ในการปรับปรุงการขนส่งและการจราจรให้มีประสิทธิภาพ หรือที่เรียกว่าระบบการขนส่งและจราจรอัจฉริยะ (ITS) ภายใต้การกำกับ แนะนำ ตรวจสอบของผู้บังคับบัญชาในศูนย์เทคโนโลยีสารสนเทศ

(๒) บำรุงรักษาระบบสารสนเทศที่เกี่ยวข้องกับความปลอดภัยและอำนวยความสะดวกในการขนส่งทางถนน

(๓) กำหนดมาตรฐาน และส่งเสริมให้การขนส่งและการจราจรทางถนนเกิดความปลอดภัยและอำนวยความสะดวกในการขนส่งทางถนน

๒.๙ รับผิดชอบในการศึกษา วิเคราะห์ กำกับดูแล เร่งรัดและประเมินผลการดำเนินงานโครงการตามแผนแม่บทเทคโนโลยีสารสนเทศ การของบประมาณ การกำหนดมาตรฐาน การเผยแพร่ข้อมูล และการให้คำปรึกษาเกี่ยวกับการจัดทำแผนงาน/โครงการ การของบประมาณด้านเทคโนโลยีสารสนเทศ รวบรวม ติดตาม พิจารณา โครงการและนำเสนอคณะกรรมการบริหารและจัดหาคอมพิวเตอร์กระทรวงคมนาคม ผู้รับผิดชอบ ดังนี้

หัวหน้ากลุ่มนโยบายและมาตรฐานเทคโนโลยีสารสนเทศ	นางสาวพนิดา อุตสาหภูมิ	โทร. ๐๘-๗๑๑๓-๗๒๒๓
หัวหน้างานนโยบายและแผนงานเทคโนโลยีสารสนเทศ	นางวรรณี บุญทาเลิศ	โทร. ๐๘-๖๘๙๔-๓๕๕๐
นักวิชาการคอมพิวเตอร์ชำนาญการ	นางสุรัสวดี รัศมีรณชัย	โทร. ๐๘-๖๓๕๓-๗๔๗๗
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นางสาวศุภวรรณ เรืองวิลัย	โทร. ๐๘-๖๕๕๔-๘๖๐๙
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ว่าที่ร้อยตรีเพชระ อินทานนท์	โทร. ๐๘-๗๕๕๘-๘๕๐๔
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายอติพล ลิ้มสุวรรณ	โทร. ๐๘-๕๑๙๗-๑๗๑๕

มีหน้าที่ความรับผิดชอบ ดังนี้

(๑) ศึกษา วิเคราะห์ กำกับดูแล เร่งรัดติดตามและประเมินผลการดำเนินงานโครงการตามแผนแม่บทเทคโนโลยีสารสนเทศ หรือแผนดิจิทัลของกรม

(๒) เสนอของบประมาณ ของศูนย์เทคโนโลยีสารสนเทศ และการให้คำปรึกษาเกี่ยวกับการจัดทำแผนงาน/โครงการ ในการของบประมาณด้านเทคโนโลยีสารสนเทศ

(๓) กำหนดมาตรฐาน การเผยแพร่ รวบรวม ติดตาม พิจารณาโครงกรและนำเสนอคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ กระทรวงคมนาคม

(๔) รวบรวม ติดตามการดำเนินการบำรุงรักษาระบบสารสนเทศและการเช่าระบบสื่อสารข้อมูล

๒.๑๐ รับผิดชอบในการประเมินความเสี่ยง การควบคุมภายใน การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร การจัดทำข้อตกลงและกำหนดมาตรฐานการเชื่อมโยงข้อมูลกับหน่วยงานภายนอก การดำเนินงานแผนการฝึกอบรมบุคลากรของศูนย์เทคโนโลยีสารสนเทศ การพัฒนาระบบการจัดเก็บองค์ความรู้ และระบบเรียนรู้ด้านเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ดังนี้

หัวหน้ากลุ่มนโยบายและมาตรฐานเทคโนโลยีสารสนเทศ	นางสาวพนิดา อุตสาหภูมิ	โทร. ๐๘-๗๑๑๓-๗๒๒๓
หัวหน้างานมาตรฐานและความปลอดภัยเทคโนโลยีสารสนเทศ	นางสาวประภัสสร กิตติวโรดม	โทร. ๐๖-๒๗๔๕-๗๖๖๖
นักวิชาการคอมพิวเตอร์ชำนาญการ	นางสาวศิญาภัสร์ มั่นคงธิติวัฒน์	โทร. ๐๘-๖๕๐๐-๙๕๔๔
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นายพงศ์พิสุทธิ์ ธีระชัย	โทร. ๐๘-๐๐๔๗-๒๕๒๕
นักวิชาการคอมพิวเตอร์ปฏิบัติการ	นางสาวกนกวรรณ ชำนาญจุ้ย	โทร. ๐๘-๖๙๒๙-๒๒๕๒

มีหน้าที่รับผิดชอบ ดังนี้

(๑) ประเมินความเสี่ยง การควบคุมภายใน การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

(๒) จัดทำความตกลงและกำหนดมาตรฐานการเชื่อมโยงข้อมูลกับหน่วยงานภายนอก

(๓) ดำเนินงานแผนการฝึกอบรมบุคลากรของศูนย์เทคโนโลยีสารสนเทศ

(๔) การพัฒนาระบบการจัดเก็บองค์ความรู้ และระบบการเรียนรู้ด้านเทคโนโลยีสารสนเทศ

(๕) จัดให้มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางบก อย่างน้อยปีละ ๑ ครั้ง

๒.๑๑ รับผิดชอบในงานธุรการ การรับส่งหนังสือ งานสารบรรณ งานประชาสัมพันธ์ และเผยแพร่การปฏิบัติงาน ติดต่อ ประสานและให้บริการทั่วไป ดำเนินการเกี่ยวกับพัสดุครุภัณฑ์องศูนย์เทคโนโลยีสารสนเทศ ควบคุมการเข้า - ออกของบุคคลภายนอก จัดทำรายงานติดตามสรุปผลเร่งรัดผลการปฏิบัติงานตามแผนงานโครงการ และงานธุรการอื่นๆ มีผู้รับผิดชอบ ดังนี้

หัวหน้างานบริหารงานทั่วไป	นางภัทรานิษฐ์ รชตะจีระพัฒน์	โทร. ๐๙-๙๐๕๙-๓๖๕๙
เจ้าพนักงานธุรการชำนาญงาน	นางสาวศิริวรรณ์ อุดมสวัสดิ์	โทร. ๐๖-๒๒๔๒-๔๙๘๗
เจ้าพนักงานธุรการปฏิบัติงาน	นางสาวสมฤดี อ่อนไทย	โทร. ๐๘-๕๕๙๒-๑๖๖๕
เจ้าหน้าที่บันทึกข้อมูล	นางสาวสุนทรีย์ สมพงษ์	โทร. ๐๘-๐๕๘๘-๗๕๕๑
เจ้าหน้าที่บันทึกข้อมูล	นางสาวมณีรัตน์ สุขชัยศรี	โทร. ๐๘-๓๗๖๖-๕๙๕๓

มีหน้าที่รับผิดชอบ ดังนี้

(๑) กำกับดูแลงานธุรการ งานสารบรรณ งานประชาสัมพันธ์และเผยแพร่การปฏิบัติงาน ของศูนย์เทคโนโลยีสารสนเทศ

(๒) ตรวจสอบ กำกับ ดูแล พัสดุ ครุภัณฑ์และการใช้ทรัพย์สินต่างๆ ภายในศูนย์เทคโนโลยีสารสนเทศ

(๓) กำกับ ดูแล การเข้า – ออก การขอใช้พื้นที่ต่างๆ ของบุคคลภายนอกที่เข้ามาติดต่อราชการกับศูนย์เทคโนโลยีสารสนเทศ

(๔) การจัดทำคำรับรองรายงานการปฏิบัติราชการของศูนย์เทคโนโลยีสารสนเทศ

(๕) จัดทำรายงานการประชุมต่างๆ ของศูนย์เทคโนโลยีสารสนเทศ

(๖) จัดทำสรุปรายงานการปฏิบัติราชการ กิจกรรมการลาพักผ่อน ลาป่วย และภารกิจที่เกี่ยวกับเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ

แผนแก้ไขปัญหาจากสถานการณ์ ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)

๑. บทนำ

ปัจจุบัน หน่วยงานทั้งภาครัฐและภาคเอกชนมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์การ การบริหารจัดการองค์การ และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มขึ้น ดังนั้นองค์การจำเป็นจะต้องมีการบริหารจัดการ เฝ้าระวัง และดูแลรักษาฐานข้อมูลและระบบสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการนำข้อมูลดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

กรมการขนส่งทางบก เป็นหน่วยงานราชการหนึ่งที่ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการประชาชนได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากภัยพิบัติตามธรรมชาติ หรือจากการถูกโจมตีจากบุคคล จากปัญหาระบบไฟฟ้า หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศและส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) เพื่อรับมือกับสถานการณ์ต่างๆ ที่อาจจะเกิดขึ้น

๒. วัตถุประสงค์

๑. เพื่อให้สามารถรับมือกับเหตุการณ์ที่ทำให้ระบบงานสำคัญหยุดชะงักได้อย่างมีประสิทธิภาพและประสิทธิผล รวมทั้งสามารถกู้คืนระบบงานเพื่อให้กลับคืนมาภายในระยะเวลาที่กำหนดไว้

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบสารสนเทศให้มีเสถียรภาพ มีความพร้อมสำหรับใช้งาน และเฝ้าระวังความเสี่ยงใหม่ๆ ที่อาจเกิดขึ้นได้ตลอดเวลา

๓. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๕. เพื่อจัดให้มีการบริหารและจัดการความเสี่ยงที่มีต่อระบบงานสำคัญ อันจะก่อให้เกิดการหยุดชะงักของระบบได้

๖. เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทาธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๗. สร้างกรอบและแนวทางในการดำเนินงานให้แก่บุคลากรในองค์กร เพื่อให้สามารถบริหาร จัดการความไม่แน่นอนที่จะเกิดขึ้นกับองค์กรได้อย่างเป็นระบบและมีประสิทธิภาพ

๓. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของกรมการขนส่งทางบกมีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาและลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศกรมการขนส่งทางบกเป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

กรมการขนส่งทางบกจึงได้วิเคราะห์ความเสี่ยงที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของกรมการขนส่งทางบก แบ่งได้ดังนี้

๑. ความเสี่ยงทางด้านเทคนิค ที่เกิดจากระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสารข้อมูล และอุปกรณ์คอมพิวเตอร์ต่างๆ ขัดข้อง อาจเนื่องด้วยสาเหตุของการถูกก่อกวน หรือโจมตี จากผู้ไม่ประสงค์ดี หรือด้วยความรู้เท่าไม่ถึงการณ์ของเจ้าหน้าที่ผู้ปฏิบัติงาน

๒. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน หรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง

๓. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมการขนส่งทางบกมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมการขนส่งทางบก

๔. ขอบเขตการดำเนินงานของแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

ในการใช้งานแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ มีขอบเขตที่กำหนดไว้ ดังนี้

๑. แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัตินี้ครอบคลุมเฉพาะเหตุการณ์ ดังต่อไปนี้

๑.๑ ความเสี่ยงทางด้านเทคนิค

- กรณีโดนเจาะระบบ
- กรณีเครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง
- กรณีระบบเครือข่ายสื่อสารขัดข้อง

๑.๒ ความเสี่ยงทางด้านภัยหรือสถานการณ์ฉุกเฉิน

- กรณีไฟดับ
- กรณีไฟไหม้
- กรณีน้ำท่วม

- ลิฟต์โดยสารขัดข้อง

๒. ระบบงานสำคัญที่จะต้องดำเนินการ ประกอบด้วย

(๑) ระบบงานทะเบียนและภาษีรถยนต์และรถขนส่ง

(๒) ระบบงานใบอนุญาตขับรถและผู้ประจำรถและระบบพิมพ์บัตรพลาสติก

(๓) ระบบงานใบอนุญาตประกอบการขนส่ง

(๔) ระบบงานโครงข่ายเส้นทางและเงื่อนไขการเดินรถ

(๕) ระบบงานใบอนุญาตประกอบการรถรับจ้างและบริการ

(๖) ระบบงานการเงิน บัญชี งบประมาณ

(๗) ระบบงานควบคุมพัสดุและครุภัณฑ์

(๘) ระบบงานควบคุมบัญชีรถและเครื่องยนต์

(๙) ระบบรับรองเครื่องบันทึกข้อมูลการเดินทางของรถ

(๑๐) ระบบงานเพื่อให้บริการแบบ e-Service

(๑๑) ระบบตรวจสภาพรถเอกชน (ตรอ.)

(๑๒) ระบบบริหารจัดการเดินรถด้วยระบบ GPS

(๑๓) ระบบเปรียบเทียบปรับทั่วไทย

(๑๔) ระบบบริหารทรัพยากรบุคคล

(๑๕) ระบบรับเรื่องร้องเรียน ๑๕๘๔

(๑๖) ระบบแผนที่ข้อมูล

(๑๗) ระบบงานสารบรรณ

(๑๘) ระบบงานสถิติการขนส่ง

๓. ระยะเวลาที่ไม่สามารถให้บริการระบบงานสำคัญเกินกว่า ๖ ชั่วโมง

๔. เจาะระบบ หมายถึง เหตุการณ์ที่ระบบถูกเปลี่ยนแปลง เครื่องคอมพิวเตอร์แม่ข่ายเสียหาย อันเกิดจากผู้ไม่ประสงค์ดีเข้ามาทำลายระบบ หรือทำความเสียหายต่อข้อมูล

๕. เครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายสื่อสารขัดข้อง หมายถึง เหตุการณ์ที่เครื่องคอมพิวเตอร์แม่ข่ายระบบเครือข่ายสื่อสาร และอุปกรณ์อื่นๆ ที่เกี่ยวข้อง ไม่สามารถใช้งานได้

๖. ไฟดับ หมายถึง เหตุการณ์ที่ไฟดับหรือระบบไฟขัดข้องทำให้ไม่มีไฟหล่อเลี่ยงระบบและอุปกรณ์ในห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) และห้องเครือข่ายสื่อสาร (Network Room) และ DLT SYSTEM CONTROL (ห้อง LAN Network Room, WAN Network Room และ Server Room) ณ อาคาร ๙ ชั้น ๒ ศูนย์เทคโนโลยีสารสนเทศ ขัดข้อง

๗. ไฟไหม้ หมายถึง เหตุการณ์ที่ทำให้เกิดประกายไฟ หรือกลุ่มควันที่ลุกลามเป็นเพลิงไหม้หรือก่อให้เกิดความเสียหายต่อห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) ห้องเครือข่ายสื่อสาร (Network Room) และอุปกรณ์คอมพิวเตอร์ โดยจะต้องดำเนินการปรับปรุง/แก้ไขห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) ห้องเครือข่ายสื่อสาร (Network Room) และจัดซื้อจัดหาอุปกรณ์คอมพิวเตอร์ใหม่ สำหรับติดตั้ง ณ ศูนย์เทคโนโลยีสารสนเทศ ห้อง LAN Network Room, WAN Network Room และ Server Room ณ อาคาร ๙ ชั้น ๒

๘. น้ำท่วมหรืออุทกภัย หมายถึง ภัยที่เกิดขึ้นเนื่องจากมีน้ำเป็นสาเหตุ อาจจะเป็นน้ำท่วมขัง น้ำป่า หรืออื่นๆ โดยปกติ อุทกภัยเกิดจากฝนตกหนักต่อเนื่องกันเป็นเวลานาน บางครั้งทำให้เกิดแผ่นดินถล่ม อาจมีสาเหตุจากพายุหมุนเขตร้อน ลมมรสุมมีกำลังแรง ร่องความกดอากาศต่ำมีกำลังแรง อากาศแปรปรวน น้ำทะเลหนุน เขื่อนพัง ทำให้เกิดอุทกภัยได้เสมอ

๙. ภัยพิบัติอื่นๆ เช่น แผ่นดินไหว อาคารทรุด เกิดการประท้วง การจลาจล ภาวะโรคระบาด เป็นต้น และเป็นเหตุให้ไม่สามารถเข้าดำเนินงานหรือปฏิบัติงานได้ตามปกติ

๑๐. แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัตินี้ ให้ความสำคัญกับทีมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ดังนั้นบุคลากรส่วนใหญ่หรือทั้งหมดจะต้องอยู่ครบหรือมอบหมายผู้เกี่ยวข้อง เพื่อให้การแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัตินี้ ประสิทธิภาพและประสิทธิผล

๑๑. หากเกิดภัยพิบัติในช่วงนอกเวลาราชการหรือในวันหยุดราชการ แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติอาจไม่สามารถปฏิบัติได้หรืออาจไม่สัมฤทธิ์ผลเท่าที่ควร

๑๒. ในแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฉบับนี้ สถานที่สำรองข้อมูล (Backup Site) ตั้งอยู่ที่อาคารระบบข้อมูลกลางและสำรองข้อมูล สำนักงานขนส่งจังหวัดนนทบุรี

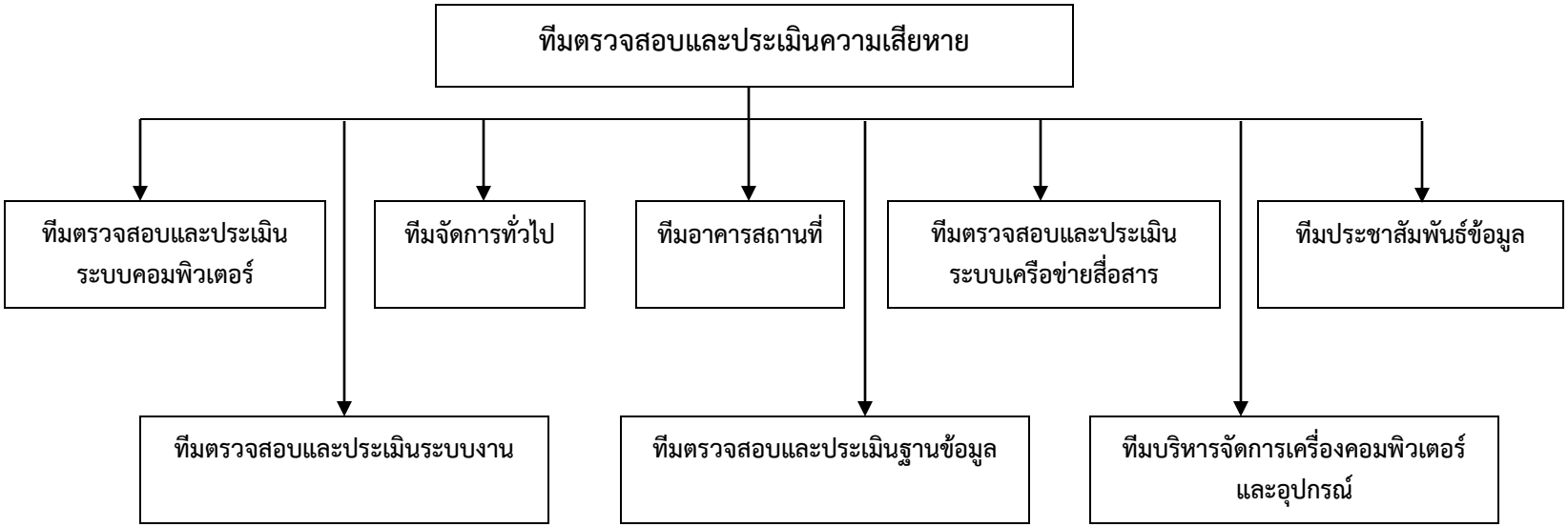
๑๓. แต่ละทีมย่อยของทีมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ สามารถใช้บุคลากรร่วมกันได้

๕. ผู้รับผิดชอบและหน้าที่ของทีมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

ศูนย์เทคโนโลยีสารสนเทศ ได้แต่งตั้งทีมงานในการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่างๆ ที่อาจจะเกิดขึ้นกับระบบสารสนเทศของกรมการขนส่งทางบก ประกอบไปด้วยทีมย่อยที่เกี่ยวข้องจำนวน ๘ ทีม ดังนี้

ทีมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

Organization Chart



ทีมตรวจสอบและประเมินความเสียหาย

หัวหน้าทีม : ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

ทีมงาน : หัวหน้ากลุ่มนโยบายและมาตรฐานเทคโนโลยีสารสนเทศ
หัวหน้ากลุ่มบริหารข้อมูลและระบบสารสนเทศ
หัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย
หัวหน้ากลุ่มเทคโนโลยีการขนส่งทางถนน

หน้าที่รับผิดชอบ

๑. ทำหน้าที่ควบคุม กำหนด สั่งการ คณะทำงานที่เกี่ยวข้อง ดำเนินการตามขั้นตอนที่กำหนด
๒. รายงานปัญหา และวิธีการแก้ไขปัญหาที่เกิดขึ้นให้ผู้บริหารรับทราบ

ทีมตรวจสอบและประเมินระบบคอมพิวเตอร์

หัวหน้าทีม : หัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย

ทีมงาน : หัวหน้างานระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย
นายศุภชัย พลโก
นายโชคอำนวย เถื่อนสันเทียะ
นายจักริน ไอศุริยสมบัติ

หน้าที่รับผิดชอบ :

๑. ตรวจสอบความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ โดยมุ่งเน้นที่เครื่องคอมพิวเตอร์แม่ข่ายหลักของกรมฯ พร้อมประเมินความเสียหาย วิธีการ และระยะเวลาที่จะทำให้ระบบสามารถใช้งานได้ปกติ
๒. จัดทำสรุปผลการตรวจสอบความเสียหายและเสนอแนวทางการดำเนินงานในแต่ละด้าน เสนอผู้บริหารและผู้เกี่ยวข้องดำเนินการแก้ไข

ทีมอาคาร สถานที่

หัวหน้าทีม : หัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย

ทีมงาน : หัวหน้างานระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย
นายศุภชัย พลโก
นายโชคอำนวย เถื่อนสันเทียะ

หน้าที่รับผิดชอบ :

๑. จัดเตรียมพื้นที่ต่างๆ รวมถึงระบบไฟฟ้าและสื่อสารต่างๆ ณ Backup Site เพื่อให้พร้อมใช้งาน
๒. ประสานสำนักเลขานุการกรม เพื่อตรวจสอบความเสียหายของสถานที่ และร่วมประเมินความเสียหาย
๓. ดูแลการซ่อมแซมหรือก่อสร้างศูนย์เทคโนโลยีสารสนเทศ อาคาร ๙ ที่เกิดความเสียหายขึ้นใหม่
๔. ตรวจสอบความพร้อมและการทำงานของอุปกรณ์สำรองไฟฟ้า (UPS) และอุปกรณ์เครื่องปั่นไฟ (Generator)
๕. รักษาความปลอดภัยในบริเวณที่ต้องมีการควบคุมต่างๆ

ทีมตรวจสอบและประเมินระบบเครือข่าย

หัวหน้าทีม: หัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย

ทีมงาน : หัวหน้างานระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย
นายศุภชัย พลโก
นายโชคอำนวย เถื่อนสันเทียะ
นายจักริน ไอศุริยสมบัติ

หน้าที่รับผิดชอบ

๑. ประเมิน ตรวจสอบ ความเสียหายที่เกิดขึ้น
๒. ให้ข้อมูลที่จำเป็นเพื่อจัดหาอุปกรณ์ที่สำคัญเพื่อให้ทีมจัดการทั่วไปดำเนินการจัดหาอุปกรณ์
๓. ประเมินระยะเวลาในการซ่อมแซมหรือเปลี่ยนทดแทนทรัพย์สินสารสนเทศที่เกิดความเสียหาย
๔. ติดตั้งระบบคอมพิวเตอร์และเครือข่าย ให้สามารถใช้งานได้ดังเดิม
๕. ดูแลกู้คืนระบบคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ให้สามารถใช้งานได้
๖. ประสานงานกับทีมอาคารสถานที่ในการแก้ปัญหา

ทีมตรวจสอบและประเมินฐานข้อมูล

หัวหน้าทีม : หัวหน้ากลุ่มบริหารข้อมูลและระบบสารสนเทศ

ทีมงาน : หัวหน้างานบริหารฐานข้อมูล
นางสาวรัชชาภรณ์ สกุลพราหมณ์
นายวีระพงษ์ จันทร์วงศ์
นาวสาวธนพร แสงอินทร์
นายวโรภาส วุ่นศรี

หน้าที่รับผิดชอบ :

๑. ตรวจสอบความเสียหายของฐานข้อมูล
๒. ตรวจสอบความครบถ้วนของฐานข้อมูล
๓. ร่วมมือกับทีมกู้คืนและติดตั้งระบบคอมพิวเตอร์และเครือข่าย ทีมตรวจสอบและประเมินระบบงาน ในการทดสอบระบบภายหลังจากการกู้คืน

ทีมตรวจสอบและประเมินระบบงาน

หัวหน้าทีม : หัวหน้ากลุ่มบริหารข้อมูลและระบบสารสนเทศ

ทีมงาน : หัวหน้างานพัฒนาระบบสารสนเทศบริการ
หัวหน้างานพัฒนาระบบสารสนเทศบริหาร
นายนันทัช กวีวุฒิพันธุ์
นายเอกพันธุ์ ศรีวงษ์
นายพิชญ์พิศุทธิ์ เรืองสว่าง
นายกันตธร พูลสวัสดิ์

นายยุรนันท์ สุภาวิตา
นายพฤฒิ บุญชูวงศ์
นายวลัญชน์ บุญแก้วขวัญ
นายธิรเดช แสงแก้ว
นางสาวกาญจนา กิจส่งเสริมกุล

หน้าที่รับผิดชอบ :

๑. ตรวจสอบความเสียหายของระบบงาน และระบบสารสนเทศอื่น ๆ ที่อยู่ในความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศ
๒. ตรวจสอบความครบถ้วนของระบบงานที่กู้คืน
๓. ร่วมมือกับทีมกู้คืนและติดตั้งระบบคอมพิวเตอร์และเครือข่าย ทีมตรวจสอบและประเมินฐานข้อมูลในการทดสอบระบบภายหลังจากการกู้คืน
๔. ทดสอบระบบงานร่วมกับผู้ใช้งาน

