นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์การขนส่งมวลชนกรุงเทพ

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นในการให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชนรวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบายและการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วยหลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้อง ความสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมั่นคงปลอดภัยในระบบสารสนเทศ ที่มีรูปแบบหลากหลาย ส่งผลทวีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องมาจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศ การขาดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

โดยคณะอนุกรรมการความมั่นคงปลอดภัยภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ ของหน่วยงานภาครัฐ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

องค์การขนส่งมวลชนกรุงเทพ จึงได้จัดทำนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ ประจำปีงบประมาณ พ.ศ.๒๕๖๖ ขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงานในองค์การขนส่งมวลชนกรุงเทพ เพื่อให้บุคลากรทุกคนในองค์การขนส่งมวลชนกรุงเทพ มีความรู้ เข้าใจในนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

องค์การขนส่งมวลชนกรุงเทพ

สารบัญ

๑. บทนำ

๑.๑ หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ *"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"* และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กรซึ่งจะได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัยเช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีสำคัญอย่างยิ่งต่อองค์กร ที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมายและมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้อนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

๑.๒ วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การขนส่งมวลชนกรุงเทพ ฉบับนี้มีวัตถุประสงค์เพื่อ

๑) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ ที่สอดคล้องกับบริบทองค์กร และกฎหมายที่เกี่ยวข้อง

๒) จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศเทคโนโลยีและการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

๓) เพื่อให้มั่นใจได้ว่าข้อมูลและระบบสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ มีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจจะเกิดขึ้นในระบบสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ และใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ องค์การขนส่งมวลชนกรุงเทพ

๑.๓ องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การขนส่งมวลชนกรุงเทพ โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ อ้างอิงตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ และมาตรา ๗ ซึ่งกำหนดให้หน่วยงานภาครัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยแนวทางปฏิบัตินี้ประกอบด้วย วัตถุประสงค์ ผู้เกี่ยวข้อง และรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ

๑.๔ บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุนและติดตามการประยุกต์ใช้ โดยผู้อำนวยการองค์การขนส่งมวลชนกรุงเทพ

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้อำนวยการองค์การขนส่งมวลชนกรุงเทพเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๑.๕ การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ ฉบับนี้ จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) องค์การขนส่งมวลชนกรุงเทพ จัดพิมพ์เผยแพร่เพื่อให้บุคลากรขององค์การขนส่งมวลชนกรุงเทพ และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒. คำนิยาม

๑. **คำเรียกแทนหน่วยงานในเอกสารฉบับนี้ เช่น กรม, สำนักงาน, ฝ่าย** หมายถึง องค์การขนส่งมวลชนกรุงเทพ

๒. **ผู้บริหารระดับสูง** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารราชการขององค์การขนส่งมวลชนกรุงเทพ

๓. **การรักษาความมั่นคงปลอดภัย** หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับด้านสารสนเทศ ขององค์การขนส่งมวลชนกรุงเทพ

๔. **ผู้ใช้งาน** หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับผิดชอบ ผู้ใช้งานทั่วไป อันได้แก่

๔.๑ ผู้บริหารสูงสุด หมายความว่า ผู้อำนวยการองค์การขนส่งมวลชนกรุงเทพ

๔.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Office : CIO) หมายความว่า รองผู้อำนวยการฝ่ายบริหาร ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔.๓ ผู้ดูแลระบบ/ผู้ดูแลห้องเครื่อง หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์

๔.๔ ผู้พัฒนาระบบ หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนาระบบแอพพลิเคชั่น

๔.๕ เจ้าหน้าที่ หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการขององค์กร

๔.๖ บุคคลภายนอก หมายความว่า บุคคลที่องค์การขนส่งมวลชนกรุงเทพอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของกรมทางหลวงชนบทได้ชั่วคราว เพื่อประโยชน์ในการดำเนินงานขององค์การขนส่งมวลชนกรุงเทพ เช่น พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับองค์การขนส่งมวลชนกรุงเทพ หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง หรือนิสิตนักศึกษาฝึกงาน

๕. **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๖. **สินทรัพย์** (Asset) หรือ ทรัพย์สินสารสนเทศ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่

๖.๑ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๒ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

๖.๓ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๗. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจะอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๘. **ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ (Information Security)** หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) ห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

๙. **เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันนำไปสู่ปัญหาด้านความมั่นคงปลอดภัย

๑๐. **สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๓. นโยบายการรักษาความมั่นคงปลอดภัย

หมวดที่ ๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

ส่วนที่ ๑
การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานที่เป็นบุคลากรขององค์การ และบุคคลภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ

๒. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

หมวดหมู่สินทรัพย์ตามระดับความสำคัญ ความลับ คุณค่า เพื่อหาวิธีการบริหารจัดการที่เหมาะสม เพื่อนำข้อมูลของสินทรัพย์ไปใช้เพื่อประเมินความเสี่ยงต่างๆ