ทีมบริหารจัดการเครื่องคอมพิวเตอร์และอุปกรณ์

หัวหน้าทีม : หัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย
ทีมงาน : หัวหน้างานสนับสนุนระบบสารสนเทศ
นายทวีป นาคงาม
นายกิตติชัย เกษลา
นายณัฐพล นกดี

หน้าที่รับผิดชอบ :

๑. แก้ไขปัญหาที่เกิดขึ้นกับเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้อง
๒. หากมีอุปกรณ์เสียหาย จัดทำรายละเอียดเพื่อของงบประมาณในการซ่อมแซมหรือจัดหาใหม่

ทีมประชาสัมพันธ์ข้อมูล

หัวหน้าทีม : หัวหน้ากลุ่มบริหารระบบคอมพิวเตอร์และเครือข่าย
ทีมงาน : หัวหน้างานสนับสนุนระบบสารสนเทศ
นางสาวชนิดา เจริญสมบัติอมร
นายทวีป นาคงาม
นายกิตติชัย เกษลา

หน้าที่รับผิดชอบ :

แจ้งรายละเอียด สาเหตุ และระยะเวลาในการแก้ไขปัญหา กรณีไม่สามารถใช้งานระบบคอมพิวเตอร์และเครือข่ายให้ผู้ใช้งานทั้งส่วนกลางและส่วนภูมิภาคทราบ

ทีมจัดการทั่วไป

หัวหน้าทีม : หัวหน้ากลุ่มนโยบายและมาตรฐานเทคโนโลยีสารสนเทศ

ทีมงาน : หัวหน้างานบริหารงานทั่วไป
หัวหน้างานนโยบายและแผนงานเทคโนโลยีสารสนเทศ
หัวหน้างานมาตรฐานและความปลอดภัยเทคโนโลยีสารสนเทศ
นางสาวศิริวรรณ์ อุดมสวัสดิ์
นางสาวพิชญ์สิณี มาลา
นางสาวสมฤดี อ่อนไทย
นางสาวศิญาภัสร์ มั่งคงธิติวัฒน์
นางสุรัสวดี รัศมีรณชัย
นางสาวศุภวรรณ เรืองวิลัย
นางสาวกนกวรรณ ชำนาญจุ้ย
นายพงศ์พิสุทธิ์ ธีระชัย
ว่าที่ร้อยตรีเพชระ อินทานนท์
นายอติพล ลิ้มสุวรรณ

หน้าที่รับผิดชอบ :

๑. ประสานและจัดการงานทั่วไป เกี่ยวกับการจัดหาอุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติงาน
๒. ช่วยดำเนินการด้านการของบประมาณในการจัดหาอุปกรณ์และซอร์ฟแวร์ต่างๆ ที่จำเป็นต่อการกู้คืนระบบ
๓. ช่วยจัดทำเอกสารต่างๆ ที่เกี่ยวข้อง
๔. ให้ความช่วยเหลือทีมอื่นๆ

๖. สถานที่สำรองข้อมูล (Backup Site)

สถานที่สำรองข้อมูล (Backup Site) ตั้งอยู่ที่อาคารระบบข้อมูลกลางและสำรองข้อมูล สำนักงานขนส่งจังหวัดนนทบุรี ซึ่งมีอุปกรณ์คอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้อง ดังนี้

ลำดับที่	เครื่องคอมพิวเตอร์แม่ข่าย (Server) /อุปกรณ์เครือข่าย	จำนวน	ยี่ห้อ/รุ่น
๑	เครื่องคอมพิวเตอร์แม่ข่าย (Database Server)	๑ เครื่อง	ยี่ห้อ IBM รุ่น p๖๘๐
๒	เครื่องคอมพิวเตอร์แม่ข่าย (Application Server)	๓ เครื่อง	ยี่ห้อ IBM รุ่น p๖๖๐
๓	เครื่องคอมพิวเตอร์แม่ข่าย (Web Server)	๑ เครื่อง	ยี่ห้อ IBM รุ่น Xseries ๓๔๖
๔	เครื่องคอมพิวเตอร์แม่ข่าย (Report Server)	๔ เครื่อง	ยี่ห้อ IBM รุ่น Xseries ๓๔๖
๕	เครื่องคอมพิวเตอร์แม่ข่าย (MOI Broker)	๒ เครื่อง	ยี่ห้อ IBM รุ่น Xseries ๓๐๖m

ลำดับที่	เครื่องคอมพิวเตอร์แม่ข่าย (Server) /อุปกรณ์เครือข่าย	จำนวน	ยี่ห้อ/รุ่น
๖	อุปกรณ์จัดเก็บข้อมูล (SAN)	๑ เครื่อง	ยี่ห้อ IBM รุ่น Fast T๕๐๐
๗	อุปกรณ์ Main Gigabit Switch	๒ เครื่อง	ยี่ห้อ Cisco รุ่น Catalyst ๔๕๐๑R
๘	อุปกรณ์ Switch Routing	๒ เครื่อง	ยี่ห้อ Cisco รุ่น CS - 4948
๙	อุปกรณ์ Database Switch	๒ เครื่อง	ยี่ห้อ D - Link รุ่น DGS - 3308FG/TG
๑๐	อุปกรณ์ Application Switch (Load Balance)	๑ เครื่อง	Load Balance รุ่น BIG - IP 2400
๑๑	อุปกรณ์ Firewall	๑ เครื่อง	ยี่ห้อ Fortinet รุ่น Fortigate 800A
๑๒	อุปกรณ์ Router Type 2	๑ เครื่อง	ยี่ห้อ Cisco รุ่น CS - 2811
๑๓	อุปกรณ์ Main Router	๑ เครื่อง	ยี่ห้อ Cisco รุ่น CS - 7204VXR
๑๔	ระบบไฟฟ้า และระบบปรับอากาศ	๑ ระบบ	

๖.๑ การตรวจสอบความพร้อมใช้งานของสถานที่สำรองข้อมูล (Backup Site)

ดำเนินการตรวจสอบความพร้อมใช้งานของสถานที่สำรองข้อมูล (Backup Site) มีรายละเอียดในการตรวจสอบ ดังนี้

๑) ความพร้อมใช้งานของสถานที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายและอุปกรณ์ที่เกี่ยวข้อง โดยดำเนินการตรวจสอบเดือนละ ๑ ครั้ง

(๑) ระบบไฟฟ้า

(๒) ระบบปรับอากาศ

๒) ความพร้อมใช้งานของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์ที่เกี่ยวข้อง โดยดำเนินการตรวจสอบสัปดาห์ละ ๑ ครั้ง

(๑) ระบบงานที่อยู่ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) แต่ละเครื่อง

(๒) สถานะของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์

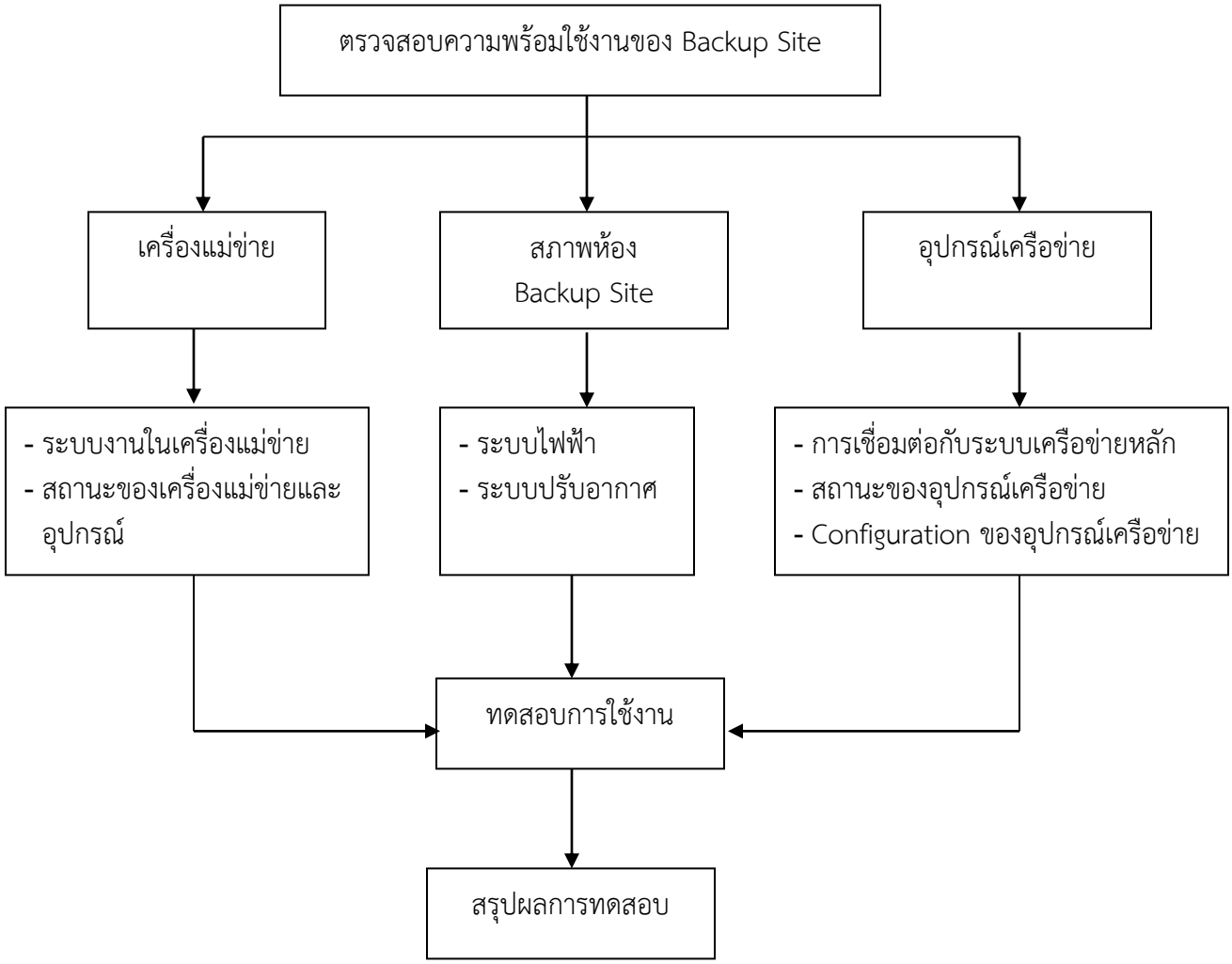
๓) ความพร้อมใช้งานของอุปกรณ์เครือข่าย โดยดำเนินการตรวจสอบสัปดาห์ละ ๑ ครั้ง

(๑) การเชื่อมต่อกับระบบเครือข่ายหลัก

(๒) สถานะของอุปกรณ์เครือข่า

(๓) Configuration ของอุปกรณ์เครือข่าย

ขั้นตอนการตรวจสอบความพร้อมใช้งาน Backup Site



กระบวนการการตรวจสอบความพร้อมใช้งานของสถานที่สำรองข้อมูล (Backup Site)

ขั้นตอน	ระยะเวลาในการดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
กระบวนการตรวจความพร้อมใช้งานของสถานที่สำรองข้อมูล (Backup Site)		ทีมอาคาร สถานที่	มีการบำรุงรักษาอุปกรณ์
๑. ตรวจสอบความพร้อมใช้งานของห้อง	๔ ชั่วโมง	ทีมตรวจสอบและประเมิน	ที่ติดตั้ง ณ อาคารระบบ
๑.๑ ระบบไฟฟ้า		ระบบคอมพิวเตอร์	ข้อมูลกลางและสำรอง
๑.๒ ระบบปรับอากาศ		ทีมตรวจสอบและประเมิน	ข้อมูล (Backup Site)
๒. ตรวจสอบความพร้อมใช้งานของเครื่องคอมพิวเตอร์แม่ข่าย	๒ ชั่วโมง	ระบบเครือข่าย	
๒.๑ ระบบงานของเครื่องคอมพิวเตอร์แม่ข่าย (Server) แต่ละเครื่อง			
๒.๒ สถานะของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์			
๓. ตรวจสอบความพร้อมใช้งานของอุปกรณ์และระบบเครือข่าย	๒ ชั่วโมง		
๓.๑ การเชื่อมต่อกับระบบเครือข่ายหลัก			
๓.๒ สถานะของอุปกรณ์เครือข่าย			
๓.๓ Configuration ของอุปกรณ์เครือข่าย			
๔. ทดสอบการใช้งานของทุกระบบ	๒-๔ ชั่วโมง		
๕. รายงานผลการตรวจสอบอุปกรณ์	๒-๔ ชั่วโมง		

๖.๒ ระยะเวลาในการสำรองข้อมูล (Backup Data) ระบบงาน

๑) ทำการสำรองข้อมูลตามคำร้องของผู้ดูแลฐานข้อมูล โดยผู้ดูแลระบบเป็นผู้ดำเนินการ

๒) ทำการสำรองข้อมูลทั้งหมดของระบบฐานข้อมูล (Full Backup) ทุกวันทำการ

๓) ทำการสำรองข้อมูลไปยังอาคารระบบข้อมูลกลางและสำรองข้อมูล โดยข้อมูลจะทำการอัพเดท ภายหลังเวลา ๑๘.๐๐ น. ของทุกวัน ประกอบด้วยระบบงานที่สำคัญ ดังนี้

(๓.๑) ระบบงานทะเบียนและภาษีรถยนต์และรถขนส่ง

(๓.๒) ระบบงานใบอนุญาตขับรถและผู้ประจำรถ

(๓.๓) ระบบงานใบอนุญาตประกอบการ

(๓.๔) ระบบงานการเงิน บัญชี งบประมาณ

(๓.๕) ระบบงานควบคุมพัสดุและครุภัณฑ์

(๓.๖) ระบบงานสถิติการขนส่ง

(๓.๗) ระบบงานข้อกำหนดการขนส่ง

(๓.๘) ระบบสารบรรณ

๗. แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฉบับนี้แสดงถึงขั้นตอนในการป้องกันจากเหตุการณ์ภัยพิบัติที่สามารถทำลายหรือก่อให้เกิดความเสียหายอย่างสูงต่อระบบเทคโนโลยีสารสนเทศ ซึ่งตั้งอยู่ที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) และห้องเครือข่ายสื่อสาร (Network Room) อาคาร ๙ ชั้น ๒ ศูนย์เทคโนโลยีสารสนเทศ และห้อง DLT SYSTEM CONTROL ซึ่งประกอบด้วย ห้อง LAN Network Room, WAN Network Room และ Server Room สถานที่ปฏิบัติงานของบุคลากรศูนย์เทคโนโลยีสารสนเทศ ระบบไฟฟ้า ระบบลิฟต์โดยสาร ที่ติดตั้งอยู่ ณ อาคาร ๙ ศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบก ๑๐๓๒ ถนนพหลโยธิน แขวงจอมพล เขตจตุจักร กรุงเทพมหานคร ๑๐๙๐๐ โดยรายละเอียดของแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) ที่จัดทำขึ้นจะกล่าวถึง การเตรียมความพร้อมในด้านต่างๆ ก่อนเกิด ขณะเกิดและหลังเกิดภัยพิบัติ กับระบบสารสนเทศของกรมการขนส่งทางบก โดยมีรายละเอียดและวิธีการดังต่อไปนี้

๗.๑ ก่อนเกิดเหตุการณ์ภัยพิบัติ

๑. <u>จัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ</u>

ในแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ จะแสดงขั้นตอนที่เกี่ยวข้องทั้งหมดในการแก้ไขปัญหาที่เกิดขึ้น ซึ่งประกอบไปด้วย ๖ เหตุการณ์คือ โดนเจาะระบบ เครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายสื่อสารขัดข้อง ไฟดับ ไฟไหม้ น้ำท่วม และลิฟต์โดยสารขัดข้อง

๒. <u>จัดเตรียมสถานที่สำรองข้อมูล (Backup Site) และตรวจสอบความพร้อมใช้งาน</u>

สถานที่สำรองข้อมูล (Backup Site) ตั้งอยู่ที่อาคารระบบข้อมูลกลางและสำรองข้อมูล สำนักงานขนส่งจังหวัดนนทบุรีโดยตรวจสอบความพร้อมใช้งาน ดังนี้

(๑) จัดเตรียมและตรวจสอบความพร้อมใช้งานของสถานที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายและอุปกรณ์ ที่เกี่ยวข้อง โดยดำเนินการตรวจสอบเดือนละ ๑ ครั้ง ประกอบด้วย

- ระบบไฟฟ้า

- ระบบปรับอากาศ
- ระบบแจ้งเตือนอัตโนมัติ (Tele Alarm)
- ระบบควบคุมการเข้า-ออก (Access Control)

(๒) ความพร้อมใช้งานของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์ที่เกี่ยวข้อง โดยดำเนินการตรวจสอบสัปดาห์ละ ๑ ครั้ง ประกอบด้วย

- ระบบงานที่อยู่ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) แต่ละเครื่อง
- สถานะของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์

(๓) ความพร้อมใช้งานของอุปกรณ์เครือข่าย โดยดำเนินการตรวจสอบสัปดาห์ละ ๑ ครั้ง ประกอบด้วย

- การเชื่อมต่อกับระบบเครือข่ายหลัก
- สถานะของอุปกรณ์เครือข่าย
- Configuration ของอุปกรณ์เครือข่าย

๓. <u>การสำรองข้อมูลของระบบ</u>

การสำรองข้อมูลของระบบ จะทำการสำรองข้อมูลแยกออกเป็น ๓ ส่วนคือ

<u>ส่วนที่ ๑</u> ทำการสำรองข้อมูลตามคำร้องของผู้ดูแลฐานข้อมูล โดยผู้ดูแลระบบเป็นผู้ดำเนินการ

<u>ส่วนที่ ๒</u> ทำการสำรองข้อมูลทั้งหมดของระบบฐานข้อมูล (Full Backup) ทุกวันทำการ โดยข้อมูลที่ทำการสำรองแล้วจะจัดเก็บในรูปแบบของเทป (Tape Backup) จำนวน ๑ ชุด (มีเทปสำหรับหมุนเวียนในการใช้สำรองข้อมูล จำนวน ๕ ชุด) จัดเก็บไว้ที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) อาคาร ๔ ชั้น ๖ ศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบก

<u>ส่วนที่ ๓</u> ทำการสำรองข้อมูลของฐานข้อมูลโดยอัตโนมัติไปยังอาคารระบบข้อมูลกลางและสำรองข้อมูล สำนักงานขนส่งจังหวัดนนทบุรี โดยจะทำการอัพเดทข้อมูลหลัง ๑๘.๐๐ น. ของทุกวัน

๒. <u>ระบบสำรองไฟฟ้า</u>

ทำการตรวจสอบความพร้อมใช้งานของอุปกรณ์สำรองไฟฟ้า และเครื่องกำเนิดไฟฟ้า ทั้งในส่วนที่ติดตั้ง ณ อาคาร ๙ ชั้น ๑ รวมทั้งอุปกรณ์ที่ติดตั้ง ณ อาคาระบบข้อมูลกลางและสำรองข้อมูล สำนักงานขนส่งจังหวัดนนทบุรี

๓. <u>การจัดเก็บแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ</u>

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ จัดทำขึ้นจำนวน ๓ ชุด โดยชุดหนึ่งเก็บไว้ที่ศูนย์เทคโนโลยีสารสนเทศ อาคาร ๙ ณ กรมการขนส่งทางบก จตุจักร และสถานที่สำรองข้อมูล (Backup Site) ตั้งอยู่ที่อาคารระบบข้อมูลกลางและสำรองข้อมูล สำนักงานขนส่งจังหวัดนนทบุรี และจะมีการนำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) ฉบับที่ปรับปรุงใหม่ไปเปลี่ยนทดแทนทันทีที่มีการปรับปรุง

๗.๒ ขณะเกิดเหตุการณ์ภัยพิบัติ

ประสานงานแจ้งผู้บริหารและทีมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติทันทีหรือในขณะเกิดเหตุการณ์ภัยพิบัติ ผู้ที่รับทราบเหตุการณ์ รีบแจ้งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศรับทราบ จากนั้นทีมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติปฏิบัติตามแผนฯ ที่ได้กำหนดไว้

๗.๓ หลังเกิดเหตุการณ์ภัยพิบัติ

(๑) ประเมินความเสียหายและกำหนดสถานที่สำหรับการกู้คืน

ภายหลังจากเหตุการณ์บรรเทาหรือสงบลงแล้ว ทีมประเมินความเสียหายระบบคอมพิวเตอร์และเครือข่ายทำการสำรวจและประเมินความเสียหายของอุปกรณ์คอมพิวเตอร์และเครือข่าย รวมทั้งกำหนดระยะเวลาโดยประมาณในการปรับปรุง แก้ไข ซ่อมแซม เพื่อให้กลับมาใช้งานได้ดังเดิม

ในส่วนของการประเมินความเสียหายของห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) และห้องเครือข่ายสื่อสาร (Network Room) ทำการประเมินความเสียหายโดยทีมประเมินความเสียหายระบบคอมพิวเตอร์และเครือข่ายและทีมอาคารสถานที่ เพื่อร่วมกันพิจารณาว่าห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) และห้องเครือข่ายสื่อสาร (Network Room) เกิดความเสียหายมากน้อยเพียงใด

ผลจากการประเมินความเสียหายทำให้ทราบว่าอุปกรณ์ใดที่เสียหายหรือสูญหายในระหว่างที่เกิดเหตุ อุปกรณ์ใดที่ยังใช้ได้อยู่ อุปกรณ์ที่เสียหายหรือสูญหายจะได้นำไปสู่การจัดหาต่อไป นอกจากนั้นผลการประเมินความเสียหายจะช่วยในการกำหนดระยะเวลาในการใช้งานศูนย์เทคโนโลยีสารสนเทศ อาคาร ๙ ชั้น ๒ เพื่อให้ทีมกู้คืนและติดตั้งระบบคอมพิวเตอร์และเครือข่าย ทีมตรวจสอบและประเมินฐานข้อมูล และทีมตรวจสอบและประเมินระบบงาน เริ่มดำเนินการโดยทันที

(๒) การกู้คืนระบบและข้อมูล

ภายหลังจากเหตุภัยพิบัติยุติลง ทีมกู้คืนและติดตั้งระบบคอมพิวเตอร์และระบบเครือข่าย ทีมตรวจสอบและประเมินฐานข้อมูล ทีมตรวจสอบและประเมินระบบงาน และทีมบริหารจัดการเครื่องคอมพิวเตอร์และอุปกรณ์ดำเนินการแก้ไข/ติดตั้งระบบงานและข้อมูลลงไปใหม่

(๓) ตรวจสอบความพร้อมใช้งาน

ภายหลังจากการกู้คืนระบบและข้อมูล ทีมตรวจสอบและประเมินระบบงาน และทีมบริหารจัดการเครื่องคอมพิวเตอร์และอุปกรณ์ ทำการทดสอบการทำงานของระบบร่วมกับผู้ใช้งาน ก่อนเปิดใช้งานจริง

๘. เหตุการณ์ที่นำไปสู่ภัยพิบัติและมาตรการป้องกัน

เหตุการณ์ที่ไม่คาดคิดเกี่ยวกับภัยพิบัติที่อาจเกิดขึ้น จึงได้กำหนดวิธีป้องกันแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ เพื่อป้องกันไม่ให้เกิดภัยพิบัติต่อหน่วยงานได้ ประกอบด้วย

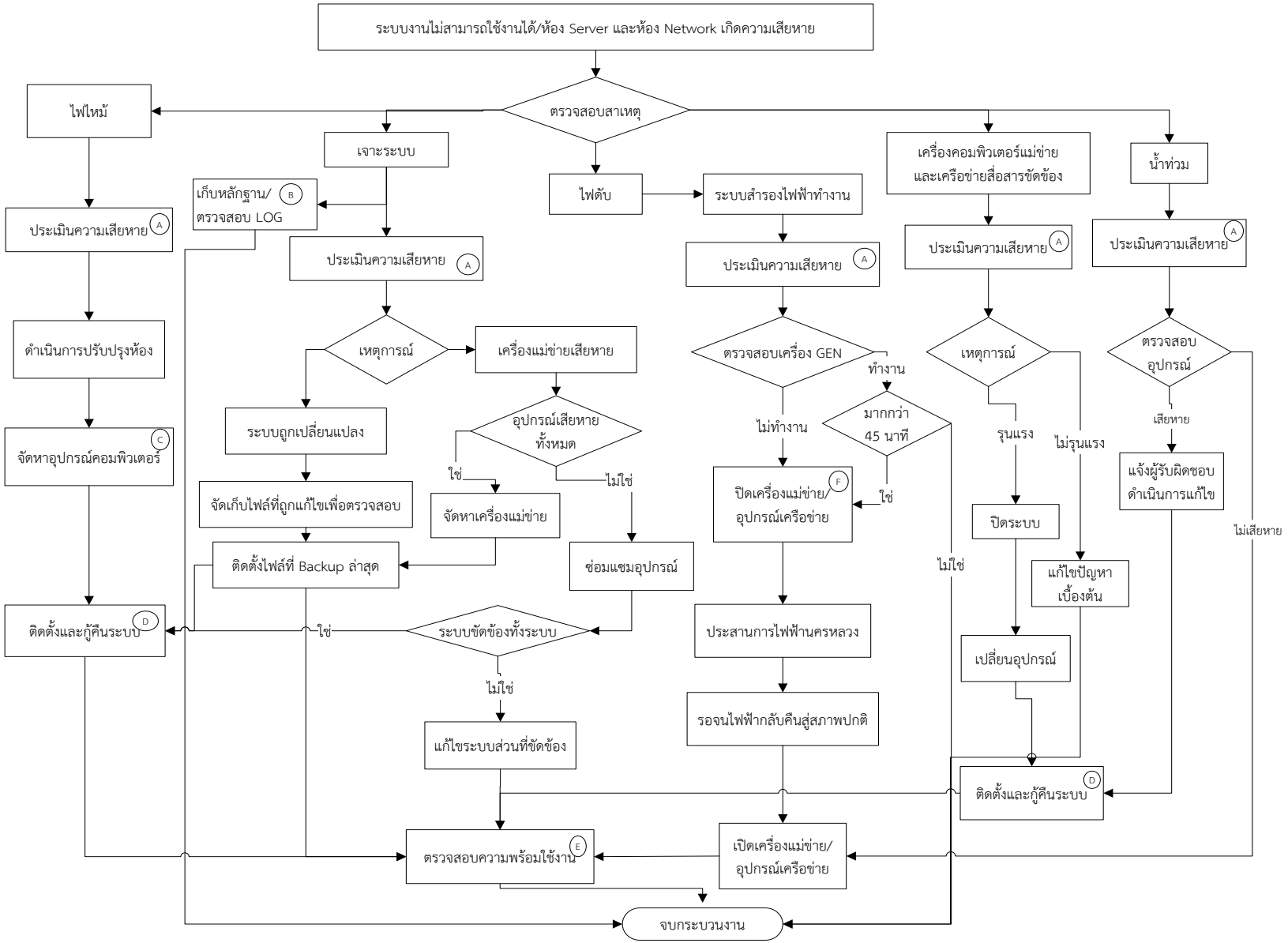
๘.๑ เหตุการณ์ทางด้านเทคนิค

- กรณีโดนเจาะระบบ
- กรณีเครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง
- กรณีระบบเครือข่ายสื่อสารขัดข้อง

๘.๒ เหตุการณ์ทางด้านภัยหรือสถานการณ์ฉุกเฉิน

- กรณีไฟดับ
- กรณีไฟไหม้
- กรณีน้ำท่วม
- กรณีลิฟต์โดยสารขัดข้อง

ขั้นตอนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ



๘.๑ เหตุการณ์ด้านเทคนิค

- **กรณีโดนเจาะระบบ**

ก่อนเกิดเหตุโดนเจาะระบบ

ก่อนโดนเจาะระบบ มีมาตรการและวิธีการป้องกัน ดังนี้

(๑) ดำเนินการตรวจสอบการกำหนดค่า Policy ของอุปกรณ์ Firewall เพื่อป้องกันไม่ให้ผู้ไม่ได้รับอนุญาตเข้ามาในเครือข่ายอินเทอร์เน็ตได้

(๒) ตรวจสอบ IPS ว่ามีผู้ไม่ประสงค์ดีพยายามบุกรุกเข้ามาในระบบหรือไม่

(๓) ทำการ Backup Configuration ของอุปกรณ์เครือข่ายทั้งหมด สำรองเก็บไว้กรณีมีเหตุขัดข้อง

(๔) เผยแพร่ ประชาสัมพันธ์ ให้เจ้าหน้าที่ในหน่วยงานปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กรมการขนส่งทางบก พ.ศ. ๒๕๕๘

(๕) จัดเจ้าหน้าที่ดูแลและตรวจสอบระบบเครือข่าย เพื่อตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ต ของกรมการขนส่งทางบก

(๖) ดำเนินการตรวจสอบด้วยการ IP scan ทุก ๖ เดือน และ Upgrade Firmware ทุกปี หรือเมื่อมี Version ที่ปรับปรุงใหม่

(๗) รายงานผลการตรวจสอบการป้องกันการเจาะระบบแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

ขณะถูกเจาะระบบ

ขณะถูกเจาะระบบ มีขั้นตอนการดำเนินการ ดังนี้

(๑) วิเคราะห์ปัญหา สาเหตุ และประมาณการเวลาในการแก้ไข

(๒) แจ้งเจ้าหน้าที่ที่เกี่ยวข้องเพื่อรับทราบปัญหา และดำเนินการตัดระบบการเชื่อมต่อจากภายนอกเพื่อยับยั้งการรบกวนหรือเจาะระบบ

(๓) แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ กรณีเป็นปัญหากระทบในปริมาณมากหรือต้องใช้เวลาในการแก้ไขนานกว่า ๔ ชั่วโมง

(๔) กรณีที่มีความเสี่ยงสูงให้ดำเนินการตัดระบบที่ถูกบุกรุกจากระบบเครือข่าย ปิดช่องทางในการเข้ามาเจาะระบบ ปิด port ที่ตรวจพบ

หลังเกิดเหตุโดนเจาะระบบ

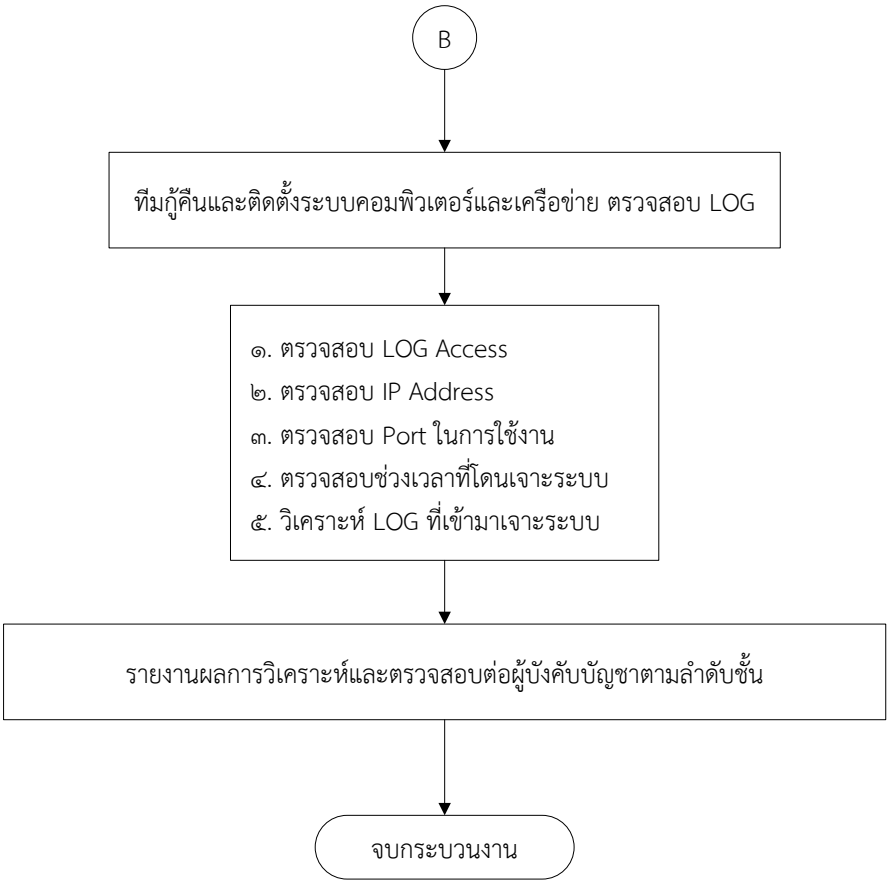
หลังโดนเจาะระบบ มีขั้นตอนการดำเนินการดังนี้

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีโดนเจาะระบบ

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณีโดนเจาะระบบ	หลังโดนเจาะระบบ		ทีมตรวจสอบและ	
		๑. เก็บหลักฐาน พร้อมทำหารทดสอบ LOG	๘ ชั่วโมง	ประเมินระบบ	
		๒. ตรวจสอบและประเมินความเสียหาย		คอมพิวเตอร์	
		๒.๑ ตรวจสอบอุปกรณ์ Hardware เครื่องคอมพิวเตอร์แม่ข่าย		ทีมตรวจสอบและ	
		๒.๑.๑ กรณีเครื่องคอมพิวเตอร์แม่ข่ายเสียหายทั้งหมด	๒๔ ชั่วโมง	ประเมินระบบ	
		(๑) จัดหาเครื่องคอมพิวเตอร์แม่ข่าย		เครือข่าย	
		(๒) ติดตั้งโปรแกรมระบบ		ทีมตรวจสอบและ	
		(๓) ติดตั้งระบบโครงสร้างฐานข้อมูล		ประเมินระบบงาน	
		(๔) ติดตั้งระบบงานสารสนเทศหลัก		ทีมตรวจสอบและ	
		๒.๑.๒ กรณีเครื่องคอมพิวเตอร์แม่ข่ายเสียหายบางส่วน	๑๒ ชั่วโมง	ประเมินฐานข้อมูล	
		(๑) ตรวจสอบความเสียหายของอุปกรณ์ (Hardware) และ			
		ดำเนินการซ่อมแซม			
		(๒) ตรวจสอบความเสียหายของโครงสร้างฐานข้อมูล			
		(๒.๑) ขัดข้องบางส่วน ดำเนินการแก้ไข			
		(๒.๒) ขัดข้องทั้งหมด ดำเนินการจัดทำโครงสร้างฐานข้อมูลใหม่			

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
		(๓) ตรวจสอบความเสียหาย/ขัดข้อง ของระบบงานสารสนเทศหลัก			
		(๓.๑) ขัดข้องบางส่วน ดำเนินการแก้ไข			
		(๓.๒) ขัดข้องทั้งหมด ดำเนินการติดตั้งระบบงานใหม่			
		๒.๒ ตรวจสอบพบการเปลี่ยนแปลงหน้าระบบงาน	๘ ชั่วโมง		
		(๑) จัดเก็บไฟล์ที่ถูกแก้ไขไปดำเนินการตรวจสอบ			
		(๒) ติดตั้งไฟล์ของหน้าระบบงานให้สามารถใช้งานได้ปกติ			
		๓. ทดสอบการใช้งาน พร้อมเปิดให้บริการ			

ขั้นตอนการตรวจสอบ LOG



กระบวนการแก้ไขปัญญา โดยการตรวจสอบ LOG

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีโดนเจาะระบบ (ตรวจสอบ LOG)

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณีโดนเจาะระบบ	หลังจากเก็บหลักฐานแล้ว ดำเนินการดังนี้	๘ ชั่วโมง	ทีมตรวจสอบและ	ดำเนินการ
		๑. ตรวจสอบ Log Access ที่มีการ Access เข้ามาใช้งาน		ประเมินระบบ	ตรวจสอบ
		ในระบบงาน โดยตรวจสอบจากอุปกรณ์ที่เกี่ยวข้อง		คอมพิวเตอร์	ตามคู่มือ
		๒. ตรวจสอบ IP Address ที่เข้ามา		ทีมตรวจสอบและ	การปฏิบัติงาน
		๓. ตรวจสอบ Port ที่ถูกบุกรุก		ประเมินระบบ	ของ กบข.
		๔. ตรวจสอบเวลาที่โดนเจาะระบบ		เครือข่าย	
		๕. ทำการวิเคราะห์ Log			
		๖. รายงานผลการวิเคราะห์แก่ผู้บังคับบัญชาตามลำดับชั้น			

หน่วยงานที่มีภารกิจในการช่วยเหลือในกรณีถูกเจาะระบบ

หน่วยงาน	หน้าที่ความรับผิดชอบ	รายละเอียดการติดต่อ
กองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจและเทคโนโลยี	ดำเนินการสืบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	กองบังคับการปราบปรามอาชญากรรม ทางเศรษฐกิจและเทคโนโลยี ถนนสาทรเหนือ แขวงสีลม เขตบางรัก กรุงเทพมหานคร ๑๐๕๐๐ โทรศัพท์ ๐-๒๒๓๗-๑๑๙๙ โทรสาร ๐-๒๒๓๔-๖๘๐๖ Website : http://www.ecdpolice.com
ศูนย์ตรวจสอบและวิเคราะห์ การกระทำผิดทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ	ดำเนินการสอบสวนการกระทำความผิดทางกฎหมาย โดยใช้เครื่องมือทางเทคโนโลยีสารสนเทศและการสื่อสาร	ศูนย์ตรวจสอบและวิเคราะห์การกระทำผิดทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ อาคาร ๓๓ ชั้น ๔ ถนนพระรามที่ ๑ เขตปทุมวัน กรุงเทพมหานคร ๑๐๓๓๐ โทรศัพท์ ๐-๒๒๐๕-๒๖๒๗ โทรสาร ๐-๒๒๐๕-๑๘๘๙ Website : http://itc.police.go.th
สำนักคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ	ปฏิบัติงานด้านการป้องกันปราบปรามและสืบสวนผู้กระทำความผิดในคดีเกี่ยวกับเทคโนโลยีและสารสนเทศ	สำนักคดีเทคโนโลยีและสารสนเทศ ชั้น ๙ กรมสอบสวนคดีพิเศษ ๑๒๘ ซอย ๙ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐ โทรศัพท์/โทรสาร ๐๒-๙๗๕-๙๘๓๒ Website : http://www.dsi.go.th
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	เป็นผู้ออกและบังคับใช้ พรบ. การกระทำผิดเกี่ยวกับคอมพิวเตอร์ ๒๕๕๐	ชั้น ๘ อาคาร B ศูนย์ราชการแจ้งวัฒนะ ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐ โทรศัพท์ ๐-๒๕๐๕-๗๓๗๐ E-Mail : pr@mdes.go.th Website : https://www.mdes.go.th/
ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT)	มีภาระหน้าที่ ในการรับแจ้งเหตุ และประสานงานกับหน่วยงานต่างๆ ภายในประเทศไทย และหน่วยงาน CSIRT ในต่างประเทศ เพื่อตอบสนองและจัดการต่อเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ รวมถึงการให้การสนับสนุนข้อมูลต่างๆที่จำเป็นต่อหน่วยงานเพื่อดำเนินการแก้ไขเหตุการณ์ที่ได้รับแจ้ง	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ เลขที่ ๑๒๐ ม.๓ อาคารหน่วยราชการ (อาคาร B) ชั้น ๗ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ โทรศัพท์ ๐-๒๑๔๒-๒๔๘๓ Website : http://www.thaicert.or.th

- **กรณีเครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายสื่อสารขัดข้อง**

  ก่อนเกิดเหตุเครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายสื่อสารขัดข้อง

  ก่อนเกิดเครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายสื่อสารขัดข้อง มีขั้นตอนดังนี้

  (๑) จัดให้มีเจ้าหน้าที่ตรวจสอบการทำงาน (Monitor) เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายสื่อสาร และอุปกรณ์ที่เกี่ยวข้อง ตลอดเวลาที่ให้บริการ

  (๒) จัดให้มีเจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศ ตลอด ๒๔ ชั่วโมง ไม่เว้นวันหยุดราชการ

  (๓) รายงานผลการตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่เกี่ยวข้องเสนอผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อทราบ เดือนละ ๑ ครั้ง

ขณะเกิดเหตุเครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง

ขณะเกิดเหตุเครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง มีวิธีปฏิบัติดังนี้

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีเครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณี	ขณะเกิดเหตุเครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง		ทีมตรวจสอบและ	ดำเนินการ
	เครื่องคอมพิวเตอร์	ประเมินความเสียหายเครื่องคอมพิวเตอร์แม่ข่าย		ประเมินระบบ	ตามคู่มือ
	แม่ข่ายขัดข้อง	๑. กรณีที่เกิดจากอุปกรณ์เสียหาย ทำการ shutdown	๓๐ นาที	คอมพิวเตอร์	การปฏิบัติงาน
		เครื่องคอมพิวเตอร์แม่ข่ายที่มีอุปกรณ์ขัดข้อง			ของ กบข.
		๒. กรณีเกิดจากโปรแกรมระบบปฏิบัติการ/โปรแกรมประยุกต์	๓๐ นาที		
		ทำการ shutdown เครื่องที่โปรแกรมขัดข้อง			
		๓. กรณีที่เกิดจากระบบฐานข้อมูลเสียหาย ทำการปิดระบบ	๓๐ นาที		
		๔. กรณีเกิดจากทรัพยากรระบบไม่เพียงพอต่อการใช้งาน	๓๐ นาที		
		ทำการจำกัดผู้ใช้งาน			

หลังเกิดเหตุเครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง

หลังเกิดเหตุเครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง มีขั้นตอนดังนี้

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีเครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณี	หลังเกิดเหตุเครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง		ทีมตรวจสอบและ	ดำเนินการ
	เครื่องคอมพิวเตอร์	๑. กรณีที่เกิดจากอุปกรณ์เสียหาย ทำการเปลี่ยนอุปกรณ์ที่ขัดข้อง		ประเมินระบบ	ตามคู่มือ
	แม่ข่ายขัดข้อง	และ Start เครื่องคอมพิวเตอร์แม่ข่าย	๔ ชั่วโมง	คอมพิวเตอร์	การปฏิบัติงาน
		๒. กรณีเกิดจากโปรแกรมระบบปฏิบัติการ/โปรแกรมประยุกต์			ของ กบข.
		ทำการกู้คืนโปรแกรมฯ	๔ ชั่วโมง		
		๓. กรณีที่เกิดจากระบบฐานข้อมูลเสียหาย ทำการกู้คืนระบบ			
		ฐานข้อมูล	๑๒ ชั่วโมง		
		๔. กรณีเกิดจากทรัพยากรระบบไม่เพียงพอต่อการใช้งาน			
		ทำการปิด Session ที่ไม่ใช่ระบบงานของกรมฯ และให้มีการ	๒ ชั่วโมง		
		ตรวจสอบข้อมูลเบื้องต้นก่อนที่จะ run งานใด ๆ			

- **กรณีระบบเครือข่ายสื่อสารขัดข้อง**

ก่อนเกิดเหตุระบบเครือข่ายสื่อสารขัดข้อง

ก่อนเกิดระบบเครือข่ายสื่อสารขัดข้อง มีขั้นตอนดังนี้

(๑) จัดให้มีเจ้าหน้าที่ตรวจสอบการทำงาน (Monitor) เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายสื่อสาร และอุปกรณ์ที่เกี่ยวข้องตลอดเวลาที่ให้บริการ

(๒) จัดให้มีเจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศ เพื่อรับแจ้งปัญหาด้านระบบเครือข่ายสื่อสารเบื้องต้น ตลอด ๒๔ ชั่วโมง ไม่เว้นวันหยุดราชการ และประสานกับผู้ให้บริการตรวจสอบและแก้ไขต่อไป

(๓) รายงานผลการตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายสื่อสารและอุปกรณ์ที่เกี่ยวข้อง เสนอผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อทราบ เมื่อไม่สามารถใช้งานวงจรเครือข่ายสื่อสารพร้อมกันทั้ง ๒ วงจร

ขณะเกิดเหตุระบบเครือข่ายสื่อสารขัดข้อง

ขณะเกิดเหตุระบบเครือข่ายสื่อสารขัดข้อง มีวิธีปฏิบัติดังนี้

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีระบบเครือข่ายสื่อสารขัดข้อง

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณี	ขณะเกิดเหตุระบบเครือข่ายสื่อสารขัดข้อง		ทีมตรวจสอบและ	ดำเนินการ
	ระบบเครือข่าย	ประเมินความเสียหายระบบเครือข่ายสื่อสาร		ประเมินระบบ	ตามคู่มือ
	สื่อสารขัดข้อง	๑. กรณีที่เกิดจากอุปกรณ์เสียหายไม่สามารถแก้ไขได้ ต้องเปลี่ยน	๔-๖ ชั่วโมง	เครือข่าย	การปฏิบัติงาน
		อุปกรณ์ทดแทนอุปกรณ์ที่ขัดข้อง			ของ กบข.
		๒. กรณีค่า Configuration ของอุปกรณ์เสียหาย ทำการ shutdown	๑ ชั่วโมง		
		อุปกรณ์ที่ขัดข้อง และ Reconfigure ใหม่			
		๓. กรณีมีปัญหาการเชื่อมโยงข้อมูล			* สลับใช้
		๓.๑ Main Link ขัดข้อง แจ้งผู้ให้บริการ (ทีโอที)	๑๐ นาที		เครือข่าย
		๓.๒ Backup Link ขัดข้อง แจ้งผู้ให้บริการ (กสท.)	๑๐ นาที		สำรอง

หลังเกิดเหตุระบบเครือข่ายสื่อสารขัดข้อง

หลังเกิดเหตุระบบเครือข่ายสื่อสารขัดข้อง มีขั้นตอนดังนี้

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีระบบเครือข่ายสื่อสารขัดข้อง

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณี	หลังเกิดเหตุระบบเครือข่ายสื่อสารขัดข้อง		ทีมตรวจสอบและ	ดำเนินการ
	ระบบเครือข่าย	๑. กรณีที่เกิดจากอุปกรณ์เสียหาย ทำการเปลี่ยนอุปกรณ์ขัดข้อง	๔-๖ ชั่วโมง	ประเมินระบบ	ตามคู่มือ
	สื่อสารขัดข้อง	และ Start อุปกรณ์		เครือข่าย	การปฏิบัติงาน
		๒. กรณีค่า Configuration ของอุปกรณ์เสียหาย ทำการกู้คืนค่า	๑-๒ ชั่วโมง		ของ กบข.
		Configuration			
		๓. กรณีมีปัญหาการเชื่อมโยงข้อมูล			* ขึ้นกับ
		๓.๑ Main Link ขัดข้อง ผู้ให้บริการ ดำเนินการแก้ไข	๔ ชั่วโมง		สภาพปัญหา
		๓.๒ Backup Link ขัดข้อง แจ้งผู้ให้บริการ ดำเนินการแก้ไข	๔-๖ ชั่วโมง		และลักษณะ
					ที่ขัดข้อง

๘.๒ เหตุการณ์ทางด้านภัยหรือสถานการณ์ฉุกเฉิน

- **กรณีไฟดับ**

ก่อนเกิดเหตุไฟดับกรณีเครื่องคอมพิวเตอร์แม่ข่าย

ก่อนเกิดเหตุไฟดับ มีขั้นตอนดังนี้

(๑) จัดหาเครื่องสำรองไฟฟ้า (UPS) และอุปกรณ์ปั่นไฟ (Generator)

(๒) จัดให้มีเจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศ ตลอด ๒๔ ชั่วโมง ไม่เว้นวันหยุดราชการ

(๓) ทำการตรวจสอบการทำงานของเครื่องสำรองไฟฟ้าที่ติดตั้ง ณ ห้องเครื่องแม่ข่าย (Server Room) และห้องอุปกรณ์เครือข่าย (Network Room) และห้อง DLT SYSTEM CONTROL เดือนละ ๑ ครั้ง

(๔) ทำการตรวจสอบปริมาณน้ำมันที่บรรจุในอุปกรณ์ปั่นไฟ (Generator) เดือนละ ๑ ครั้ง

(๕) รายงานผลการตรวจสอบการทำงานของเครื่องสำรองไฟฟ้า (UPS) และอุปกรณ์ปั่นไฟ (Generator) เสนอผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อทราบ เดือนละ ๑ ครั้ง

(๖) ตรวจสอบการทำงานของลิฟต์โดยสาร โดยสามารถดูรายละเอียดได้ที่ กรณีลิฟต์โดยสารขัดข้อง

ขณะเกิดเหตุไฟดับ

ขณะเกิดไฟดับ มีวิธีปฏิบัติดังนี้

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีไฟดับ

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณีไฟดับ	ขณะเกิดเหตุไฟดับ	ดำเนินการทันที		ดำเนินการ
		๑. ตรวจสอบการต่อพ่วงเครื่องแม่ข่าย และอุปกรณ์เครือข่ายและ	เมื่อไฟดับ	ทีมกู้คืนและติดตั้ง	ตามคู่มือ
		อุปกรณ์ที่เกี่ยวข้อง กับระบบสำรองไฟฟ้า (UPS) และเครื่องปั่นไฟ		ระบบคอมพิวเตอร์	การปฏิบัติงาน
		(Generator)		และเครือข่าย	ของ กบข.
		๒. ประชาสัมพันธ์ให้ผู้ใช้งานทราบ		ทีมประชาสัมพันธ์	
				ข้อมูล	
		๓. ตรวจสอบปริมาณน้ำมันที่เตรียมไว้สำหรับให้อุปกรณ์ปั่นไฟทำงาน	๕ นาที	ทีมอาคารสถานที่	
		๓.๑ กรณีอุปกรณ์เครื่องปั่นไฟ (Generator) ไม่ทำงาน ทำการปิด	๓๐ นาที		
		ระบบเครื่องแม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์ที่เกี่ยวข้อง			
		๓.๒ กรณีอุปกรณ์เครื่องปั่นไฟ (Generator) ทำงาน รองรับ	๓๐ นาที		
		การทำงานได้ไม่ถึง ๔๕ นาที ทำการปิดระบบเครื่องแม่ข่าย			
		อุปกรณ์เครือข่าย และอุปกรณ์ที่เกี่ยวข้อง			

หลังเกิดเหตุไฟดับ

หลังเกิดไฟดับ มีขั้นตอนดังนี้

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีไฟดับ

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณีไฟดับ	หลังเกิดเหตุไฟดับ			
		๑. แก้ไขอุปกรณ์เครื่องปั่นไฟ (Generator) ให้สามารถทำงานได้	๔ ชั่วโมง	ทีมอาคารสถานที่	
		๒. ประสานการไฟฟ้านครหลวง เพื่อขทราบสาเหตุของไฟดับ			
		และระยะเวลาในการแก้ไขปัญหา			
		๓. เมื่อไฟฟ้ากลับคืนสู่สภาพปกติ ทำการเปิดระบบเครื่องคอมพิวเตอร์	๑ - ๒ ชั่วโมง	ทีมกู้คืนและติดตั้ง	
		แม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์ที่เกี่ยวข้อง		ระบบคอมพิวเตอร์	
				และเครือข่าย	
		๔. หาแนวทางป้องกัน หากเกิดไฟฟ้าดับและอุปกรณ์เครื่องปั่นไฟ		ทีมอาคารสถานที่	
		(Generator) และเครื่องสำรองไฟฟ้า (UPS) ไม่ทำงาน หรือทำงานได้			
		ในระยะเวลาไม่ถึง ๔๕ นาที			

- **กรณีไฟไหม้**

ก่อนเกิดเหตุไฟไหม้

ก่อนเกิดเหตุไฟไหม้ มีวิธีการป้องกัน ดังนี้

๑) จัดหาระบบดับเพลิงอัตโนมัติ และติดตั้งภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) และห้องเครือข่ายสื่อสาร (Network Room) อาคาร ๔ ชั้น ๖ และห้อง DLT SYSTEM CONTROL อาคาร ๙ ชั้น ๒

๒) จัดหาถังดับเพลิงชนิดเคมีพร้อมคู่มือการใช้งานกระจายอยู่ตามจุดต่าง ๆ ภายในศูนย์เทคโนโลยีสารสนเทศ