๒.๑ กำหนดให้ห้องควบคุมระบบ (System Control Room) เป็นบริเวณที่ต้องรักษาความปลอดภัย และจัดให้มีการควบคุมการเข้า-ออก เฉพาะผู้ได้รับอนุญาตเท่านั้น

๒.๒ จัดทำแผนป้องกันอุบัติภัย เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ เพื่อสามารถรับมือกับอุบัติภัยที่เกิดขึ้นและกู้คืนระบบให้สามารถกลับมาใช้งานได้ตามเป้าหมายที่กำหนด

๒.๓ ดูแลอุปกรณ์ระบบเครือข่ายไร้สายที่ใช้งานภายในสำนักเทคโนโลยีสารสนเทศโดยควบคุมการใช้งานจากส่วนกลาง ซึ่งได้รับการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อลดความเสี่ยงในการเข้าใช้งานระบบเครือข่าย

๒.๔ มีระบบการดูแลสภาพแวดล้อมที่ดี ตามมาตรฐานการควบคุมด้านระบบไฟฟ้า เขม่าควัน และฝุ่นละออง

๒.๕ ตรวจสอบความเหมาะสมของข้อมูลที่เผยแพร่ออกสู่สาธารณะ ต้องไม่ขัดต่อกฎหมายที่เกี่ยวข้องและ กลไกป้องกันการเข้าไปแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

๒.๖ แบ่งแยกเครือข่ายโดยแยกตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศด้วย LAN

๒.๗ การควบคุมการนำเข้าและการส่งออก เครื่องคอมพิวเตอร์ และอุปกรณ์สารสนเทศ ของสำนักเทคโนโลยีสารสนเทศ

๒.๘ การนำฮาร์ดแวร์และซอฟต์แวร์ใหม่มาติดตั้งใช้งาน จะต้องผ่านตรวจสอบ และหากต้องมีการทดสอบก่อนเชื่อมต่อกับระบบเดิม ห้ามมิให้ใช้ฐานข้อมูลจริงในการทดสอบ

๒.๙ ผู้ครอบครองสื่อบันทึกข้อมูล ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อตรวจสอบข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้งหรือเขียนทับ ก่อนจำหน่ายอุปกรณ์ดังกล่าว

๒.๑๐ ผู้ดูแลระบบ ต้องควบคุมการให้บริการของหน่วยงานภายนอก (Outsource) ที่เกี่ยวข้องกับระบบสารสนเทศ และให้ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์การ

(๑) ผู้รับจ้าง หรือ Outsource ต้องลงนามบันทึกข้อกำหนดเงื่อนไขการทำงานร่วมกับองค์การท้ายสัญญา ห้ามเผยแพร่หรือทำซ้ำ ส่วนหนึ่งส่วนใดของ Software ที่พัฒนาขึ้น หรือการบำรุงรักษา Software ต่างๆ ให้บุคคลภายนอกรับรู้ หรือนำไปใช้งาน โดยเด็ดขาด

(๒) ผู้รับจ้างที่เป็นนิติบุคคลจะต้องกำชับพนักงาน ให้ปฏิบัติตามเงื่อนไขท้ายสัญญาโดยเคร่งครัดและมิให้ปฏิเสธความผิดชอบ หากความเสียเกิดจากพนักงานของผู้รับจ้างเอง

๒.๑๑ กำหนดพื้นที่ใช้งาน และพื้นที่ติดตั้ง รวมทั้งพื้นที่จัดเก็บอุปกรณ์ระบบสารสนเทศรวมทั้งระบบคอมพิวเตอร์และเครือข่าย

๒.๑๒ กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ และระบบเครือข่าย

๒.๑๓ กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและระบบเครือข่าย

๒.๑๔ กำหนดให้หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์มาเพื่อใช้ในการปฏิบัติงานบนระบบเครือข่ายภายในองค์การขนส่งมวลชนกรุงเทพจะต้องลงบันทึกขออนุญาตโดยต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๒.๑๕ สนับสนุนการควบคุมความเสี่ยงและการตรวจสอบภายในขององค์การ

ส่วนที่ ๒
การใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

๑. วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้งานที่เป็นบุคลากรของสำนักงานและบุคคลภายนอก ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของสำนักงาน ให้เป็นความลับ มีความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. ผู้รับผิดชอบ

๒.๑ สำนักเทคโนโลยีสารสนเทศ

๒.๒ ผู้ดูแลระบบสารสนเทศและ Outsource

๓. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๓.๑ ไม่ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายขององค์การขนส่งมวลชนกรุงเทพ โดยมีวัตถุประสงค์เพื่อเผยแพร่ข้อมูลที่ส่งผลกระทบกระเทือนต่อความมั่นคงและความสงบเรียบร้อยของชาติ ศาสนา และสถาบันพระมหากษัตริย์