๓) จัดทำเส้นทางการอพยพหนีไฟและจุดรวมพล

๔) มีระบบแจ้งเตือน (Alarm) เพื่อแจ้งเหตุกรณีเกิดไฟไหม้

๕) จัดให้มีเจ้าหน้าที่ประจำศูนย์เทคโนโลยีสารสนเทศ ตลอด ๒๔ ชั่วโมง ไม่เว้นวันหยุดราชการ

๖) ทำการตรวจสอบระบบ อุปกรณ์ต่าง ๆ ทุกเดือน

๗) กำหนดแผนให้มีการซักซ้อมการหนีไฟปีละ ๑ ครั้ง

๘) จัดทำรายงานผลการซ้อมหนีไฟ เพื่อนำมาปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติในครั้งต่อไป

๙) ในส่วนของการใช้งานลิฟต์โดยสาร ให้ดูรายละเอียดในหัวข้อ กรณีลิฟต์โดยสารขัดข้อง หน้า ๔๔

ขณะเกิดเหตุไฟไหม้

ขณะเกิดเหตุไฟไหม้ มีวิธีปฏิบัติดังนี้

๑) เมื่อได้ยินเสียงสัญญาณแจ้งเหตุเพลิงไหม้ให้รีบอพยพตามเส้นทางที่ได้กำหนดไว้

(๑) ให้ผู้นำทางหนีไฟนำเจ้าหน้าที่ออกจากห้องทำงานให้เร็วที่สุด

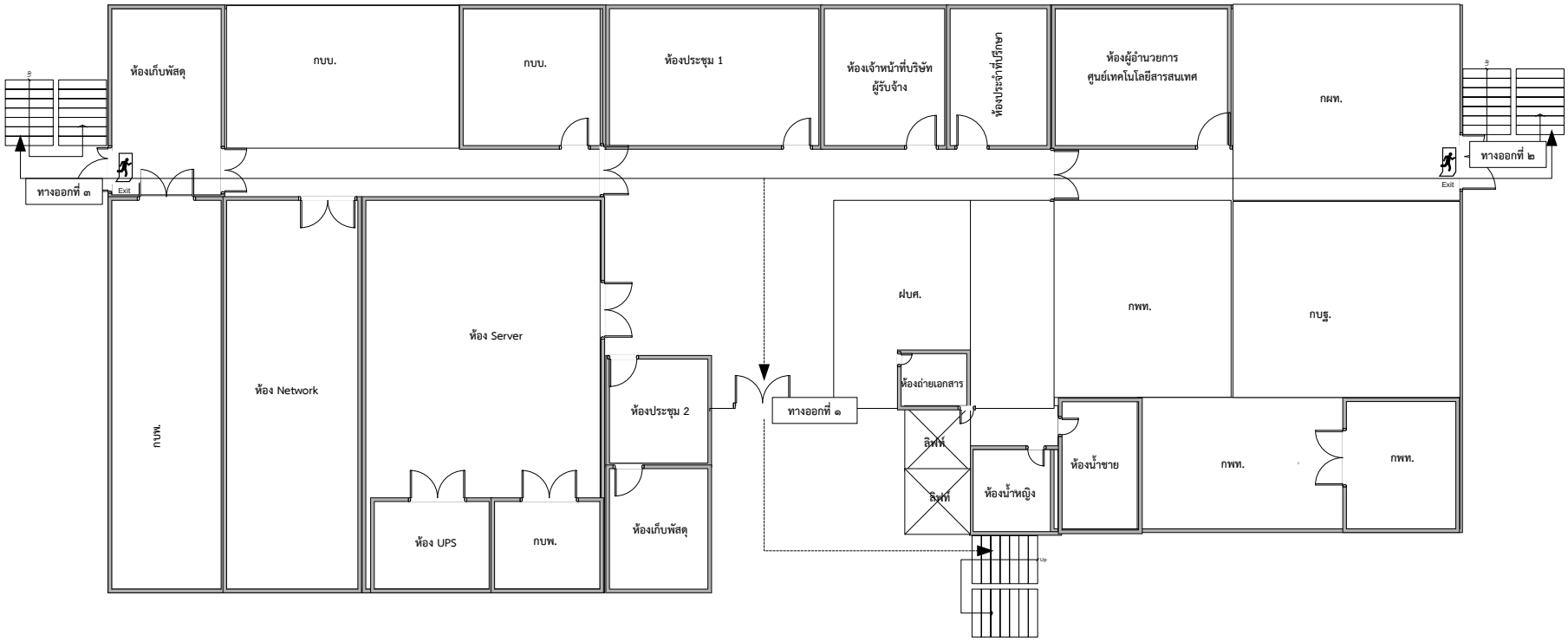
(๒) ผู้นำทางหนีไฟนำเจ้าหน้าที่ออกไปยังทางหนีไฟที่ใกล้ที่สุดที่ได้กำหนดไว้ และให้ไปรวมตัวกันที่จุดรวมพล เพื่อฟังขั้นตอนการปฏิบัติต่อไป

(๓) ให้ทุกคนเดินอย่างรวดเร็วเป็นระเบียบตามผู้นำทางหนีไฟ ห้ามวิ่งโดยเด็ดขาด เดินชิดขวาเป็นสองแถว ห้ามผลัก ห้ามแซง ห้ามดึง ห้ามดัน และไม่ควรกลับเข้าไปในอาคารอีก

๒) หากเส้นทางหนีไฟเต็มไปด้วยกลุ่มควันให้ใช้ผ้าชุบน้ำมาคลุมตัว และปิดจมูก ป้องกันการสำลักควัน แล้วหมอบคลานเนื่องจากอากาศบริสุทธิ์จะอยู่ด้านล่าง

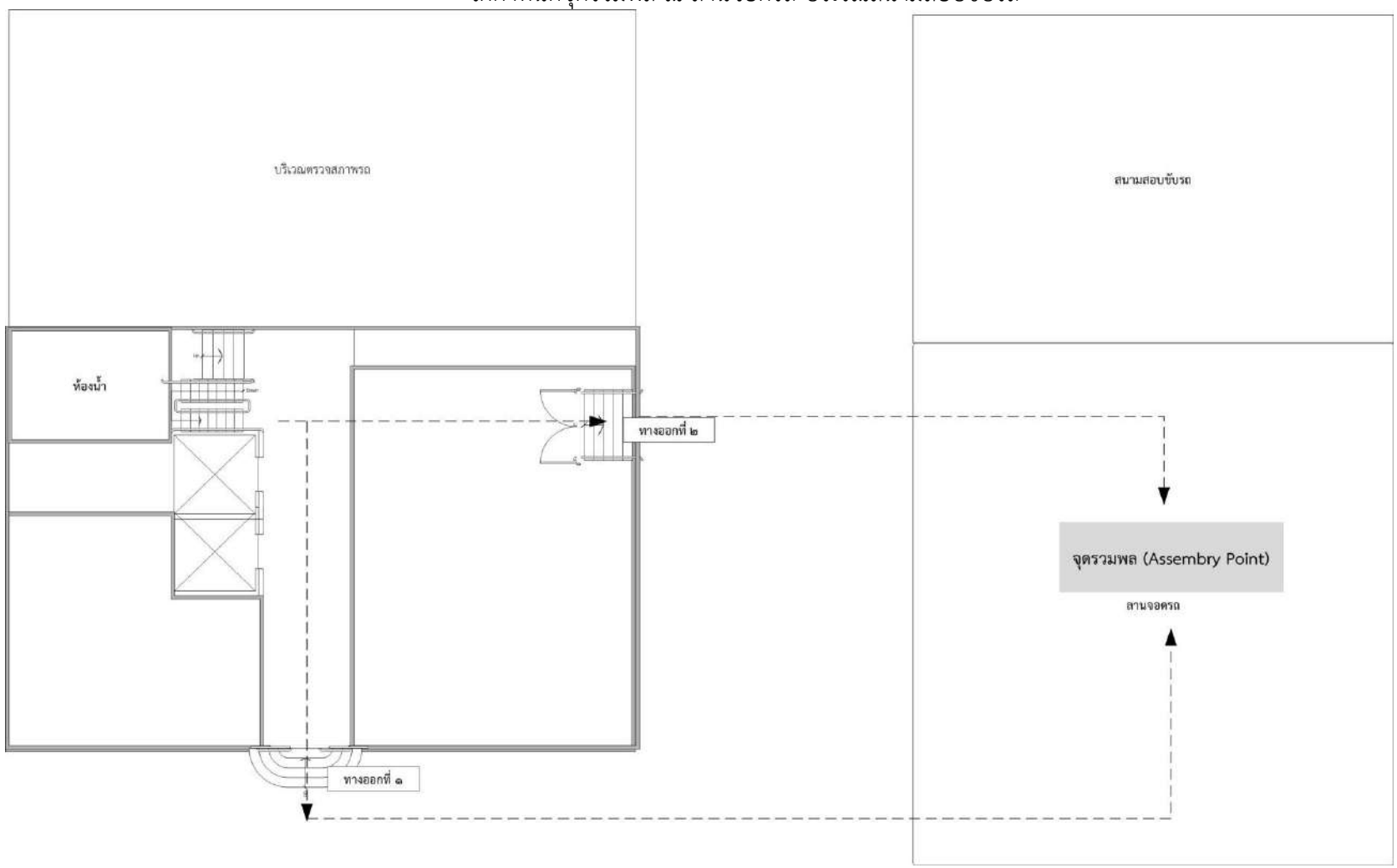
๓) ห้ามใช้ลิฟต์ เพราะขณะเกิดเพลิงไหม้ ไฟฟ้าจะดับทำให้ลิฟต์ไม่สามารถใช้งาน ทั้งนี้วิธีการปฏิบัติตัวหากติดค้างภายในลิฟต์โดยสาร ให้ดูวิธีการปฏิบัติที่ กรณีลิฟต์โดยสารขัดข้อง หน้า ๔๔

เส้นทางการอพยพหนีไฟของศูนย์เทคโนโลยีสารสนเทศ อาคาร ๔ ชั้น ๖

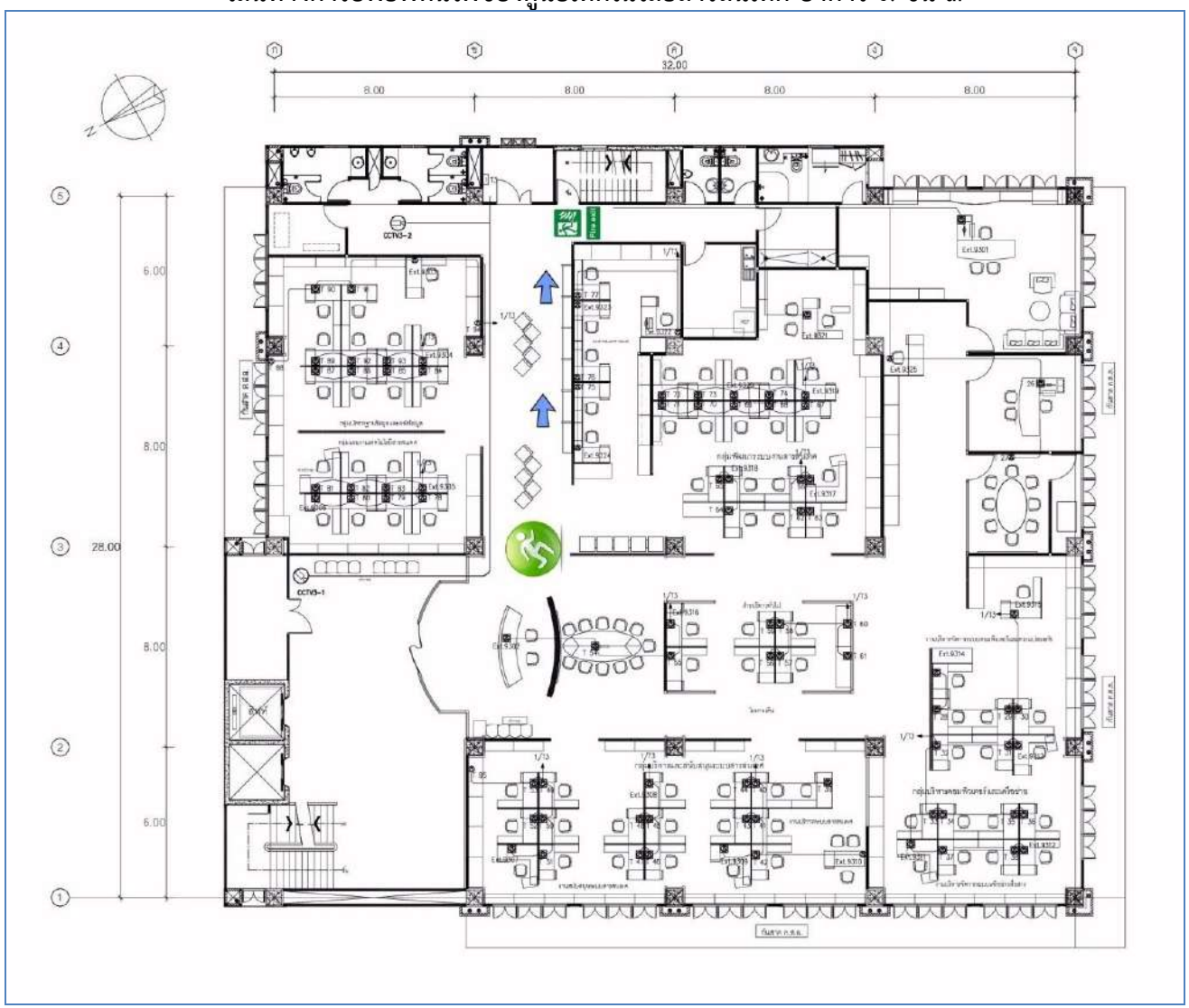


จุดรวมพล

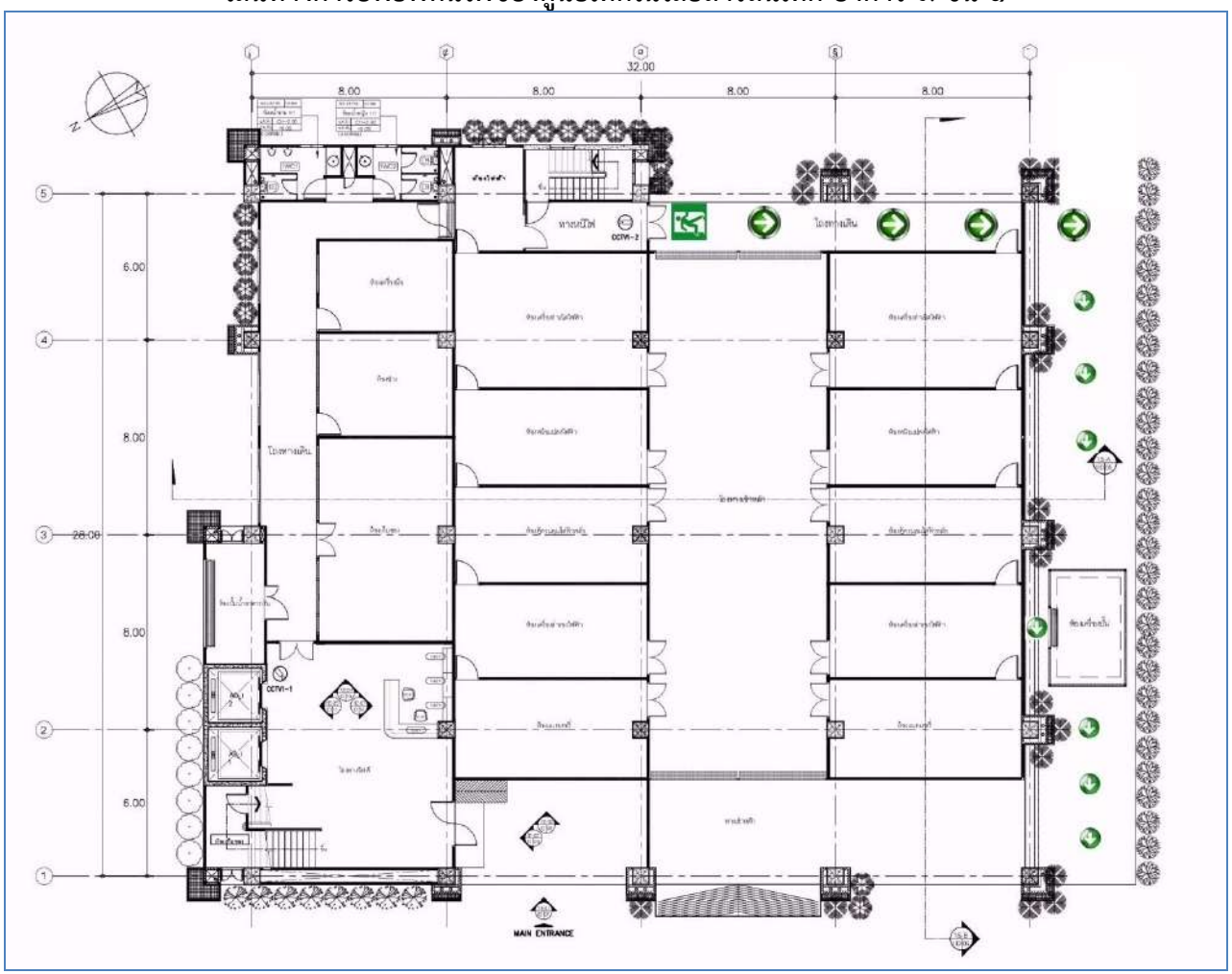
ได้กำหนดจุดรวมพล ณ ลานจอดรถ บริเวณสนามสอบขับรถ



เส้นทางการอพยพหนีไฟของศูนย์เทคโนโลยีสารสนเทศ อาคาร ๙ ชั้น ๓

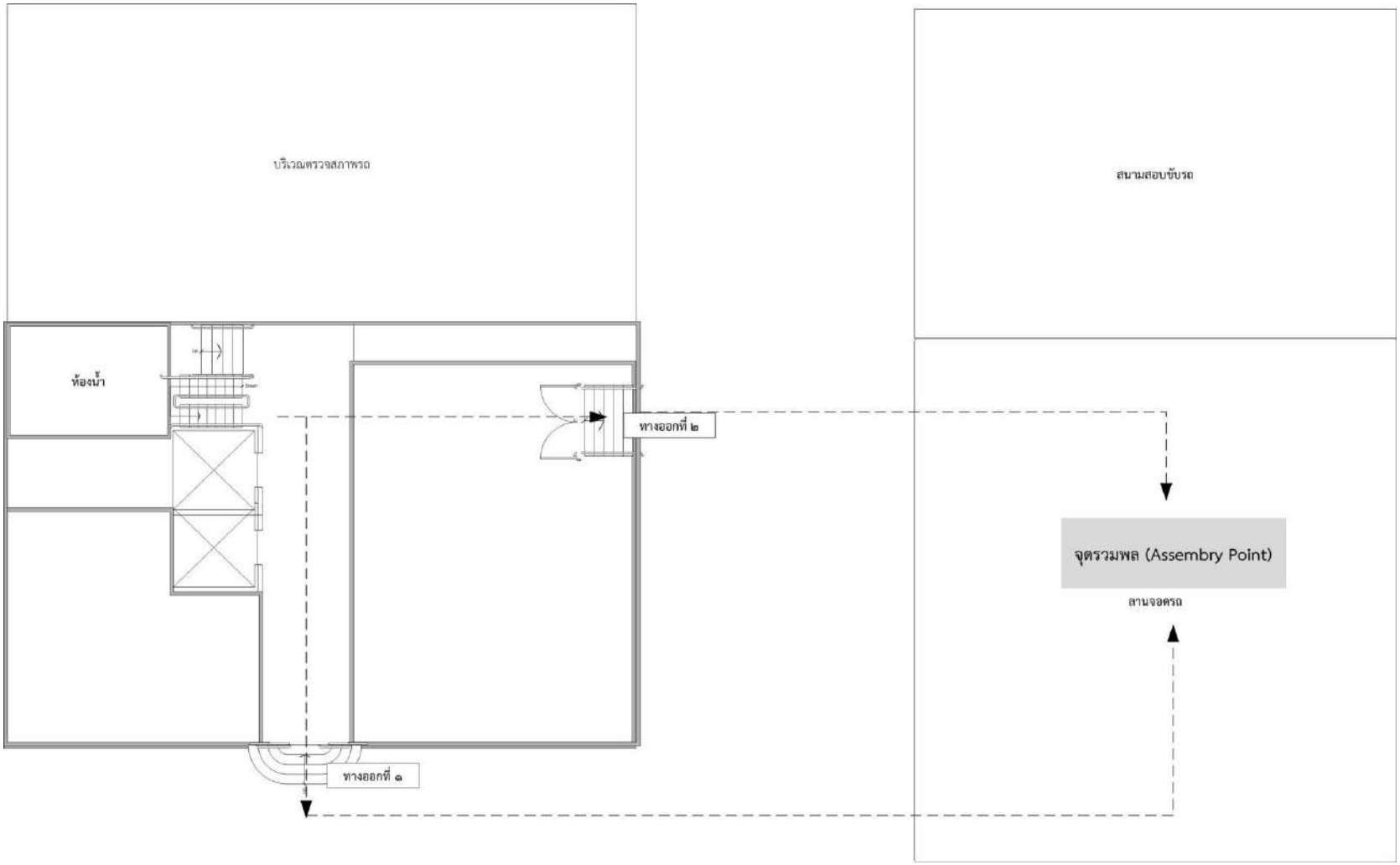


เส้นทางการอพยพหนีไฟของศูนย์เทคโนโลยีสารสนเทศ อาคาร ๙ ชั้น ๑



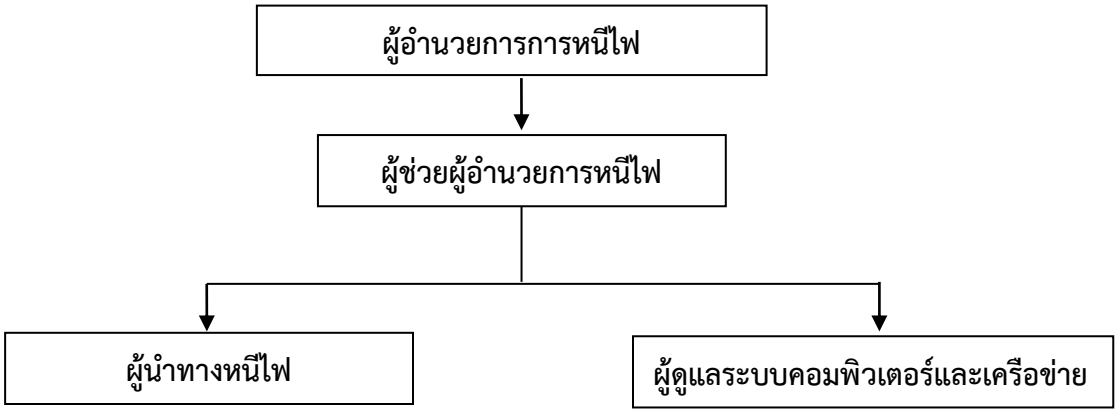
จุดรวมพล

ได้กำหนดจุดรวมพล ณ ลานจอดรถ บริเวณสนามสอบขับรถ



ทีมอพยพหนีไฟ

ในกรณีที่เกิดไฟไหม้ ทีมอพยพหนีไฟจะเริ่มดำเนินการตามหน้าที่ที่ได้รับมอบหมาย



หน้าที่ความรับผิดชอบ

หน้าที่/ความรับผิดชอบ	ผู้ปฏิบัติ
ผู้อำนวยการการหนีไฟ ทำหน้าที่สั่งการในการอพยพหนีไฟ	ผศท.
ผู้ช่วยผู้อำนวยการหนีไฟ ๑. สั่งการแทนผู้อำนวยการในการหนีไฟ กรณีที่ผู้อำนวยการหนีไฟไม่สามารถปฏิบัติหน้าที่ได้ ๒. ดูแลความเรียบร้อยในการหนีไฟ	หบข. หทถ. หขร. หมส.
ผู้นำทางหนีไฟ นำทางให้กับเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศในการอพยพหนีไฟ	นายทวีป นาคงาม นายกิตติชัย เกษลา นายณัฐพล นกดี นายทรงสวัสดิ์ พูลสวัสดิ์
ผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย เตรียมปิดระบบและตัดการเชื่อมต่อไปยัง Backup Site	นายกิตติพล วิมุกติพันธุ์ นายศุภชัย พลโก นายโชคอำนวย เถื่อนสันเทียะ นายจักริน ไอศุริยสมบัติ

หลังเกิดเหตุไฟไหม้

หลังเกิดเหตุไฟไหม้ เจ้าหน้าที่ที่เกี่ยวข้องปฏิบัติ ดังนี้

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีไฟไหม้

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณีไฟไหม้	หลังเกิดเหตุไฟไหม้			
		๑. ตรวจสอบและประเมินความเสียหาย	ภายใน ๒๔ ชั่วโมง		
		๑.๑ ทีมอาคาร สถานที่ ตรวจสอบความเสียหายของอาคาร สถานที่		ทีมอาคารสถานที่	
		๑.๒ ตรวจสอบและประเมินความเสียหายของเครื่องคอมพิวเตอร์		ทีมกู้คืนและติดตั้ง	
		แม่ข่าย		ระบบคอมพิวเตอร์	
		๑.๓ ตรวจสอบและประเมินความเสียหายของอุปกรณ์และ		และเครือข่าย	
		ระบบเครือข่าย			
		๑.๔ ตรวจสอบและประเมินความเสียหายของข้อมูล		ทีมตรวจสอบและ	
				ประเมินฐานข้อมูล	
		๑.๕ ตรวจสอบและประเมินความเสียหายของระบบงานหลัก			
		๒. กู้คืนระบบ	ขึ้นอยู่กับความรุนแรง		ดำเนินการได้
		๒.๑ ปรับปรุงห้อง Server และห้อง Network	ของสถานการณ์	ทีมอาคารสถานที่	ภายหลังจาก
		๒.๒ ติดตั้งและกู้คืนโปรแกรมระบบที่เกี่ยวข้องกับ		ทีมกู้คืนและติดตั้ง	จัดหาอุปกรณ์
		ระบบสารสนเทศหลัก		ระบบคอมพิวเตอร์	ที่เกี่ยวข้อง
		๒.๓ ติดตั้งอุปกรณ์และกำหนดค่า configuration ของ		และเครือข่าย	
		ระบบเครือข่าย			
		๒.๔ ติดตั้งโครงสร้างฐานข้อมูลของระบบสารสนเทศหลัก		ทีมตรวจสอบและ	
				ประเมินฐานข้อมูล	
		๒.๕ ติดตั้งระบบงานสารสนเทศหลัก		ทีมตรวจสอบและ	
				ประเมินระบบงาน	

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
		๓. ประชาสัมพันธ์ให้ผู้ใช้งานทราบ	เมื่อเกิดเหตุภายใน	ทีมประชาสัมพันธ์	เมื่อทราบเหตุ
		๔. ให้บริการระบบสารสนเทศหลัก	๒๔ ชั่วโมงหลังจาก	ข้อมูล	และแจ้งผู้ใช้งาน
			การติดตั้งฯ แล้ว		เป็นระยะ

- **กรณีน้ำท่วม**

ก่อนเกิดเหตุการณ์น้ำท่วม

ก่อนเกิดเหตุการณ์น้ำท่วม ต้องดำเนินการดังนี้

๑) ดูแล อุปกรณ์ สถานที่ติดตั้งอุปกรณ์ ให้มีความพร้อมใช้งานอยู่เสมอ

๒) จัดเตรียมเครื่องมือป้องกันน้ำท่วมให้กับอุปกรณ์ที่ติดตั้งในจุดเสี่ยงต่อการถูกน้ำท่วม

๓) เติมน้ำมันให้กับเครื่อง Generator

๔) ปิดทางเข้าออกที่น้ำจะเข้าถึงอุปกรณ์ที่อยู่ในความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศ

๕) ออกคำสั่งให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศมาปฏิบัติงานในแต่ละกลุ่มที่รับผิดชอบ

ขณะเกิดเหตุการณ์น้ำท่วม

ขณะเกิดน้ำท่วม ผู้เกี่ยวข้องดำเนินการดังนี้

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีน้ำท่วม

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	น้ำท่วม	ขณะเกิดน้ำท่วม	ดำเนินการทันที	ทีมกู้คืนและติดตั้ง	
		๑. ตรวจสอบอุปกรณ์ที่อยู่ในจุดเสี่ยงที่น้ำจะท่วมถึง	เมื่อรับทราบ	ระบบคอมพิวเตอร์	
		๒. ประเมินสถานการณ์	สถานการณ์น้ำท่วม	และเครือข่าย	
		๒.๑ รุนแรง		ทีมอาคารสถานที่	
		- ปิดระบบ			
		๒.๒ ไม่รุนแรง			
		- ดำเนินการเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่อยู่ในจุดเสี่ยง			
		๒.๒.๑ กรณีไม่สามารถเคลื่อนย้ายได้			
		- ปิดการใช้งานอุปกรณ์			
		- จัดหาเครื่องมือและวัสดุเพื่อห่อหุ้มอุปกรณ์ ป้องกัน			
		ไม่ให้น้ำเข้าไปทำความเสียหาย			
		๒.๒.๒ กรณีที่สามารถเคลื่อนย้ายได้			
		- ปิดการใช้งานอุปกรณ์			
		- ดำเนินการเคลื่อนย้ายอุปกรณ์ไปไว้ในสถานที่			
		ที่เตรียมไว้ และปลอดภัย			
		๓. กรณีต้องทำการย้ายอุปกรณ์เครื่องปั่นไฟ (Generator) หรือ	เมื่อรับทราบ		
		ต้องหยุดการทำงานของอุปกรณ์เครื่องปั่นไฟ (Generator) จะต้อง			
		ดำเนินการปิดระบบเครื่องแม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์ที่			
		เกี่ยวข้องทันทีที่การไฟฟ้าฯ ไม่สามารถจ่ายกระแสไฟฟ้าได้ตามปกติ			
		(ดำเนินการตามข้อ ๓.๑ ของการแก้ไขปัญหาจากภัยพิบัติ กรณีไฟดับ)			

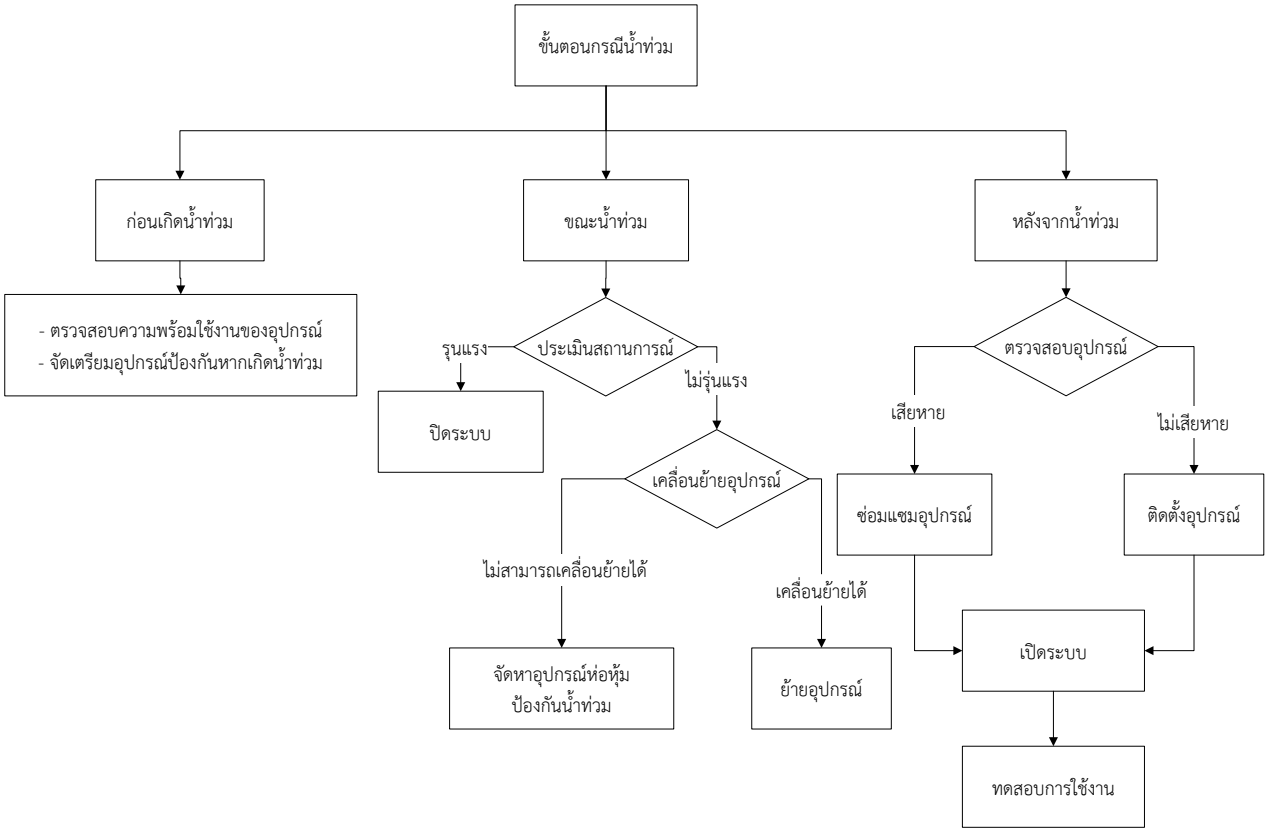
หลังเกิดเหตุการณ์น้ำท่วม

หลังเกิดน้ำท่วม ผู้เกี่ยวข้องดำเนินการดังนี้

กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีน้ำท่วม

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	น้ำท่วม	หลังน้ำท่วม	ดำเนินการทันที	ทีมกู้คืนและติดตั้ง	
		๑. ตรวจสอบและประเมินความเสียหายที่เกิดขึ้นกับอุปกรณ์	เมื่อน้ำท่วม	ระบบคอมพิวเตอร์	
		๑.๑ กรณีอุปกรณ์เกิดความเสียหาย		และเครือข่าย	
		- ดำเนินการแก้ไขซ่อมแซม หากไม่สามารถดำเนินการได้			
		ให้แจ้งบริษัทฯ ที่รับผิดชอบ			
		- ดำเนินการติดตั้งอุปกรณ์			
		- ทำการเปิดระบบและทดสอบการเข้าใช้งาน			
		๑.๒ กรณีอุปกรณ์ไม่เสียหาย			
		- ดำเนินการติดตั้งอุปกรณ์			
		- ทำการเปิดระบบและทดสอบการเข้าใช้งาน			
		๒. ทบทวนแผนในการบำรุงรักษาอุปกรณ์ และกำหนดจุดในการติดตั้ง			
		อุปกรณ์ เพื่อป้องกันความที่เสียหายที่อาจจะเกิดขึ้นหากเกิดน้ำท่วม			

ขั้นตอนการการดำเนินงานกรณีน้ำท่วม



- **กรณีลิฟต์โดยสารขัดข้อง**

ก่อนเกิดเหตุขัดข้อง

๑) จัดทำคู่มือการปฏิบัติตัวขณะลิฟต์โดยสารขัดข้อง และประชาสัมพันธ์ให้ผู้ใช้งานรับทราบอย่างต่อเนื่อง พร้อมทั้งติดประกาศให้ชัดเจนในลิฟต์

๒) จัดทำและตรวจสอบความชัดเจนของหมายเลขประจำชั้นภายในลิฟต์โดยสาร โดยสามารถมองเห็นได้ทั้งในขณะที่มีไฟส่องสว่างและขณะที่ไฟดับ

๓) จัดเตรียมเครื่องมือสำหรับการใช้งานเพื่อช่วยเหลือผู้ติดค้างในลิฟต์ เช่น บันไดสำหรับออกจากลิฟต์ เป็นต้น

๔) ทำการบำรุงรักษาลิฟต์อย่างสม่ำเสมอ

๕) ติดข้อความห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้ ให้อยู่ในระดับที่สามารถมองเห็นได้ชัดเจน

ขณะเกิดเหตุขัดข้อง

กรณีมีผู้โดยสารติดค้างลิฟต์

๑) แจ้งให้ผู้ที่ติดค้างอยู่ในลิฟต์ห้ามงัดลิฟต์โดยเด็กขาด และแจ้งว่ากำลังดำเนินการแก้ไขให้ภายใน ๑๐ นาที

๒) ตรวจสอบว่าผู้โดยสารติดอยู่ชั้นไหน โดยสอบถามผู้โดยสารและให้ผู้โดยสารมองไปที่สัญลักษณ์แสดงหมายเลขชั้นที่ติดอยู่ในตู้โดยสาร

๓) ผู้ที่ทำการช่วยเหลือทำการปิดระบบไฟฟ้าของอุปกรณ์ เพื่อป้องกันอันตรายหากลิฟต์สามารถใช้งานได้ในขณะที่ทำการช่วยเหลือ

๔) นำกุญแจลิฟต์ที่จัดเก็บไว้ ณ งานบริหารงานทั่วไป มาเปิดลิฟต์ และให้ผู้ที่มีประสบการณ์ในการใช้งานเป็นผู้ดำเนินการเปิดลิฟต์

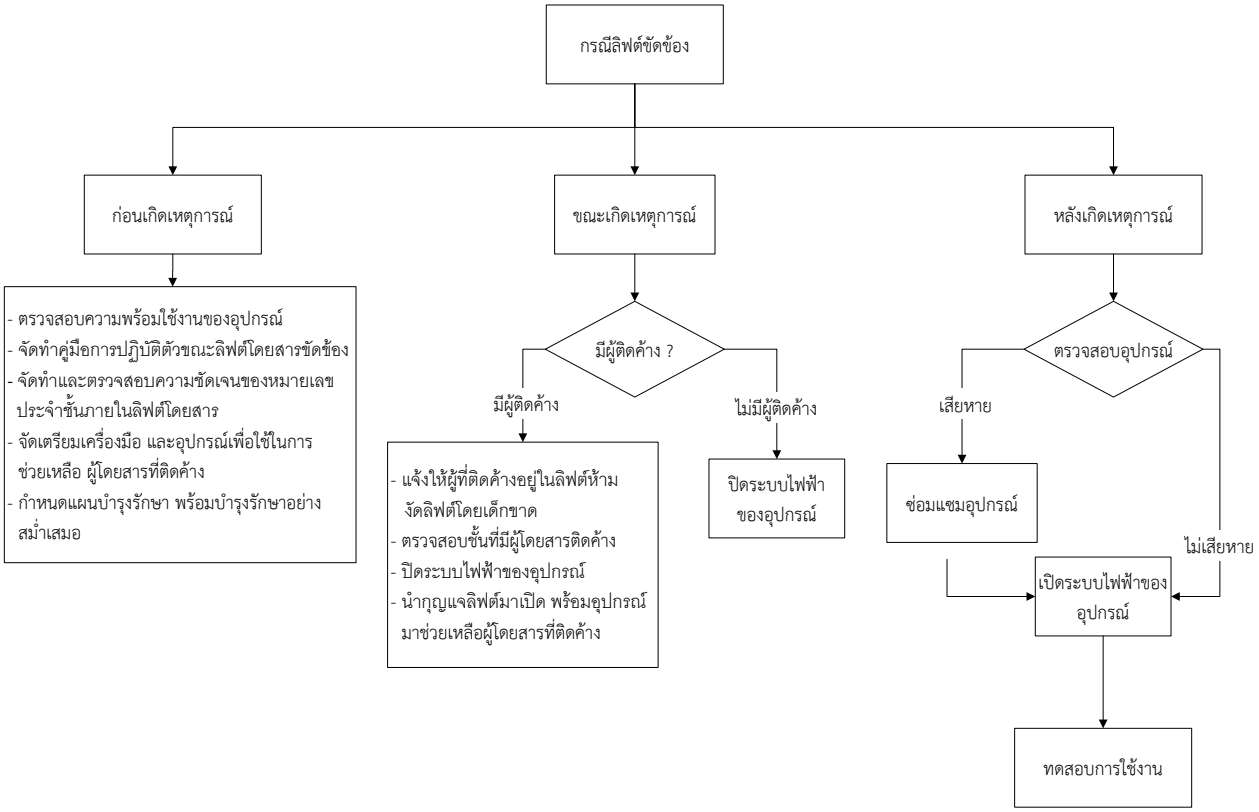
๕) แจ้งให้บริษัทที่รับผิดชอบเข้ามาดำเนินการแก้ไข

หลังเกิดเหตุขัดข้อง

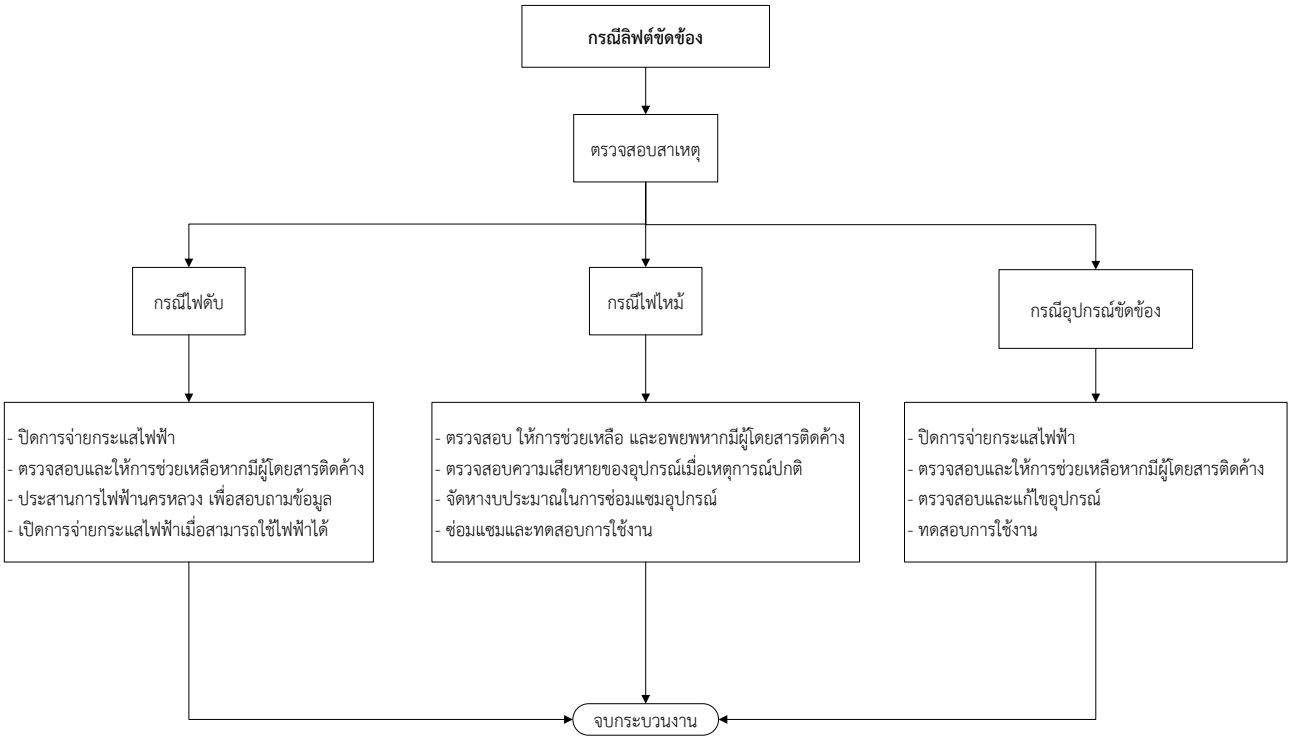
๑) แจ้งบริษัทดำเนินการแก้ไข กรณีลิฟต์ไม่สามารถใช้งานได้ และรายงานผลการแก้ไขให้ผู้ดูแลรับทราบ

๒) จัดทำรายงานการเปลี่ยนแปลง (กรณีไม่สามารถซ่อมแซมได้) ให้ผู้รับผิดชอบรับทราบ

ขั้นตอนการดำเนินการ กรณีลิฟต์โดยสารขัดข้อง



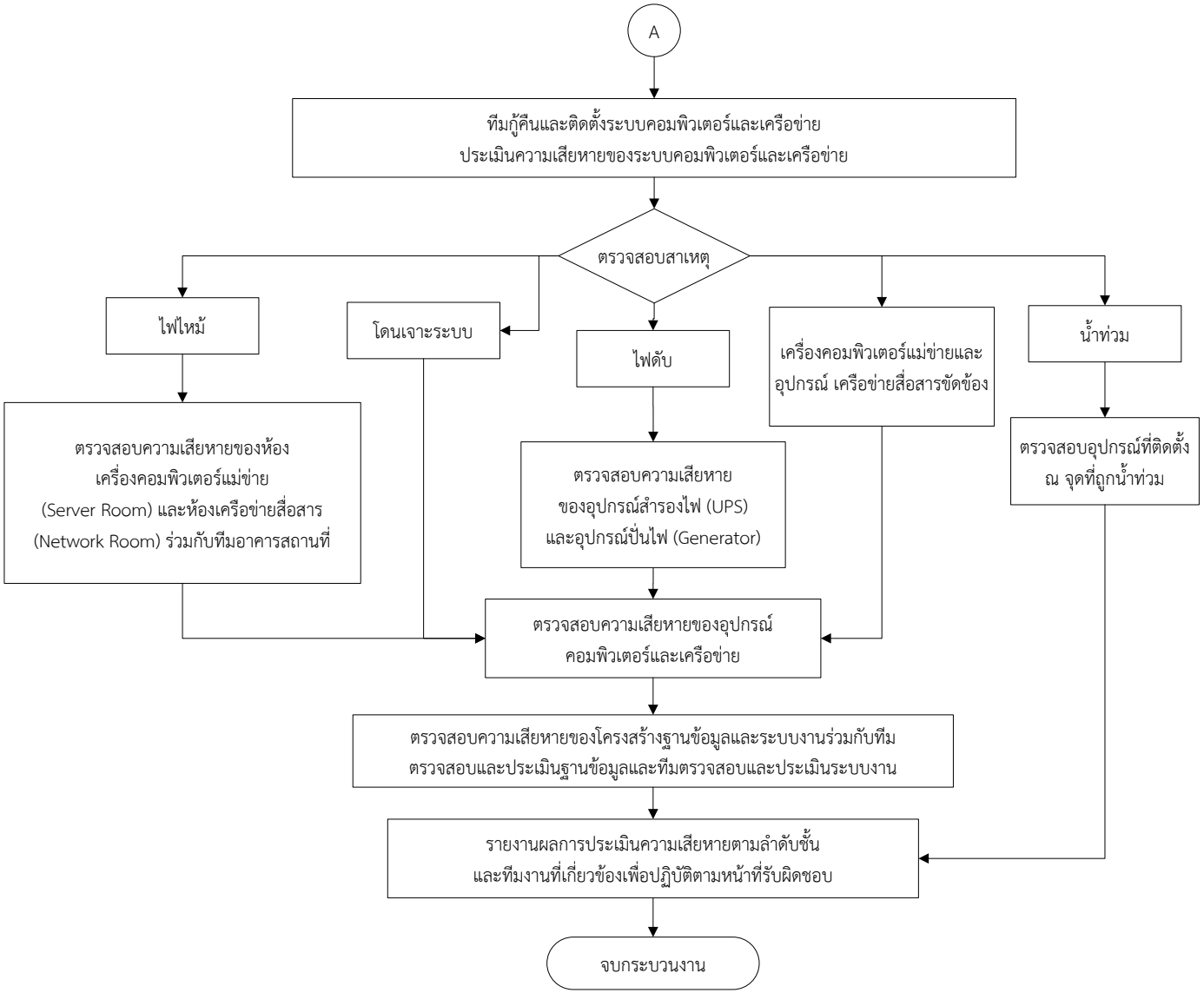
ขั้นตอนการแก้ไขกรณีลิฟต์โดยสารขัดข้องจากสาเหตุต่างๆ



กระบวนการแก้ไขปัญหาจากภัยพิบัติ กรณีลิฟต์ขัดข้อง

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณีลิฟต์	ขณะเกิดปัญหา	ดำเนินการทันที	ทีมกู้คืนและติดตั้ง	
	โดยสาร	๑. เกิดจากอุปกรณ์	เมื่อน้ำท่วม	ระบบคอมพิวเตอร์	
	ขัดข้อง	- ปิดการจ่ายไฟฟ้าให้กับอุปกรณ์		และเครือข่าย	
		- ตรวจสอบมีผู้โดยสารติดค้างหรือไม่			
		** มีผู้โดยสารให้การช่วยเหลือตามขั้นตอน			
		** ไม่มีผู้โดยสารดำเนินการแก้ไข			
		- ดำเนินการแก้ไข			
		- ทดสอบการทำงาน			
		๒. เกิดจากไฟฟ้าขัดข้อง			
		- ปิดการจ่ายไฟฟ้าให้กับอุปกรณ์			
		- ตรวจสอบมีผู้โดยสารติดค้างหรือไม่			
		** มีผู้โดยสารให้การช่วยเหลือตามขั้นตอน			
		** ไม่มีผู้โดยสารดำเนินการแก้ไข			
		- ดำเนินการแก้ไข			
		- ทดสอบการทำงาน			
		๓. เกิดจากไฟไหม้			
		- ปิดการจ่ายไฟฟ้าให้กับอุปกรณ์			
		- ตรวจสอบมีผู้โดยสารติดค้างหรือไม่			
		** มีผู้โดยสารให้การช่วยเหลือตามขั้นตอน			
		** ไม่มีผู้โดยสาร ออกจากที่เกิดเหตุ			

ขั้นตอนการประเมินความเสียหายระบบคอมพิวเตอร์และเครือข่าย



กระบวนการประเมินความเสียหายของระบบคอมพิวเตอร์และเครือข่าย

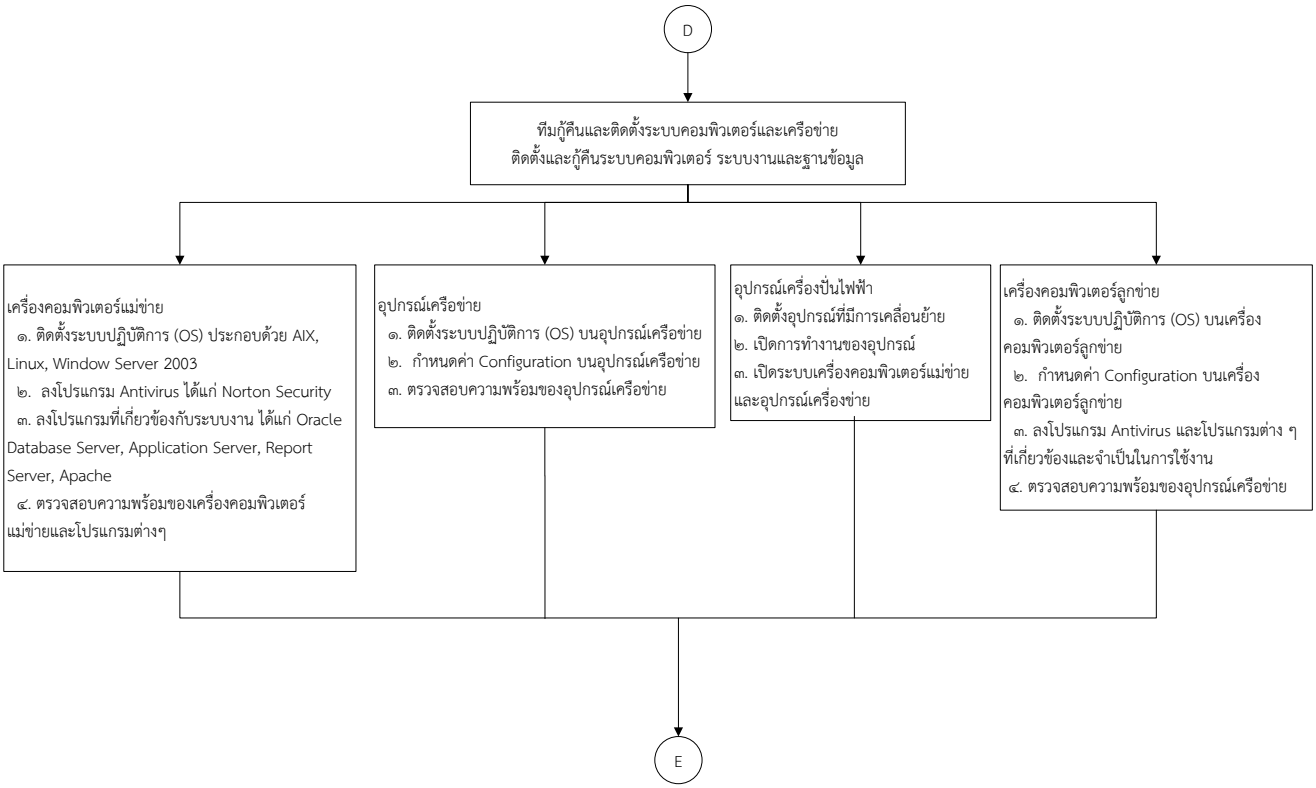
ประเมินความเสียหายของระบบคอมพิวเตอร์และเครือข่าย