๓.๒ ไม่นำเข้าหรือเผยแพร่ข้อมูลใดๆ ที่ก่อให้เกิดความเสียหายแก่ผู้อื่น

๓.๓ ไม่นำเข้าหรือเผยแพร่ข้อมูลใดๆ ที่มีลักษณะเป็นสื่อลามกอนาจาร

๓.๔ ไม่นำเข้าหรือเผยแพร่ข้อมูลใดๆ ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเกิดจากการสร้างขึ้น ตัดต่อ ต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่จะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๓.๕ ไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๓.๖ ไม่ฝ่าฝืนการเข้าถึงระบบสารสนเทศ ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

๓.๗ ไม่นำมาตรการป้องกันการเข้าถึงระบบสารสนเทศที่หน่วยงานจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบ

๓.๘ ไม่กระทำการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลของผู้อื่นที่อยู่ระหว่างการส่งในระบบสารสนเทศ และข้อมูลนั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

๓.๙ ไม่กระทำการอันอาจก่อให้เกิดความเสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลของผู้อื่นโดยมิชอบ

๓.๑๐ ไม่กระทำการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

๓.๑๑ ไม่ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์ของบุคคลอื่น

๓.๑๒ ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายขององค์การขนส่งมวลชนกรุงเทพ อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่หน่วยงาน

๓.๑๓ ไม่คัดลอกโปรแกรมต่างๆ ที่องค์การขนส่งมวลชนกรุงเทพเป็นเจ้าของลิขสิทธิ์อย่างถูกต้องตามกฎหมาย เพื่อนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓.๑๔ ไม่ทำการเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์และระบบเครือข่ายภายในองค์การขนส่งมวลชนกรุงเทพ

๓.๑๕ ผู้ใช้งานที่มีความประสงค์จะขอใช้เลขที่อยู่ไอพีสาธารณะ (Public IP Address) จะต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย

๓.๑๖ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย

๓.๑๗ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ขององค์การขนส่งมวลชนกรุงเทพเพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายขององค์การขนส่งมวลชนกรุงเทพได้ เว้นแต่จะได้รับอนุญาต

๓.๑๘ ห้ามใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

๓.๑๙ เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ขององค์การ

๓.๒๐ ผู้ใช้งานห้ามอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายขององค์การขนส่งมวลชนกรุงเทพร่วมกัน มิฉะนั้นเจ้าของชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการเข้าใช้งานของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๒๑ การตั้งรหัสผ่าน (Password) ในการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน

๓.๒๒ ทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งาน

๓.๒๓ ผู้ใช้งานจะต้องเก็บรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น

๓.๒๔ การใช้รหัสผ่าน (Password) สำหรับเครื่องคอมพิวเตอร์ ควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็ก หรือตัวพิมพ์ใหญ่ตัวอักขระพิเศษและสัญลักษณ์ต่างๆ ด้วย

๓.๒๕ ห้ามกำหนดรหัสผ่านจากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัวบุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์

๓.๒๖ กำหนดระยะเวลาในการเปลี่ยนรหัสผ่านที่เหมาะสม เพื่อใช้งานเครื่องคอมพิวเตอร์หรือเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุมีการรั่วไหล

(๑) สำหรับผู้ดูแลระบบ Administrator ต้องมีการเปลี่ยนแปลง Password ๓ เดือน / ครั้ง

(๒) สำหรับผู้ใช้งานระบบ User ต้องมีการเปลี่ยนแปลง Password ๑ เดือน / ครั้ง

๓.๒๗ การป้องกันจากโปรแกรมประสงค์ร้าย (Malware) เครื่องคอมพิวเตอร์ที่ใช้งานต้องติดตั้งโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้ายรวมทั้งปรับปรุงให้ทันสมัยอยู่เสมอ

๓.๒๘ ทำการปรับปรุง (Update) โปรแกรมคอมพิวเตอร์อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๓.๒๙ ไม่ทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์โดยมิได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๓.๓๐ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้ายห้ามเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้ายไปยังเครื่องคอมพิวเตอร์อื่นๆ และแจ้งผู้ดูแลระบบทราบ

๓.๓๑ ในการรับส่งข้อมูลคอมพิวเตอร์ หรือสารสนเทศ (Information) ผ่านทางระบบเครือข่าย ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) ก่อนการรับส่งทุกครั้ง

๓.๓๒ การใช้งานระบบอินเทอร์เน็ต ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น

๓.๓๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลและมีการจำกัดระยะเวลา ๒ ชม. สำหรับการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือ โปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๓.๓๔ ไม่ใช้ระบบอินเทอร์เน็ตขององค์การขนส่งมวลชนกรุงเทพเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ส่งผลกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหาย