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณีไฟไหม้	ดำเนินการประเมินความเสียหาย ดังนี้		ทีมประเมินความ	
	ถูกเจาะระบบ	๑. ไฟไหม้	๕ วัน	เสียหายระบบ	
	ไฟดับ	๑.๑ ตรวจสอบความเสียหายของห้องเครื่องคอมพิวเตอร์แม่ข่าย		คอมพิวเตอร์และ	
	เครื่อง	(Server Room) และห้องเครือข่ายสื่อสาร (Network Room)		เครือข่าย	
	คอมพิวเตอร์	ร่วมกับทีมอาคารสถานที่		ทีมอาคารสถานที่	
	แม่ข่ายและ	๑.๒ ตรวจสอบความเสียหายของอุปกรณ์คอมพิวเตอร์และเครือข่าย		ทีมกู้คืนและติดตั้ง	
	เครือข่าย	ร่วมกับทีมกู้คืนและติดตั้งระบบคอมพิวเตอร์และเครือข่าย		ระบบคอมพิวเตอร์	
	สื่อสาร	๑.๓ ตรวจสอบการทำงานของระบบ ร่วมกับทีมตรวจสอบและ		และเครือข่าย	
	ขัดข้อง	ประเมินระบบงาน		ทีมตรวจสอบและ	
	น้ำท่วม	๒. โดนเจาะระบบ	๑๒ ชั่วโมง	ประเมินระบบงาน	
		๒.๑ ตรวจสอบความเสียหายของอุปกรณ์คอมพิวเตอร์และเครือข่าย		ทีมตรวจสอบและ	
		ร่วมกับทีมกู้คืน และติดตั้งระบบคอมพิวเตอร์และเครือข่าย		ประเมินฐานข้อมูล	
		๒.๒ ตรวจสอบการทำงานของระบบ ร่วมกับทีมตรวจสอบและ		ทีมบริหารจัดการ	
		ประเมินระบบงาน		เครื่องคอมพิวเตอร์	
		๒.๓ ตรวจสอบความครบถ้วนถูกต้องของข้อมูล ร่วมกับ		และอุปกรณ์	
		ทีมตรวจสอบและประเมินฐานข้อมูล			
		๓. ไฟดับ	๔ – ๑๒ ชั่วโมง		
		๓.๑ ตรวจสอบการทำงานของเครื่องสำรองไฟ (UPS) ร่วมกับ			
		ทีมอาคารสถานที่			

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
		๓.๒ ตรวจสอบการทำงานของเครื่องปั่นไฟ (Generator) ร่วมกับ			
		ทีมอาคารสถานที่			
		๓.๓ ตรวจสอบความเสียหายของอุปกรณ์คอมพิวเตอร์และเครือข่าย			
		ร่วมกับทีมกู้คืน และติดตั้งระบบคอมพิวเตอร์และเครือข่าย			
		๓.๔ ตรวจสอบการทำงานของระบบ ร่วมกับทีมตรวจสอบและ			
		ประเมินระบบงาน			
		๓.๕ ตรวจสอบความครบถ้วนถูกต้องของข้อมูล ร่วมกับ			
		ทีมตรวจสอบและประเมินฐานข้อมูล			
		๔. น้ำท่วม	๒ – ๓ ชั่วโมง		
		๔.๑ ตรวจสอบสถานที่และตำแหน่งที่ติดตั้งอุปกรณ์ ร่วมกับ			
		ทีมอาคารสถานที่			
		๔.๒ ประเมินสถานการณ์ เคลื่อนย้ายอุปกรณ์ที่สามารถ			
		เคลื่อนย้ายได้ และติดตั้งอุปกรณ์ป้องกัน			
		๔.๓ ตรวจสอบความเสียหายของอุปกรณ์ที่ไม่สามารถเคลื่อนย้ายได้			
		ร่วมกับทีมกู้คืนและติดตั้งระบบคอมพิวเตอร์และเครือข่าย			
		๕. เครื่องคอมพิวเตอร์แม่ข่าย และการสื่อสารขัดข้อง	๔ – ๖ ชั่วโมง		
		๕.๑ ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย และ			
		อุปกรณ์ที่เกี่ยวข้อง			
		๕.๒ ตรวจสอบการทำงานของอุปกรณ์เครือข่าย และอุปกรณ์			
		ที่เกี่ยวข้อง			
		๕.๓ ตรวจสอบความครบถ้วน ถูกต้องของระบบ โปรแกรม และ			
		ข้อมูล ร่วมกับทีมกู้คืนและติดตั้งระบบคอมพิวเตอร์และเครือข่าย			

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
		๖. รายงานผลการประเมินความเสียหายตามลำดับชั้น และ	๕ วัน		
		แจ้งผู้เกี่ยวข้องดำเนินการต่อไป ประกอบด้วย			
		๖.๑ ผลการตรวจสอบความเสียหายของเครื่องคอมพิวเตอร์แม่ข่าย			
		(Server Room) และห้องเครือข่ายสื่อสาร (Network Room)			
		๖.๒ ผลการตรวจสอบความเสียหายของอุปกรณ์คอมพิวเตอร์และ			
		เครือข่าย			
		๖.๓ ผลการตรวจสอบความเสียหายของระบบงาน			
		๖.๔ ผลการตรวจสอบความเสียหายของฐานข้อมูล			
		๖.๕ ผลการตรวจสอบความเสียหายของเครื่องสำรองไฟ (UPS)			
		และอุปกรณ์ปั่นไฟ (Generator)			

ขั้นตอนกระบวนการแก้ไขปัญหาจากภัยพิบัติ การติดตั้งและการกู้คืนระบบ



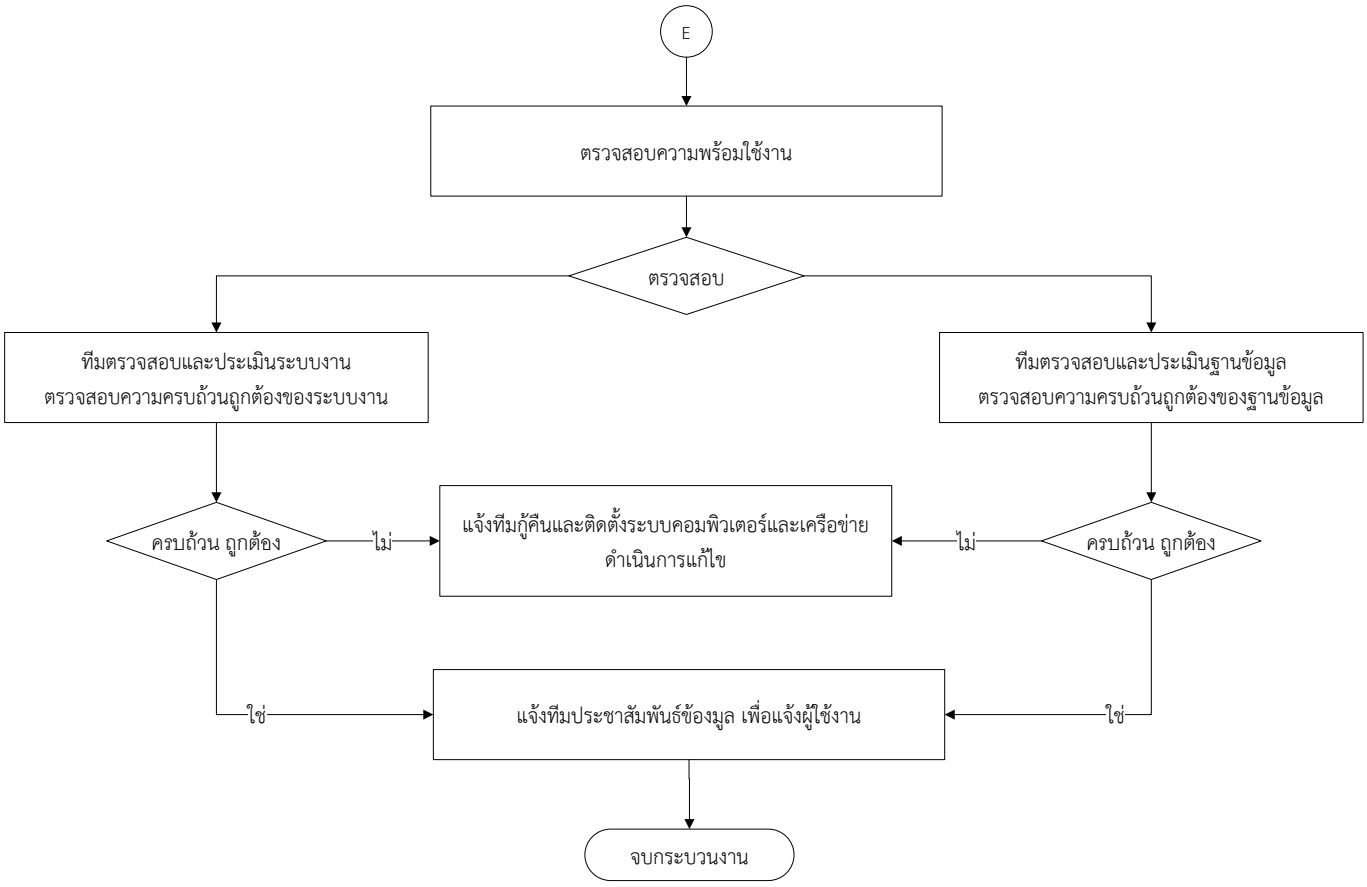
กระบวนการแก้ไขปัญหาจากภัยพิบัติ ติดตั้งและกู้คืนระบบ

กระบวนการแก้ไขปัญหาจากภัยพิบัติ ติดตั้งและกู้คืนระบบ

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณีไฟไหม้	ดำเนินการติดตั้งระบบคอมพิวเตอร์และโปรแกรม ดังนี้	๔ – ๑๒ ชั่วโมง	ทีมกู้คืนและติดตั้ง	ดำเนินการ
	กรณีโดน	เครื่องคอมพิวเตอร์แม่ข่าย		ระบบคอมพิวเตอร์	ตรวจสอบตาม
	เจาะระบบ	๑. ติดตั้งระบบปฏิบัติการ (OS) ประกอบด้วย AIX, Linux,		และเครือข่าย	คู่มือการ
	กรณีเครื่อง	Window Server ๒๐๐๓		ทีมบริหารจัดการ	ปฏิบัติงาน
	คอมพิวเตอร์	๒. ลงโปรแกรม Antivirus ได้แก่ NOD ,McAfee		เครื่องคอมพิวเตอร์	ศทส.
	แม่ข่ายและ	๓. ลงโปรแกรมที่เกี่ยวข้องกับระบบงาน ได้แก่ Oracle Database		และอุปกรณ์	
	เครือข่าย	Server, Application Server, Report Server, Apache			
	สื่อสาร	๔. ตรวจสอบความพร้อมเครื่องคอมพิวเตอร์แม่ข่าย			
	ขัดข้อง	อุปกรณ์เครือข่าย			
	น้ำท่วม	๑. ติดตั้งระบบปฏิบัติการ (OS) บนอุปกรณ์เครือข่าย			
		๒. กำหนดค่า Configuration บนอุปกรณ์เครือข่าย			
		๓. ตรวจสอบความพร้อมของอุปกรณ์เครือข่าย			
		อุปกรณ์เครื่องปั่นไฟฟ้า			
		๑. ติดตั้งอุปกรณ์ที่มีการเคลื่อนย้าย			
		๒. เปิดการทำงานของอุปกรณ์			
		๓. เปิดระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย			
		เครื่องคอมพิวเตอร์ลูกข่าย			
		๑. ติดตั้งระบบปฏิบัติการ (OS) บนเครื่องคอมพิวเตอร์ลูกข่าย			
		๒. กำหนดค่า Configuration บนเครื่องคอมพิวเตอร์ลูกข่าย			

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
		๓. ลงโปรแกรม Antivirus และโปรแกรมต่าง ๆ ที่เกี่ยวข้อง			
		และจำเป็นในการใช้งาน			
		๔. ตรวจสอบความพร้อมของอุปกรณ์เครือข่าย			

ขั้นตอนกระบวนการแก้ไขปัญหาจากภัยพิบัติ ตรวจสอบความพร้อมใช้งาน



กระบวนการแก้ไขปัญหาจากภัยพิบัติ ตรวจสอบความพร้อมใช้งาน

กระบวนการแก้ไขปัญหาจากภัยพิบัติ ตรวจสอบความพร้อมใช้งาน

เหตุการณ์	สาเหตุ	การแก้ไขปัญหา	ระยะเวลาดำเนินงาน	ผู้รับผิดชอบ	หมายเหตุ
เกิดภัยพิบัติ	กรณีไฟไหม้	ดำเนินการตรวจสอบ ดังนี้		ทีมกู้คืนและติดตั้ง	
	กรณีโดน	๑. ทีมตรวจสอบและประเมินระบบงาน ตรวจสอบความถูกต้อง	๒ ชั่วโมง	ระบบคอมพิวเตอร์	
	เจาะระบบ	ครบถ้วนของระบบงานที่กู้คืน		และเครือข่าย	
	กรณีเครื่อง	๑.๑ ไม่ครบถ้วน แจ้งทีมกู้คืนและติดตั้งระบบคอมพิวเตอร์และ	๔ ชั่วโมง	ทีมตรวจสอบและ	
	คอมพิวเตอร์	เครือข่ายดำเนินการตรวจสอบ		ประเมินระบบงาน	
	แม่ข่ายและ	๑.๒ ครบถ้วน แจ้งทีมประชาสัมพันธ์ข้อมูล แจ้งผู้ใช้งาน		ทีมตรวจสอบและ	
	การสื่อสาร	๒. ทีมตรวจสอบและประเมินฐานข้อมูล ตรวจสอบความถูกต้อง	๔ ชั่วโมง	ประเมินฐานข้อมูล	
	ขัดข้อง	ครบถ้วน ของฐานข้อมูลที่กู้คืน		ทีมประชาสัมพันธ์	
		๒.๑ ไม่ครบถ้วน แจ้งทีมกู้คืนและติดตั้งระบบคอมพิวเตอร์และ	๘ ชั่วโมง	ข้อมูล	
		เครือข่ายดำเนินการตรวจสอบ			
		๒.๒ ครบถ้วน แจ้งทีมประชาสัมพันธ์ข้อมูล แจ้งผู้ใช้งาน			

๙. การทดสอบแผนแก้ไขปัญหาสถานการณ์ความไม่แน่นอนและภัยพิบัติ

ปีงบประมาณ	เหตุการณ์	วัน – เวลาในการทดสอบ	หมายเหตุ
๒๕๖๕	๑. กรณีโดนเจาะระบบ	ดำเนินการทดสอบทุก ๖ เดือน (ประมาณเดือนมกราคม และกรกฎาคม)	จำลองและปฏิบัติตามขั้นตอนตามแผนการทดสอบกรณีการโดนเจาะระบบ
	๒. กรณีเครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายสื่อสารขัดข้อง	สิงหาคม	ปฏิบัติตามขั้นตอนทุกครั้งที่เครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายสื่อสารขัดข้อง
	๓. กรณีไฟดับ	สิงหาคม	มีการปฏิบัติตามขั้นตอนทุกครั้งที่กระแสไฟฟ้าดับ
	๔. กรณีลิฟต์โดยสารขัดข้อง	สิงหาคม	ดำเนินการตามแผนกรณีลิฟท์โดยสารขัดข้อง
	๕. กรณีไฟไหม้	กันยายน	ดำเนินการตามแผนซักซ้อมการหนีไฟ
	๖. กรณีน้ำท่วม	กันยายน	มีขั้นตอนเพื่อศึกษาและการปฏิบัติตามขั้นตอนเมื่อเกิดกรณีน้ำท่วม

๑๐. การทบทวน ตรวจสอบและปรับปรุงแผน

ศูนย์เทคโนโลยีสารสนเทศ ทำการทบทวน ตรวจสอบและปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ปีละ ๑ ครั้ง

แผนบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
กรมการขนส่งทางบก

จัดทำโดย

ศูนย์เทคโนโลยีสารสนเทศ

กรมการขนส่งทางบก

ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

คำนำ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมการขนส่งทางบก จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ และการสื่อสาร ซึ่งการกำหนดวัตถุประสงค์มนการจัดทำแผนดังกล่าวได้ทำการวิเคราะห์สถานภาพของระบบสารสนเทศ กรมการขนส่งทางบก ทั้งในด้านโครงสร้างพื้นฐาน ระบบเครือข่ายสื่อสารข้อมูล สถานภาพศูนย์คอมพิวเตอร์ (Data Center) ระบบรักษาความมั่นคงปลอดภัย และศูนย์คอมพิวเตอร์สำรอง เพื่อวิเคราะห์ระบบสารสนเทศของกรมการขนส่งทางบก และพิจารณาความเสี่ยงในองค์ประกอบอื่นๆ รวมทั้งได้จัดทำแนวทางในการบริหารความเสี่ยงที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมการขนส่งทางบก เพื่อลดความสูญเสียหรือความเสียหายที่อาจจะเกิดขึ้น

ศูนย์เทคโนโลยีสารสนเทศ
กรมการขนส่งทางบก
สิงหาคม ๒๕๖๔

สารบัญ

แผนบริหารความเสี่ยงด้านระบบสารสนเทศกรมการขนส่งทางบก

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสาร มีบทบาทสำคัญต่อการดำเนินงานตามภารกิจของหน่วยงานทั้งในภาครัฐและภาคเอกชน ซึ่งหน่วยงานต้องมีการจัดการความเสี่ยงที่อาจจะเกิดขึ้นกับเทคโนโลยีสารสนเทศและการสื่อสารที่นำมาใช้

กรมการขนส่งทางบกเป็นอีกหน่วยงานหนึ่งที่นำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ในการดำเนินการให้เป็นไปตามภารกิจของกรมฯ จึงได้ตระหนักและเห็นความสำคัญของการบริหารความเสี่ยง จึงจัดให้มีการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศขึ้น เพื่อการบริหารปัจจัยและควบคุม กิจกรรม รวมทั้งกระบวนงานต่าง ๆ โดยลดโอกาส และผลกระทบที่อาจจะเกิดขึ้นในอนาคตให้อยู่ในระดับที่ยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามยุทธศาสตร์เป็นอันดับแรก และเป้าหมายตามแผนการปฏิบัติราชการ

การบริหารความเสี่ยงเป็นการพิจารณาว่าจะมีสิ่งใด เหตุการณ์ใดที่อาจจะเป็นปัญหา อุปสรรค ทำให้ไม่สามารถบรรลุเป้าหมาย และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจหลักตามกฎหมายจัดตั้งส่วนราชการ และเป้าหมายตามแผนปฏิบัติราชการ

วิสัยทัศน์ พันธกิจ และยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

วิสัยทัศน์กรมการขนส่งทางบก

เป็นองค์กรแห่งนวัตกรรมในการควบคุม กำกับ ดูแล ระบบการขนส่งทางถนนให้มีคุณภาพและปลอดภัย

วิสัยทัศน์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

มุ่งพัฒนาเทคโนโลยีสารสนเทศเชิงรุกบูรณาการสารสนเทศ และองค์ความรู้อย่างมืออาชีพ สู่การให้บริการด้วยคุณภาพที่เป็นเลิศของกรมการขนส่งทางบก

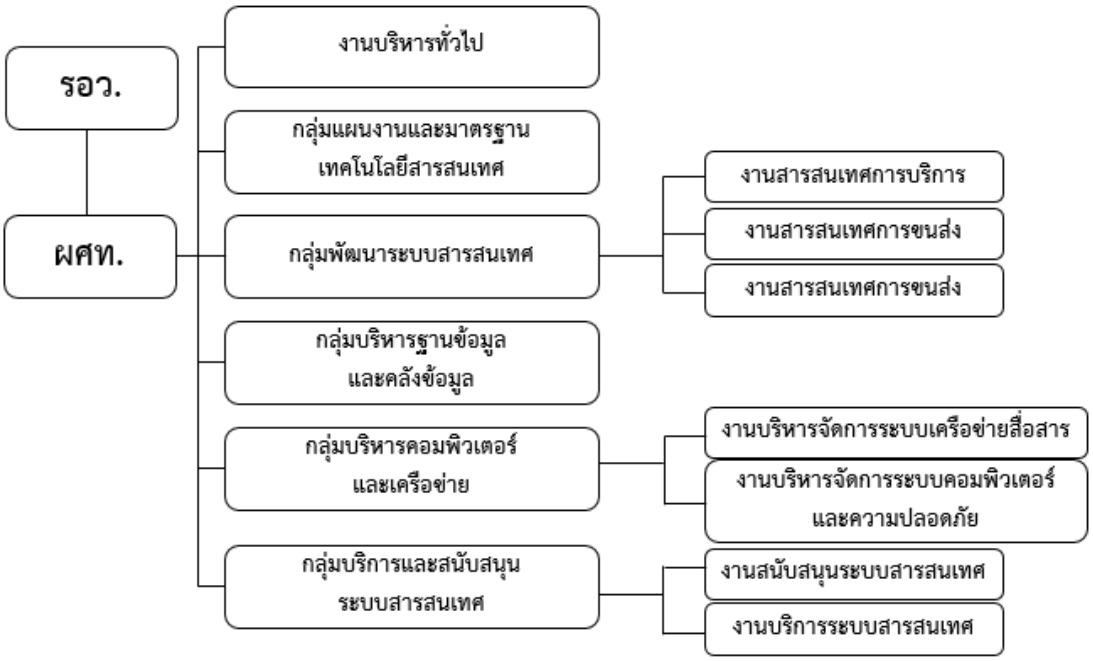
พันธกิจ

๑. จัดหาและให้บริการระบบสารสนเทศ เพื่อสนับสนุนงานบริหารและงานบริการของกรมการขนส่งทางบกได้อย่างบูรณาการ มีเสถียรภาพ มีประสิทธิภาพ และสร้างความพึงพอใจแก่ผู้รับบริการ
๒. ศึกษา วิเคราะห์ ปรับปรุงและพัฒนาระบบสารสนเทศ เพื่อสนับสนุนกระบวนการทำงาน การบริหารและการบริการของกรมการขนส่งทางบกให้มีประสิทธิภาพตามมาตรฐานสากล
๓. เป็นศูนย์กลางองค์ความรู้ด้านเทคโนโลยีสารสนเทศของกรมการขนส่งทางบก
๔. พัฒนาระบบเชื่อมโยงองค์ความรู้ สู่การเป็นศูนย์กลางในการสนับสนุนการทำงานของเครือข่ายความร่วมมือทั้งในและต่างประเทศ
๕. เตรียมความพร้อมด้านเทคโนโลยีสารสนเทศให้กับบุคลากรให้สามารถทำงานได้อย่างมีประสิทธิภาพ

ยุทธศาสตร์

๑. พัฒนาและปรับปรุงคุณภาพข้อมูลและระบบสารสนเทศให้สามารถประยุกต์ใช้ให้เกิดประโยชน์อย่างเต็มรูปแบบ
๒. พัฒนาเทคโนโลยีสารสนเทศเพื่อก้าวไปข้างหน้าทั้งด้านการบริหาร และการให้บริการอย่างมีมาตรฐาน
๓. มุ่งพัฒนาคน กระบวนการทำงาน และการให้บริการที่มีประสิทธิภาพได้มาตรฐานสากล

โครงสร้างการบริหารงานศูนย์เทคโนโลยีสารสนเทศ



วัตถุประสงค์ของการบริหารความเสี่ยง

๑. เพื่อให้การจัดการภายในศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบก มีประสิทธิภาพ และมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศของกรมการขนส่งทางบก

๒. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของกรมการขนส่งทางบก

๓. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการด้านเทคโนโลยีสารสนเทศ

๔. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบสารสนเทศของกรมการขนส่งทางบก

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหาร และผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของกรมการขนส่งทางบก

๖. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

นิยามและความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายของหน่วยงาน ทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเนิบผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุต้องเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการเพื่อให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่หน่วยงานยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับการลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยงและทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

ประเภทความเสี่ยง

ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สามารถแบ่งออกได้เป็น ๗ ประเภท คือ

๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม
๒. ความเสี่ยงด้านบุคลากร
๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ
๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์
๕. ความเสี่ยงด้านระบบฐานข้อมูล
๖. ความเสี่ยงด้านกลยุทธ์
๗. ความเสี่ยงด้านการเงิน

๑. <u>ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม</u>

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การไม่มีระบบรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย และการก่อการร้าย

๒. <u>ความเสี่ยงด้านบุคลากร</u>

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ การวางแผน การตรวจสอบ การทำงาน การมอบหมายหน้าที่และสิทธิของบุคลากร/คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ล้วน เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบสารสนเทศ รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งเป็นความเสี่ยงทั้งสิ้น

๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่อง อุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ ไวรัสคอมพิวเตอร์

๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่าง ๆ การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง การถูกผู้ไม่หวังดีทำลายระบบ (Hacker)

๕. ความเสี่ยงด้านระบบข้อมูล

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบสารสนเทศอันอาจจะก่อให้เกิดความเสียหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล การโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ความเสี่ยงเหล่านี้ล้วนมีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล

๖. ความเสี่ยงด้านกลยุทธ์

หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหาร องค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่าง ๆ ในด้านเทคโนโลยีสารสนเทศ ทำให้การกำหนดยุทธศาสตร์และกลยุทธ์เปลี่ยนแปลงไป

๗. ความเสี่ยงด้านการเงิน

หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยงตามมาตรฐานของ COSO (Committee of Sponsoring Organizations of the Tread way Commission) คือ

๑. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
๒. การระบุความเสี่ยง (Event Identification)
๓. การประเมินความเสี่ยง (Risk Assessment)
๔. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
๔. กิจกรรมการบริหารความเสี่ยง (Control Activities)
๖. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
๗. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

๑. การกำหนดเป้าหมายการบริหารความเสียง (Objective Setting) วัตถุประสงค์ของแต่ละกิจกรรมที่กำหนดไว้ จะต้องสนับสนุนและสอดคล้องต่อการบรรลุวัตถุประสงค์ของการดำเนินงานในภาพรวมขององค์กร เพื่อให้การดำเนินงานบรรลุเป้าหมายหรือตัวชี้วัด ดังต่อไปนี้

๑. การบรรลุเป้าหมายและพันธกิจในภาพรวม (Strategic Risk : S)
๒. ประสิทธิผลและประสิทธิภาพของการปฏิบัติงาน (Operational Risk : O)
๓. การบริหารงบประมาณและการเงิน (Financial Risk : F)
๔. การปฏิบัติตามกฎหมาย ระเบียบปฏิบัติ และนโยบาย (Compliance Risk : c)

ซึ่งการกำหนดวัตถุประสงค์ของแต่ละกิจกรรมนั้น ต้องมีลักษณะดังนี้

๑. มีการกำหนดเป้าหมายและตัวชี้วัดความสำเร็จที่ชัดเจนและสามารถวัดผลได้

๒. สามารถปฏิบัติได้ตามที่กำหนด

๓. มีการกำหนดระยะเวลาที่แน่นอน

๒. การระบุความเสี่ยง (Event Identification) เป็นขั้นตอนที่สำคัญมากสำหรับการบริหารความเสี่ยงขององค์การ เพราะถ้าหากการระบุความเสี่ยงไม่ได้รับการศึกษาอย่างละเอียดถี่ถ้วนแล้ว ความเสี่ยงซึ่งไม่ปรากฏในขั้นตอนนี้จะกลายเป็นความเสี่ยงที่เหลืออยู่กับองค์การโดยไม่ได้รับการวิเคราะห์วางแผนการจัดการใด ๆ ซึ่งความเสี่ยงเหล่านี้อาจนำมาซึ่งความสูญเสียที่ยิ่งใหญ่ต่อองค์การได้ ในขั้นตอนการระบุความเสี่ยงขององค์การนี้ทางทีมบริหารความเสี่ยงจึงต้องให้ความสำคัญกับการระบุความเสี่ยงทั้งหมดที่องค์การเผชิญ ระบุความเสี่ยงให้ได้มากที่สุดเท่าที่จะมากได้

๓. การประเมินความเสี่ยง (Risk Assessment) เป็นการประเมินค่าความเสี่ยงที่เกิดขึ้นในแต่ละด้าน โดยพิจารณาจากปัจจัยต่าง ๆ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ โดยมีแนวทางการดำเนินการจากหลักเกณฑ์ดังนี้

๓.๑ หลักเกณฑ์การประเมินระดับความเสี่ยง (Risk Score) โดยกำหนดหลักเกณฑ์การประเมินระดับความเสี่ยงไว้ ดังนี้

ระดับ	เกณฑ์ในการประเมินโอกาส (Likelihood)	ผลกระทบของเหตุการณ์ (Impact)
๕	เกิดขึ้นเป็นประจำ	สูงมาก
๔	เกิดขึ้นบ่อย	สูง
๓	เกิดขึ้นปานกลาง	ปานกลาง
๒	เกิดขึ้นได้บ้าง	น้อย
๑	เกิดขึ้นได้น้อยมาก หรือไม่น่าเกิด	น้อยมาก หรือไม่ส่งผลกระทบ

๓.๒ การจัดลำดับความเสี่ยง โดยพิจารณาจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยง ผลจากการระบุความเสี่ยงและการประเมินความเสี่ยงข้างต้น ทำให้ผู้บริหารความเสี่ยงทราบถึงความสำคัญที่ไม่เท่ากันของความเสียงแต่ละเรื่องที่จะเกิดขึ้นในอนาคต ทำให้ได้ข้อมูลเบื้องต้นเพื่อจัดทำแผนภูมิการบริหารความเสี่ยง

การประเมินระดับความเสี่ยง (Risk Score) จะแบ่งระดับของความเสี่ยงออกเป็น ๔ ระดับ และมีค่าความเสี่ยงรวมเท่ากับ ๒๕ คะแนน (Level of Risk) โดยการนำผลที่ได้จากการประเมินความ เป็นไปได้และผลกระทบมาจัดทำแผนผังประเมินความเสี่ยง (Risk Assessment Matrix) เพื่อแสดงถึงความถี่และความรุนแรงของเหตุการณ์นั้น ๆ โดยมีค่าโอกาสและผลกระทบจากต่ำสุดมีค่าเท่ากับ ๑ ถึงสูงสุดมี ค่าเท่ากับ ๔ แผนภูมิความเสี่ยงจะมีความละเอียดมากขึ้น ดังนี้

แผนภูมิความเสี่ยง (Risk Assessment Matrix)

โอกาส					
๕	๑X๕ = ๕	๒X๕ = ๑๐	๓X๕ = ๑๕	๔X๕ = ๒๐	๕X๕ = ๒๕
๔	๑X๔ = ๔	๒X๔ = ๘	๓X๔ = ๑๒	๔X๔ = ๑๖	๕X๔ = ๒๐
๓	๑X๓ = ๓	๒X๓ = ๖	๓X๓ = ๙	๔X๓ = ๑๒	๕X๓ = ๑๕
๒	๑X๒ = ๒	๒X๒ = ๔	๓X๒ = ๖	๔X๒ = ๘	๕X๒ = ๑๐
๑	๑X๑ = ๑	๒X๑ = ๒	๓X๑ = ๓	๔X๑ = ๔	๕X๑ = ๕
ผลกระทบ	๑	๒	๓	๔	๕

๓.๓ <u>การกำหนดความเสี่ยงที่องค์กรยอมรับได้</u> ศูนย์เทคโนโลยีสารสนเทศ ได้กำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite) ไว้ดังนี้

ระดับความเสี่ยง	ระดับคะแนน	แทนด้วยแถบสี	ความหมาย
ต่ำ	๑ - ๔	เขียว	ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม
ปานกลาง	๕ - ๙	ฟ้า	ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
สูง	๑๐ - ๑๖	ส้ม	<u>ระดับที่ไม่สามารถยอมรับได้</u> โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
สูงมาก	๒๐ - ๒๕	แดง	<u>ระดับที่ไม่สามารถยอมรับได้</u> จำเป็นต้องเร่งจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ทันที

๔. <u>การจัดการความเสี่ยง (Risk Response)</u> มีวัตถุประสงค์ของการตอบสนองความเสี่ยง ดังนี้

- ลดโอกาสเกิดความเสี่ยงและผลกระทบของความเสียงให้เหลือน้อยที่สุด โดยการจัดการ สาเหตุของความเสี่ยงอย่างมีประสิทธิภาพ หรือจัดการผลกระทบที่อาจจะเกิดขึ้นของความเสี่ยง
- การลดผลกระทบของความเสียง การจัดทำแผนฉุกเฉิน หรือแผนฟื้นฟู เพื่อให้เกิดผลกระทบน้อยที่สุด
- การเพิ่ม/สร้าง หรือจัดการโอกาสเกิดความเสี่ยงและผลกระทบจากความเสี่ยง เพื่อให้ได้ผลลัพธ์ที่ดีขึ้น

๕. กิจกรรมการบริหารความเสี่ยง (Control Activities) เมื่อได้ทางเลือกที่เหมาะสมในการบริหารความเสี่ยง คณะทำงานบริหารความเสี่ยงต้องกำหนดแผนการบริหารความเสี่ยงจำแนกตามโครงการ หรือบางกิจกรรมที่สามารถนำมารวมเป็นแผนบริหารความเสี่ยงเดียวกันได้ แต่ละหน่วยงานที่เกี่ยวข้องจะต้องร่วมปฏิบัติ ความเสี่ยงบางรายการเป็นความเสี่ยงเฉพาะที่เกิดจากหน่วยงานใดหน่วยงานหนึ่งในองค์การเท่านั้น แต่ความเสี่ยงหลายรายการเป็นความเสี่ยงที่ทุกฝ่ายมีส่วนก่อให้เกิดการน่าแผนกลยุทธ์การบริหารความเสี่ยงไปสู่การปฏิบัติ จึงต้องอาศัยความเข้าใจและความร่วมมือจากทุกฝ่ายที่เกี่ยวข้อง ทั้งนี้ แผนบริหารความเสี่ยงต้องสอดคล้องกับผลการวิเคราะห์ความเสี่ยงดังกล่าว และมีการกำหนดตัวชี้วัดความสำเร็จของเป้าหมายของแผนอย่างชัดเจน รวมทั้งเกณฑ์การให้คะแนนของค่าเป้าหมายตัวชี้วัดดังกล่าว

๖. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication) ซึ่งเป็นหัวใจของการบริหารความเสี่ยงในทุก ๆ ขั้นตอน การสื่อสารมีวัตถุประสงค์เพื่อต้องการให้ทุกฝ่ายที่เกี่ยวข้องได้รับความเข้าใจที่ตรงกันอย่างทั่วถึง โดยมีข้อมูลความเสี่ยงของโครงการ ทางเลือกในการลดปัญหาความเสี่ยง ข้อมูลของความเสี่ยงในลักษณะต่าง ๆ และทำการตัดสินใจได้ดีที่สุดภายใต้ข้อจำกัดของแต่ละโครงการ ซึ่งการติดต่อสื่อสารและเอกสารที่เกี่ยวข้องนับว่ามีความสำคัญยิ่งต่อความสำเร็จของแต่ละขั้นตอนในกระบวนการบริหารความเสี่ยงของแต่ละโครงการ

ปัจจัยเสี่ยง

ปัจจัยเสี่ยงที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายสื่อสารหลัก ระบบฐานข้อมูลหลัก ระบบสารสนเทศที่พัฒนาขึ้นเพื่อใช้งานตามภารกิจของกรมการขบส่งทางบก ได้แก่

ปัจจัยภายนอก ได้แก่

๑. ภัยธรรมชาติ และสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องคอมพิวเตอร์แม่ข่ายหลัก (Server) ของระบบฐานข้อมูล และอุปกรณ์เครือข่ายสื่อสารหลัก เหตุการณ์ไฟไหม้ วาตภัย อุตกภัย

๒. การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล และอุปกรณ์เครือข่ายสื่อสารหลักของกรมฯ

๓. การชำรุด เสียหายของตัวเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายสื่อสาร อันเกิดจากการเคลื่อนย้าย หรือการกระทำการใด ๆ ที่ส่งให้อุปกรณ์ดังกล่าวเกิดความเสียหาย

๔. ระบบเครือข่ายสื่อสารหลักเกิดการเสียหาย หรือเกิดการขัดข้อง อันเนื่องจากสาเหตุอื่น ๆ ที่ไม่สามารถควบคุมได้

๕. ระบบกระแสไฟฟ้าขัดข้อง หรือไฟฟ้าตับ

ปัจจัยภายใน ได้แก่

๑. ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒. การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่าง ๆ

๓. การถูกเจาะระบบหรือลักลอบเข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอกโดยไม่ได้รับอนุญาต

การประเมินความเสียหาย

๑. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมขาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒. ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดขอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบบ

ขอบเขตการดำเนินการ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศฉบับนี้ เนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดขอบของศูนย์เทคโนโลยีสารสนเทศ กรมการขนส่งทางบก

การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมการขนส่งทางบก

จากกระบวนการบริหารความเสี่ยงตามมาตรฐานของ COSO (Committee of Sponsoring Organizations of the Tread way Commission) คณะกรรมการบริหารความเสี่ยงของศูนย์เทคโนโลยีสารสนเทศ ได้ทำการวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้น ดังนี้

กิจกรรม	วัตถุประสงค์	ความเสี่ยง /ปัจจัยเสี่ยง	ผลกระทบ/ ผู้ได้รับผลกระทบ
ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	เพื่อรองรับนโยบายเร่งด่วน นโยบายที่ปรับเปลี่ยน หรือผลกระทบจากปัจจัยภายนอกอื่นๆ	การเปลี่ยนแปลงผู้บริหารอาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ
ความเสี่ยงจากภัยธรรมชาติ	เพื่อรับมือกับเหตุการณ์ภัยธรรมชาติที่อาจเกิดขึ้นกับระบบสารสนเทศ	การเกิดไฟไหม้อาคาร แผ่นดินไหว จนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ
ความเสี่ยงจากเหตุการณ์บ้านเมือง	เพื่อให้มีแผนรองรับหากเกิดเหตุการณ์ความไม่สงบในบ้านเมือง	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ

กิจกรรม	วัตถุประสงค์	ความเสี่ยง /ปัจจัยเสี่ยง	ผลกระทบ/ ผู้ได้รับผลกระทบ
ความเสี่ยงด้านบุคลากร	เพื่อให้มีบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสารที่มีความเชี่ยวชาญ	จำนวนบุคลากรที่มีไม่เพียงพอต่อระบบสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ
ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	เพื่อให้มีงบประมาณในการบริหารจัดการระบบสารสนเทศ	การขาดแคลนงบประมาณในการ ดำเนินการให้ระบบสารสนเทศ สามารถดำเนินการได้ต่อเนื่อง อย่างมีประสิทธิภาพ	- ผู้ใช้งาน - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ
การป้องกันการถูกบุกรุก/โจมตีจากภายนอก	ป้องกัน/แก้ไขปัญหาที่เกิดจากการถูกผู้ไม่ประสงค์ดีบุกรุก/โจมตี	ไม่มีเครื่องมือในการตรวจจับการ ถูกบุกรุก/โจมตีจากผู้ไม่ประสงค์ดี	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ
ระบบสารสนเทศให้บริการได้ตลอดเวลา	เพื่อให้กรมฯ สามารถให้บริการประชาชนได้ตลอดเวลา	กรมฯ ไม่สามารถให้บริการได้เนื่องจาก - กระแสไฟฟ้าขัดข้อง - เครื่องแม่ข่ายขัดข้อง - ระบบเครือข่ายสื่อสารขัดข้อง เกิดภัยธรรมชาติ	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ

กิจกรรม	วัตถุประสงค์	ความเสี่ยง /ปัจจัยเสี่ยง	ผลกระทบ/ ผู้ได้รับผลกระทบ
การเข้าถึงข้อมูลของบุคคลอื่น	เพื่อให้ผู้ใช้งานเกิดความตระหนักและระมัดระวังการเข้าใช้ระบบสารสนเทศ	ผู้ใช้งานขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ
	เพื่อให้ระบบเครือข่ายสื่อสารของกรมฯ มีความปลอดภัยในการใช้งาน และสามารถตรวจสอบการใช้งานของผู้ใช้งาน	- มีการโจมตีจากภายในผ่านระบบเครือข่ายสื่อสาร - ผู้ใช้งานขาดความรู้เกี่ยวกับการใช้งานระบบเครือข่ายสื่อสาร - ผู้ดูแลระบบไม่มีความเชี่ยวชาญเฉพาะ	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ - ระบบฐานข้อมูล - ระบบสารสนเทศ
ระบบสารสนเทศมีความน่าเชื่อถือ	เพื่อให้ระบบงานกรมฯ ทำงานอย่างมีประสิทธิภาพ	หน้าจอการทำงานทำให้ผู้ใช้งานสับสน	- ผู้ใช้งาน - ผู้ดูแลระบบ - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ
ฐานข้อมูลมีความถูกต้อง	เพื่อให้ข้อมูลในฐานข้อมูลมีความถูกต้อง	ฐานข้อมูลหลักของกรมฯ ไม่ถูกต้อง	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ
	การนำเข้าข้อมูลไม่ถูกต้องตามรูปแบบที่กำหนด	ผู้ใช้งานขาดความรู้เกี่ยวกับการใช้งานที่ถูกต้อง	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ

การประเมินค่าความเสี่ยง

เป็นการประเมินค่าความเสี่ยงของกิจกรรมที่เกี่ยวข้อง โดยพิจารณาจากโอกาสและผลกระทบที่อาจจะเกิดขึ้นกับระบบสารสนเทศของกรมการขนส่งทางบก โดยอ้างอิงจาก**หลักเกณฑ์การประเมินระดับความเสี่ยง** โดยสามารถวิเคราะห์และจัดทำดับความเสี่ยงได้ดังนี้

กิจกรรม	วัตถุประสงค์	ความเสี่ยง /ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	ระดับความเสี่ยง
ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	เพื่อรองรับการเปลี่ยนแปลงนโยบายของผู้บริหารได้อย่างทันต่อสถานการณ์	การเปลี่ยนแปลงผู้บริหารอาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	๓	๔	๑๒
ความเสี่ยงจากภัยธรรมชาติ	เพื่อรับมือกับเหตุการณ์ภัยธรรมชาติที่อาจเกิดขึ้นกับระบบสารสนเทศ	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	๑	๓	๓
ความเสี่ยงจากเหตุการณ์บ้านเมือง	เพื่อมีแผนรองรับหากเหตุการณ์ความไม่สงบบ้านเมือง	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๒	๒	๔
ความเสี่ยงด้านบุคลากร	เพื่อให้มีบุคลากรด้านเทคโนโลยีสารสสนเทศและการสื่อสารที่มีความเชี่ยวชาญ	จำนวนบุคลากรที่มีไม่เพียงพอต่อระบบสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๓	๓	๙
ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	เพื่อให้มีงบประมาณในการบริหารจัดการระบบสารสนเทศ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๔	๓	๑๒
การป้องกันการถูกบุกรุก/โจมตีจากภายนอก	ป้องกัน/แก้ไขปัญหาที่เกิดจากการถูกผู้ไม่ประสงค์ดีบุกรุก/โจมตี	ไม่มีเครื่องมือในการตรวจจับการถูกบุกรุก/โจมตีจากผู้ไม่ประสงค์ดี	๔	๒	๘

กิจกรรม	วัตถุประสงค์	ความเสี่ยง /ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	ระดับความเสี่ยง
ระบบสารสนเทศไม่สามารถให้บริการได้ ตลอดเวลา	เพื่อให้กรมฯ สามารถให้บริการประชาชนได้ตลอดเวลา	กรมฯ ไม่สามารถให้บริการได้ เนื่องจาก - กระแสไฟฟ้าขัดข้อง - เครื่องแม่ข่ายขัดข้อง ระบบเครือข่ายสื่อสารขัดข้อง เกิดภัยธรรมชาติ	๓	๕	๑๕
การบริหารจัดการเครื่องคอมพิวเตอร์ลูกข่าย	เพื่อแก้ไขปัญหาทีเกิดขึ้นกับการใช้งานเครื่องคอมพิวเตอร์	เครื่องคอมพิวเตอร์ลูกข่ายมีปัญหาในการใช้งาน	๒	๒	๔
การเข้าถึงข้อมูลของบุคคลอื่น	เพื่อให้ผู้ใช้งานมีความระมัดระวังในการเข้าใช้ระบบสารสนเทศ	ผู้ใช้งานขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ	๒	๓	๖
	เพื่อให้ระบบเครือข่ายสื่อสารของกรมฯ มีความปลอดภัยในการใช้งาน และสามารถตรวจสอบการใช้งานของผู้ใช้งาน	มีการโจมตีจากภายในผ่านระบบเครือข่ายสื่อสาร	๒	๒	๔
		ผู้ใช้งานขาดความรู้เกี่ยวกับการใช้งานระบบเครือข่ายสื่อสาร	๒	๒	๔
		ผู้ดูแลระบบไม่มีความเชี่ยวชาญเฉพาะ	๒	๒	๔
ระบบสารสนเทศไม่รองรับการใช้งาน	เพื่อให้ระบบงานกรมฯ ทำงานอย่างมีประสิทธิภาพ	หน้าจอการทำงานไม่อำนวยความสะดวกให้ผู้ใช้งานเท่าที่ควร	๒	๓	๖
ฐานข้อมูลไม่ครบถ้วน ถูกต้อง	เพื่อให้ข้อมูลในฐานข้อมูลมีความถูกต้อง	ฐานข้อมูลหลักของกรมฯ ไม่ถูกต้อง	๓	๓	๙
	การนำเข้าข้อมูลไม่ถูกต้องตามรูปแบบที่กำหนด	ผู้ใช้งานขาดความรู้เกี่ยวกับการใช้งานที่ถูกต้อง	๓	๓	๙

การจัดการความเสี่ยง

จากการประเมินความเสี่ยง พบว่ามีความเสี่ยงทั้งหมด ๑๕ ความเสี่ยง โดยจำแนกได้ดังนี้

ระดับคะแนน	จำนวนความเสี่ยง	การดำเนินงาน
๑ – ๔	๒	เนื่องจากอยู่ระดับความเสี่ยงต่ำ สามารถยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง
๕ – ๙	๗	อยู่ในระดับความเสี่ยงปานกลาง พอที่จะยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับได้
๑๐ – ๑๖	๖	อยู่ในระดับความเสี่ยงสูง ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้

จากผลการประเมินความเสี่ยงข้างต้น ได้นำมากำหนดกิจกรรมในการควบคุมความเสี่ยง ดังนี้

กิจกรรมในการควบคุมความเสี่ยง

กิจกรรม	ความเสี่ยง / ปัจจัยเสี่ยง	ระดับความเสี่ยง	กิจกรรมที่ควบคุมอยู่	กิจกรรมที่ต้องปรับปรุง
ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	การเปลี่ยนแปลงผู้บริหารอาจทำให้นโยบายการบริหาร จัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	๑๒	นำเสนอและให้ข้อมูลที่อาจเป็นปัญหาหรือวิกฤตในการดำเนินหรือไม่ดำเนินนโยบายหรือโครงการของหน่วยงานในสังกัดกรมการขนส่งทางบก	จัดตารางให้มีการประชุมและติดตามข้อมูลงบประมาณ /โครงการทุกๆ ๒ เดือน
ความเสี่ยงจากภัยธรรมชาติ	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	๓	มีการจัดทำคู่มือเพื่อรองรับสถานการณ์ที่อาจเกิดขึ้นกับระบบสารสนเทศ	กำหนดเหตุการณ์ที่อาจเกิดขึ้นกับระบบสารสนเทศเพิ่มเติม เพื่อให้ครอบคลุม
ความเสี่ยงจากเหตุการณ์บ้านเมือง	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๔	จัดสรรและกำหนดให้มีผู้ดูแลระบบเพื่อควบคุมดูแลเครื่องแม่ข่ายและอุปกรณ์ประจำศูนย์คอมพิวเตอร์หลักและศูนย์สำรองข้อมูล	จัดทำแนวทางและการสื่อสารให้สามารถดำเนินงานและปฏิบัติงานทางไกลได้ (teleworking)

กิจกรรม	ความเสี่ยง / ปัจจัยเสี่ยง	ระดับความเสี่ยง	กิจกรรมที่ควบคุมอยู่	กิจกรรมที่ต้องปรับปรุง
ความเสี่ยงด้านบุคลากร	จำนวนบุคลากรที่มีไม่เพียงพอต่อระบบสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๙	จัดส่งเจ้าหน้าที่เข้ารับการอบรมในหลักสูตรที่เกี่ยวข้องกับการปฏิบัติงาน	จัดทำแผนพัฒนาบุคลากรด้านไอทีของกรมฯ ให้เป็นไปตามคุณสมบัติและสอดคล้องกับแผนพัฒนาบุคลากรด้านไอทีของกระทรวงไอซีที
ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	การขาดแคลนงบประมาณในการดำเนินการในระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๑๒	กำหนดและจัดลำดับความสำคัญของโครงการเพื่อให้สอดคล้องกับการดำเนินงานของกรมฯ และความจำเป็นเร่งด่วน	- ขอรับจัดสรรงบประมาณจากเงินนอกงบประมาณ - กำหนดโครงการที่สำคัญและจัดลำดับความสำคัญ
การป้องกันการถูกบุกรุก/โจมตีจากภายนอก	ไม่มีเครื่องมือในการตรวจจับการถูกบุกรุก/โจมตีจากผู้ไม่ประสงค์ดี	๘	- มีควบคุมการเข้า-ออก - จัดหาอุปกรณ์ IPS/IDP - จัดหา Firewall - จัดหา Web Antivirus Appliance - จัดหาอุปกรณ์ Log Management - จัดหาแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	ให้ความรู้กับเจ้าหน้าที่ผู้ใช้งานระบบสารสนเทศให้เกิดความเข้าใจเกี่ยวกับการใช้งาน และภัยที่อาจเกิดจากการงานที่ไม่ถูกต้อง
ระบบสารสนเทศไม่สามารถให้บริการได้ตลอดเวลา	กรมฯ ไม่สามารถให้บริการได้เนื่องจาก - กระแสไฟฟ้าขัดข้อง - เครื่องแม่ข่ายขัดข้อง - ระบบเครือข่ายสื่อสารขัดข้อง - เกิดภัยธรรมชาติ	๑๕	- จัดหาระบบไฟฟ้าสำรอง - บำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายเป็นประจำทุกเดือน - บำรุงรักษาระบบเครือข่ายสื่อสาร - จัดหาเครือข่ายสื่อสารสำรอง - จัดทำแผนรองรับสถานการณ์ฉุกเฉิน	-มีการกำหนดขั้นตอนวิธีเพื่อรองรับปัญหาที่อาจเกิดขึ้น - ตรวจสอบปัญหาที่เกิดขึ้นพร้อมหาแนวทางป้องกันเพื่อมิให้เกิดปัญหาซ้ำในแบบเดิม
การบริหารจัดการเครื่องคอมพิวเตอร์ลูกข่าย	เครื่องคอมพิวเตอร์ลูกข่ายมีปัญหาในการใช้งาน	๔	จัดการโปรแกรมสำหรับบริหารจัดการเครื่องคอมพิวเตอร์	จัดการโปรแกรมสำหรับบริหารจัดการเครื่องคอมพิวเตอร์ให้เพียงพอต่อเครื่องคอมพิวเตอร์ของกรมการขนส่งทางบก

กิจกรรม	ความเสี่ยง / ปัจจัยเสี่ยง	ระดับความเสี่ยง	กิจกรรมที่ควบคุมอยู่	กิจกรรมที่ต้องปรับปรุง
การเข้าถึงข้อมูลของบุคคลอื่น	ผู้ใช้งานขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ	๖	กำหนดวิธีการเข้าใช้ระบบสารสนเทศ	- ปรับปรุงโปรแกรมเพื่อป้องกันการใช้งานที่ไม่ถูกต้อง - สร้างความตระหนักในการใช้ Username และ Password ในการเข้าใช้ระบบสารสนเทศ - จัดทำแนวทางในการอนุญาตให้ใช้ Username และ Password ให้กับเจ้าหน้าที่
	มีการโจมตีจากภายในผ่านระบบเครือข่ายสื่อสาร	๔	จัดหาอุปกรณ์ในการป้องกันการบุกรุกผ่านระบบเครือข่ายสื่อสารข้อมูล (ตามโครงการ MDM)	ประชาสัมพันธ์ให้หน่วยงานในกรมฯ รับทราบ
	ผู้ใช้งานขาดความรู้เกี่ยวกับการใช้งานระบบเครือข่ายสื่อสาร	๔	- กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ - กำหนดวิธีการเข้าถึงระบบสารสนเทศในส่วนที่เกี่ยวข้องกับระบบเครือข่ายสื่อสารของกรมฯ	จัดสัมมนาให้ความรู้กับผู้ใช้งาน
	ผู้ดูแลระบบไม่มีความเชี่ยวชาญเฉพาะ	๔	กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ	จัดสัมมนาให้ความรู้กับผู้ใช้งาน
ระบบสารสนเทศไม่รองรับการใช้งาน	หน้าจอการทำงานไม่อำนวยความสะดวกให้ผู้ใช้งานเท่าที่ควร	๖	ปรับปรุงระบบสารสนเทศหลักให้สอดคล้องกับการใช้งานและรูปแบบของผลลัพธ์ที่ต้องการ	จัดให้มีทำคู่มือการปฏิบัติงานที่แสดงถึงวิธีการใช้งานโดยละเอียด
ฐานข้อมูลไม่ครบถ้วน ถูกต้อง	ฐานข้อมูลหลักของกรมฯ ไม่ถูกต้อง	๙	- ปรับปรุงฐานข้อมูลให้มีความถูกต้อง - ตรวจสอบข้อมูลและแจ้งหน่วยที่รับผิดชอบดำเนินการแก้ไขข้อมูลให้ถูกต้องครบถ้วน	ออกแบบหน้าจอและการนำเข้าข้อมูลตามขั้นตอนวิธีที่ถูกต้อง
	การนำเข้าข้อมูลไม่ถูกต้องตามรูปแบบที่กำหนด	๙	จัดทำคู่มือการใช้งานในแต่ละหน้าจอการทำงาน	ปรับปรุงคู่มือการใช้งานให้เป็นปัจจุบัน

กิจกรรมควบคุมที่ดำเนินการเพื่อจัดการความเสี่ยง

จากผลการประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศของกรมการขนส่งทางบก ศูนย์เทคโนโลยีสารสนเทศ จึงได้จัดทำคู่มือต่าง ๆ สำหรับเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อดำเนินแนวทางการปฏิบัติ ประกอบด้วย

๑. จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์เพื่อ

(๑) การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของกรม ๆ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

(๒) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ อ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

(๓) นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

(๔) เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ (System Administrators) และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการ รักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่าง เคร่งครัด

(๕) นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

สำหรับรายละเอียดของนโยบายฯ ที่จัดทำขึ้น ได้กำหนดให้สอดคล้องกับข้อกำหนดตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และประกาศหรือกฎหมายที่เกี่ยวข้อง โดยมีรายละเอียด ดังนี้

๑.๑ นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy) เพื่อการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมการขนส่งทางบก เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้าน เทคโนโลยีสารสนเทศของกรมการขนส่งทางบกให้อยู่ระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC ๒๗๐๐๑ อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศขององค์กร

๑.๒ นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy) เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานต้องผ่านการพิสูจน์ตัวตนจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย (Wireless LAN)

๑.๓ นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy) เพื่อควบคุมการสื่อสารระหว่างเครือข่ายภายในองค์กรกับเครือข่ายภายนอกองค์กร โดยการกำหนด ตั้งค่าของไฟรวอลล์ (Firewall) ขององค์กร ให้มีประสิทธิภาพในการทำงาน และกำหนดให้กับอุปกรณ์ที่ต้องการเชื่อมโยงสื่อสารภายในองค์กร รวมทั้งมีการทบทวนสิทธิ์ของผู้ใช้งานอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ (System Administrators) เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบไฟร์วอลล์ (Firewall)

๑.๔ นโยบายความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy) เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้งานจะต้องให้

ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบ (System Administrators) เครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบ (System Administrators) เครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๑.๕ นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy) เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต (Internet) อย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๑.๖ นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access control Policy) เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศและการสื่อสารขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศขององค์กรได้อย่างถูกต้อง

๑.๗ นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System/Intrusion Prevention System Policy : IDS/IPS Policy) เพื่อฟ้องกันการบุกรุกโจมตีจากภายนอกองค์กร โดยมีการตรวจสอบการใช้งานบนระบบเครือข่ายภายในองค์กร รวมไปถึงพฤติกรรมต่าง ๆ ที่เกิดขึ้นบนเครือข่ายสื่อสารขององค์กร และจะต้องมีการบันทึกเป็นลายลักษณ์อักษร สามารถตรวจสอบย้อนหลังได้

๑.๘ นโยบายการสำรองและกู้คืนข้อมูล เพื่อฟ้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลและระบบสารสนเทศของกรมการขนส่งทางบก หากระบบสารสนเทศไม่สามารถใช้งานได้ หรือข้อมูลที่อยู่ในฐานข้อมูลหลักเกิดความเสียหาย

๑.๙ นโยบายการใช้เครื่องคอมพิวเตอร์และอุปกรณ์พกพา เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกองค์กร เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์กรให้เกิดความปลอดภัย ผู้ใช้งานจึงต้องรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ต้องหลีกเลี่ยง ในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

๑.๑๐ การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศและการสื่อสาร เพื่อควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบสารสนเทศและการสื่อสารของกรมการขนส่งทางบก ให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการคัดเลือกควบคุมการปฏิบัติงานของหน่วยงานภายนอกหรือบริษัทผู้รับจ้างที่เป็นคู่สัญญากับกรมฯ

๑.๑๑ การควบคุมการเข้าถึงห้องเครื่องคอมพิวเตอร์และห้องเครือข่ายสื่อสารข้อมูล เพื่อกำหนดมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องเครื่องคอมพิวเตอร์และห้องเครือข่ายสื่อสารข้อมูล และระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบสารสนเทศ

๑.๑๒ แนวปฏิบัติการประเมินความเสี่ยงด้านสารสนเทศ เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและฟ้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๑.๑๓ การกำหนดหน้าที่ความรับผิดชอบ เพื่อกำหนดหน้าที่ให้ผู้เกี่ยวข้องสามารถติดตามและสั่งการได้ตามลำดับขั้นตอน และลดความเสี่ยงที่อาจจะเกิดขึ้น

๒. จัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) โดยวัตถุประสงค์เพื่อ

- เพื่อให้สามารถรับมือกับเหตุการณ์ที่ทำให้ระบบงานสำคัญหยุดชะงักได้อย่างมีประสิทธิภาพและประสิทธิผล รวมทั้งสามารถกู้คืนระบบงานเพื่อให้กลับคืนมาภายใน ระยะเวลาที่กำหนดไว้
- เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบสารสนเทศให้มีเสถียรภาพและ มีความพร้อมสำหรับใช้งาน
- เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบสารสนเทศ
- เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบสารสนเทศ
- เพื่อจัดให้มีการบริหารและจัดการความเสี่ยงที่มีต่อระบบงานสำคัญ อันจะก่อให้เกิดการหยุดชะงักของระบบได้

ซึ่งในแผนดังกล่าว ได้จำแนกความเสี่ยงที่อาจเกิดขึ้นเป็น ๒ ด้าน คือความเสี่ยงทางด้านเทคนิค และความเสี่ยงทางด้านภัยหรือสถานการณ์ฉุกเฉิน โดยแต่ละด้านประกอบด้วย

๒.๑ ความเสี่ยงทางด้านเทคนิค
- กรณีโดนเจาะระบบ
- กรณีเครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายสื่อสารขัดข้อง
- กรณีไวรัสคอมพิวเตอร์

๒.๒ ความเสี่ยงทางด้านภัยหรือสถานการณ์ฉุกเฉิน
- กรณีไฟดับ
- กรณีไฟไหม้
- กรณีน้ำท่วม
- กรณีลิฟต์โดยสารขัดข้อง

๓. จัดทำประกาศข้อกำหนดการเข้าปฏิบัติงานในห้อง Server และห้อง Network เพื่อควบคุมการเข้าออกศูนย์คอมพิวเตอร์หลักและการป้องกันความเสียหาย

๔. จัดทำประกาศเกี่ยวกับการกำหนดให้ศูนย์เทคโนโลยีสารสนเทศเป็นเขตหวงห้ามเฉพาะเพื่อควบคุมการเข้าออกศูนย์เทคโนโลยีสารสนเทศ อาคาร ๙

๕. จัดทำแนวปฏิบัติการเข้าถึงระบบสารสนเทศของกรมการขนส่งทางบก เพื่อเป็นแนวทางในการควบคุมการเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินทราเน็ต ระบบเครือข่ายคอมพิวเตอร์ (เฉพาะเครื่องคอมพิวเตอร์ที่ต้องการใช้งานเครือข่ายคอมพิวเตอร์ส่วนกลาง) ระบบงานสารสนเทศกรมการขนส่งทางบก และระบบฐานข้อมูลหลักของกรมการขนส่งทางบก

๖. มีระบบการรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูลและสารสนเทศ ระบบ Antivirus, ระบบไฟฟ้าสำรอง, ระบบ Firewall, ระบบสำรองข้อมูล (Backup Data)

๗. มีการจัดทำคู่มือการปฏิบัติงานของศูนย์เทคโนโลยีสารสนเทศ เพื่อสร้างมาตรฐานการปฏิบัติงานของศูนย์เทคโนโลยีสารสนเทศ และใช้คู่มืออ้างอิงในการปฏิบัติงานของเจ้าหน้าที่ในส่วนที่เกี่ยวข้อง

โดยทุกกิจกรรมที่ดำเนินการ ศูนย์เทคโนโลยีสารสนเทศได้มีการจัดทำและทบทวนรายละเอียดเป็นประจำ อย่างต่อเนื่องทุกปี เพื่อให้เหมาะสมสอดคล้องกับสถานการณ์ปัจจุบัน

ภาคผนวก ก
คำสั่งแต่งตั้งคณะทำงานบริหารความเสี่ยงระบบเทคโนโลยีสารสนเทศ

คำสั่งศูนย์เทคโนโลยีสารสนเทศ
ที่ ๕ /๒๕๖๔

เรื่อง แต่งตั้งคณะทำงานทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ของกรมการขนส่งทางบก

ตามหนังสือที่ ทก ๐๒๐๙.๔/๖๕๗๔ ลงวันที่ ๒๓ มิถุนายน ๒๕๕๘ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ขอความร่วมมือให้ส่วนราชการและหน่วยงานของรัฐดำเนินการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกรมการขนส่งทางบกได้ดำเนินการไปเรียบร้อยแล้วนั้น

ดังนั้น เพื่อให้แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมการขนส่งทางบก เกิดความถูกต้อง เหมาะสม เป็นประโยชน์แก่การปฏิบัติราชการ มีความสอดคล้องกับการดำเนินงานในสถานการณ์ปัจจุบัน และเพื่อให้สามารถดำเนินการเป็นไปด้วยความเรียบร้อย จึงขอยกเลิกคำสั่งศูนย์เทคโนโลยีสารสนเทศ ที่ ๑/๒๕๖๔ ลงวันที่ ๒๕ กุมภาพันธ์ ๒๕๖๔ และคำสั่งศูนย์เทคโนโลยีสารสนเทศ ที่ ๔/๒๕๖๔ ลงวันที่ ๒๙ เมษายน ๒๕๖๔ พร้อมแต่งตั้งคณะทำงานทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ของกรมการขนส่งทางบก โดยมีองค์ประกอบคณะทำงานและอำนาจหน้าที่ดังต่อไปนี้

๑. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ	ประธานคณะทำงาน
๒. หัวหน้ากลุ่มบริหารข้อมูลและระบบสารสนเทศ	คณะทำงาน
๓. หัวหน้ากลุ่มเทคโนโลยีการขนส่งทางถนน	คณะทำงาน
๔. หัวหน้ากลุ่มระบบคอมพิวเตอร์และเครือข่าย	คณะทำงาน
๕. หัวหน้างานบริหารงานทั่วไป	คณะทำงาน
๖. หัวหน้างานนโยบายและแผนงานเทคโนโลยีสารสนเทศ	คณะทำงาน
๗. หัวหน้างานบริหารฐานข้อมูล	คณะทำงาน
๘. หัวหน้างานพัฒนาระบบสารสนเทศบริการ	คณะทำงาน
๙. หัวหน้างานพัฒนาระบบสารสนเทศบริหาร	คณะทำงาน
๑๐. หัวหน้างานระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย	คณะทำงาน
๑๑. หัวหน้างานสนับสนุนระบบสารสนเทศ	คณะทำงาน
๑๒. หัวหน้างานพัฒนาระบบภูมิสารสนเทศ	คณะทำงาน
๑๓. หัวหน้างานเทคโนโลยีระบบความปลอดภัยการขนส่งทางถนน	คณะทำงาน
๑๔. นายศุภชัย พลโก นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน

/๑๕. นางสุรัสวดี...

๑๕. นางสุรัสวดี รัศมีรณชัย นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๑๖. นายวลัญชน์ บุญแก้วขวัญ นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๑๗. นางสาวศุภวรรณ เรืองวิลัย นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๑๘. นายพฤฒิ บุญชูวงศ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๑๙. นายจิรัถ บุรพรัตน์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๒๐. นายเอกพันธุ์ ศรีวงษ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๒๑. นางสาวรัชชาภรณ์ สุกลพราหมณ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๒๒. นายพงศ์พิสุทธิ์ ธีระชัย นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๒๓. นายโชคอำนวย เถื่อนสันเทียะ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๒๔. ว่าที่ร้อยตรีเพชระ อินทานนท์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๒๕. นายอดิพล ลิ้มสุวรรณ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๒๖. หัวหน้ากลุ่มนโยบายและมาตรฐานเทคโนโลยีสารสนเทศ	คณะทำงานและเลขานุการ
๒๗. หัวหน้างานมาตรฐานและความปลอดภัยเทคโนโลยีสารสนเทศ	คณะทำงานและผู้ช่วยเลขานุการ
๒๘. นางสาวศิญาภัสร์ มั่นคงธิติวัฒน์ นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงานและผู้ช่วยเลขานุการ
๒๙. นางสาวกนกวรรณ ชำนาญจุ้ย นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงานและผู้ช่วยเลขานุการ

โดยมอบหมายให้คณะทำงานฯ มีหน้าที่ความรับผิดชอบ ดังนี้

๑. ศึกษาแบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ตามมาตรา ๗ ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๒. ศึกษา วิเคราะห์ความเสี่ยงของระบบเทคโนโลยีสารสนเทศ และสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านสารสนเทศ (IT Contingency Plan) ของกรมการขนส่งทางบกที่อาจก่อให้เกิดความเสียหายในรูปแบบต่างๆ รวมทั้งแนวทางการฟื้นฟูระบบ/ข้อมูลจากความเสียหาย (Recovery)

/๓. พิจารณา...

๓. พิจารณาทำแบบประเมินตนเอง พร้อมแนบเอกสารอ้างอิง/ระบุเหตุผล(ถ้ามี) ตามแบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ตามมาตรา ๗ ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๔. พิจารณาทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางบก ให้มีความสอดคล้องกับแบบแสดงรายการทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ให้มีรายละเอียดครบถ้วน สมบูรณ์

๕. กำหนดนโยบาย จัดทำแผนบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศและแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านสารสนเทศ (IT Contingency Plan) ของกรมการขนส่งทางบก รวมทั้งการให้ความรู้กับผู้ที่เกี่ยวข้องในการปฏิบัติงานตามแผนฯ ที่ได้กำหนดไว้ เพื่อแก้ไข ลด และป้องกันความเสี่ยงที่อาจเกิดขึ้น

๖. กำหนดรูปแบบ วิธีการบริหารจัดการ กำกับดูแล ตรวจสอบ ติดตาม และประเมินผลการดำเนินการตามแผนบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ และแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านสารสนเทศ (IT Contingency Plan) ของกรมการขนส่งทางบก

๗. จัดทำแผนสำรอง หรือเตรียมความพร้อมฉุกเฉิน พร้อมกำหนดผู้รับผิดชอบดูแลเป็นลายลักษณ์อักษร

๘. นำเสนอแบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงานรัฐ ตามมาตรา ๗ ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ พร้อมเอกสารอ้างอิงที่เกี่ยวข้องทั้งหมด และเอกสารแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางบก นำเสนอผู้บริหารสูงสุด หรือผู้ที่ได้รับมอบอำนาจลงนามท้ายแบบฟอร์ม

๙. พิจารณาทบทวนแผนบริหารความเสี่ยงระบบเทคโนโลยีสารสนเทศ แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านสารสนเทศ (IT Contingency Plan) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แผนฯ ที่กำหนดมีความสอดคล้องกับการดำเนินงานในสถานการณ์ปัจจุบัน และสามารถแก้ไขปัญหาและผลกระทบได้ทันท่วงที

๑๐. รายงานผลการดำเนินงานตามอำนาจหน้าที่ ตลอดจนปัญหา อุปสรรค ให้ผู้บังคับบัญชาทราบตามลำดับขั้น

๑๑. ปฏิบัติงานอื่นๆ ที่เกี่ยวข้อง ตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๙ พฤษภาคม พ.ศ. ๒๕๖๔

(นายนุตนันทน์ นุตาลัย)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

ภาคผนวก ข
ข้อกำหนดการเข้าปฏิบัติงาน ณ ศูนย์เทคโนโลยีสารสนเทศ

คำสั่งศูนย์เทคโนโลยีสารสนเทศ
ที่ ๒๔ /๒๕๖๔
เรื่อง ข้อกำหนดการเข้าปฏิบัติงานภายในห้อง Server และห้อง Network

ด้วยศูนย์เทคโนโลยีสารสนเทศ เป็นสถานที่ตั้งของศูนย์ข้อมูลกลางของกรมการขนส่งทางบก ซึ่งประกอบด้วยเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่มูลค่าสูงจำนวนมาก และเป็นฐานข้อมูลกลางสำหรับรวบรวมข้อมูลเกี่ยวกับการดำเนินการ ตามกฎหมายว่าด้วยการขนส่งทางบก และกฎหมายว่าด้วยรถยนต์ ของสำนักงานขนส่งต่าง ๆ ทั่วประเทศ ซึ่งเป็นข้อมูลสำคัญทางราชการ จึงมีความจำเป็นต้องมีการรักษาความปลอดภัยอย่างเข้มงวด เพื่อป้องกันมิให้เกิดการสูญเสีย และความเสียหายต่ออุปกรณ์คอมพิวเตอร์และฐานข้อมูลกลางดังกล่าว รวมทั้งทรัพย์สินอื่น ๆ ของทางราชการ ศูนย์เทคโนโลยีสารสนเทศ จึงกำหนดให้การเข้าปฏิบัติงานภายในห้อง Server และห้อง Network ของบุคคลภายนอก ดังต่อไปนี้

๑. เจ้าหน้าที่บริษัทที่เข้ามาปฏิบัติหน้าที่อยู่ประจำ จะต้องมีหนังสือแจ้ง ชื่อ-นามสกุล ตำแหน่ง และเบอร์โทรศัพท์ที่สามารถติดต่อได้ จากบริษัทต้นสังกัดมายังศูนย์เทคโนโลยีสารสเทศ และในกรณีที่มีการเปลี่ยนตัวเจ้าหน้าที่ ที่จะมาปฏิบัติงานจะต้องทำหนังสือแจ้งมายังศูนย์เทคโนโลยีสารสนเทศทุกครั้ง และในการมาปฏิบัติงานจะต้องติดบัตรพนักงานมาด้วยทุกครั้ง

๒. กรณีบริษัทที่ทำการดูแลระบบ ที่ไม่ได้มีเจ้าหน้าที่อยู่ประจำ จะเข้ามาทำการใด ๆ กับเครื่อง Sever หรืออุปกรณ์ Network ทั้งในเวลาหรือนอกเวลาราชการ จะต้องมีหนังสือแจ้ง ชื่อ-นามสกุล ตำแหน่ง เบอร์โทรศัพท์ที่สามารถติดต่อได้ และวันเวลาที่จะเข้าปฏิบัติงาน จากบริษัทต้นสังกัดมายังศูนย์เทคโนโลยีสารสนเทศทุกครั้ง โดยให้แจ้งล่วงหน้าอย่างน้อย ๓ วัน (หากเป็นกรณีฉุกเฉินเร่งด่วนให้ทำการประสานกับเจ้าหน้าที่งานระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย เพื่อพิจารณาความเหมาะสมในการเข้าปฏิบัติงานต่อไป)

๓. กรณีที่เป็นการติดตั้งระบบใหม่ จะต้องมีหนังสือแจ้ง รายละเอียดของอุปกรณ์ที่จะทำการติดตั้ง , Network diagram พร้อมทั้ง ชื่อ-นามสกุล ตำแหน่ง เบอร์โทรศัพท์ที่สามารถติดต่อได้ และวันเวลาที่จะเข้าปฏิบัติงาน ของเจ้าหน้าที่ที่จะเข้ามาทำการติดตั้งจากบริษัทต้นสังกัดมายังศูนย์เทคโนโลยีสารสนเทศ ทุกครั้ง โดยให้แจ้งล่วงหน้าอย่างน้อย ๕ วัน

๔. ห้ามมิให้บุคคลใด ที่มิได้มีการแจ้งขอเข้าปฏิบัติงานภายในห้อง Server และห้อง Network เข้ามาปฏิบัติงานภายในห้อง Server และห้อง Network หากมิได้รับอนุญาตจากงานระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย (หากฝ่าฝืนขอสงวนสิทธิ์ ในการเชิญออกจากห้อง)

๕. เจ้าหน้าที่ผู้ที่จะเข้ามาปฏิบัติงานภายในห้อง Server และห้อง Network ต้องปฏิบัติตามข้อ ๑ - ๕ อย่างเคร่งครัด ถ้าไม่ทราบหรือไม่เข้าใจให้ติดต่อสอบถามกับเจ้าหน้าที่งานระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย

๖. ห้ามมิให้นำอาหาร เครื่องดื่มเข้ามารับประทานภายในห้อง Server และห้อง Network

๗. ห้ามถ่ายภาพหรือบันทึกภาพเคลื่อนไหว หากมิได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(นายบุดนันทน์ นุตาลัย)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

คำสั่งศูนย์เทคโนโลยีสารสนเทศ
ที่ ๓ /๒๕๖๔
เรื่อง กำหนดให้ศูนย์เทคโนโลยีสารสนเทศเป็นเขตหวงห้ามเฉพาะ

ด้วยศูนย์เทคโนโลยีสารสนเทศ เป็นสถานที่ตั้งของศูนย์ข้อมูลกลางของกรมการขนส่งทางบก ซึ่งประกอบด้วยเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่มูลค่าสูงจำนวนมาก และเป็นฐานข้อมูลกลาง สำหรับรวบรวมข้อมูลเกี่ยวกับการดำเนินการตามกฎหมายว่าด้วยการขนส่งทางบก และกฎหมายว่าด้วยรถยนต์ ของสำนักงานขนส่งต่าง ๆ ทั่วประเทศ จึงมีความจำเป็นต้องมีการรักษาความปลอดภัยอย่างเข้มงวด เพื่อป้องกันมิให้เกิดการสูญเสีย และความเสียหายต่ออุปกรณ์คอมพิวเตอร์และฐานข้อมูลกลางดังกล่าว รวมทั้งทรัพย์สินอื่น ๆ ของทางราชการ จึงกำหนดให้ศูนย์เทคโนโลยีสารสนเทศเป็นเขตหวงห้ามเฉพาะ และให้เข้มงวดกวดขันการเข้า - ออกของบุคคลภายนอก พร้อมนี้ได้กำหนดหลักเกณฑ์การปฏิบัติของเจ้าหน้าที่ขณะปฏิบัติหน้าที่ในศูนย์เทคโนโลยีสารสนเทศ และการเข้า - ออกของบุคคลภายนอกดังต่อไปนี้

๑. บุคคลภายนอก หรือ กรณีญาติหรือคนรู้จักมาขอพบ จะต้องขอรับบัตรผู้มาติดต่อที่เคาน์เตอร์ชั้น ๑ ของศูนย์เทคโนโลยีสารสนเทศ เพื่อติดแสดงให้ทราบด้วย

๒. เจ้าหน้าที่บริษัทที่มาปฏิบัติหน้าที่ (Outsource) ที่ศูนย์เทคโนโลยีสารสนเทศ จะต้องติดบัตรพนักงาน เพื่อแสดงให้ทราบด้วยทุกครั้งที่เข้ามาปฏิบัติงาน

๓. ห้ามบุคคลภายนอกเข้ามาเรี่ยไร และขายของ

๔. ห้ามสูบบุหรี่และห้ามเล่นการพนันทุกชนิดภายในบริเวณศูนย์เทคโนโลยีสารสนเทศ (ชั้น ๑ ถึงชั้น ๔) โดยเด็ดขาด

๕. ห้ามเข้าหากแต่งกายไม่สุภาพ

๖. ห้ามพกพาอาวุธ วัตถุระเบิด หรือวัตถุไวไฟทุกชนิด

(นายบุหนันทน์ บุตาลัย)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