๓.๓๕ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุง (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๓.๓๖ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) ให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๓.๓๗ การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ผู้ใช้งานที่ต้องการขอลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์โดยให้ยื่นคำขอต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย เพื่อดำเนินการกำหนดสิทธิ์บัญชีผู้ใช้บริการรายใหม่และรหัสผ่านโดยผู้ใช้บริการไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึงและควรมีการเปลี่ยนรหัสผ่านโดยกำหนดระยะที่เหมาะสม

๓.๓๘ ผู้ใช้งานห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่าน รับ-ส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน และเมื่อการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้บริการไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๓.๓๙ ในการติดต่อ รับ-ส่งข้อมูลราชการ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ (E-mail) ขององค์การขนส่งมวลชนกรุงเทพเท่านั้นเว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย

๓.๔๐ กรณีส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ผู้ใช้งานต้องสำรองข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๔.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๔.๒ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๔.๓ ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง

๔.๔ ผู้ใช้งานห้ามอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๔.๕ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๔.๖ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๔.๗ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๔.๘ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่นห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๔.๙ ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๕. การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication)

๕.๑ ผู้ใช้งานต้องได้รับอนุญาตโดยให้หน่วยงานต้นสังกัดยื่นขอ Username, Password ต่อหน่วยงานสำนักเทคโนโลยีสารสนเทศ และผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้งานระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๕.๒ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๕.๓ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่นห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๕.๔ ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๕.๕ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งาน (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้งาน (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๕.๖ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งาน (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่นห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๕.๗ ผู้ใช้งานจะต้องลงบันทึก (Login) โดยใช้บัญชีผู้ใช้งาน (Account) ของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๖. การสร้างความมั่นคงปลอดภัย

เพื่อให้การปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศขององค์การ และให้ผู้มีส่วนเกี่ยวข้องได้แก่ ผู้บริหาร พนักงาน ลูกจ้าง ผู้ใช้งานระบบ ผู้ดูแลระบบ และบุคคลภายนอก สามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ปี ๒๕๕๐

๖.๑ ผู้รับผิดชอบ

(๑) สำนักเทคโนโลยีสารสนเทศ องค์การขนส่งมวลชนกรุงเทพ

(๒) กลุ่มงานปฏิบัติการคอมพิวเตอร์และเครือข่าย

(๓) งานบริการระบบคอมพิวเตอร์และเครือข่าย

(๔) ผู้ใช้งานระบบสารสนเทศ

๖.๒ แนวปฏิบัตินี้ครอบคลุม ผู้บริหาร พนักงาน ลูกจ้าง ขององค์การฯ ที่มีหน้าที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับระบบสารสนเทศขององค์การ

๗. การปฏิบัติเพื่อการเข้าใช้งานระบบปฏิบัติการ

๗.๑ ผู้ดูแลระบบสารสนเทศองค์การต้องกำหนดมาตรฐานบัญชีผู้ใช้งานระบบ (Uername) และรหัสผ่าน (Password) ก่อนการเข้าใช้งานระบบปฏิบัติการ

๗.๒ ผู้ดูแลระบบองค์การตั้งค่าล็อคหน้าจอภาพ Screen Saver เมื่อไม่มีการใช้งานเป็นเวลา ๑๐ นาที หลังจากนั้นผู้ใช้งานระบบต้องทำการ Login ระบบอีกครั้ง

๗.๓ ผู้ใช้งานระบบต้องไม่อนุญาตให้ผู้อื่นใช้ Username Password ของตน เพื่อการเข้าใช้คอมพิวเตอร์องค์การ

๗.๔ ผู้ใช้งานระบบต้องทำการ Logout ทุกครั้งเมื่อเลิกใช้งานคอมพิวเตอร์องค์การ หรือกรณีไม่ได้อยู่ที่หน้าจอ เป็นเวลานานๆ

๘. ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต มีรายละเอียด ดังนี้

๘.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสมตัวอย่าง เช่น จัดอบรม พรบ.คอมพิวเตอร์โดยผู้เชี่ยวชาญเฉพาะด้าน

๘.๒ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) จัดให้มีการควบคุมและจำกัดสิทธิ์เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

๘.๓ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) จัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

(๑) ผู้ดูแลระบบสารสนเทศทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานให้ทำการทบทวนสิทธิ์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงของผู้ใช้งาน กรณีการย้ายตำแหน่งหน้าที่ การลาออก จะต้องมีการสอบทานสิทธิ์ในการใช้งานทุกครั้ง

(๒) จัดทำรายงานผู้มีสิทธิ์ในการใช้งานระบบสารสนเทศแยกประเภทแต่หน่วยงานที่ชัดเจน

(๓) ส่งรายชื่อผู้มีสิทธิ์ใช้งานระบบสารสนเทศของแต่ละหน่วยงานให้หัวหน้าหน่วยงาน เพื่อทำงานสอบทานสิทธิ์ว่ามีรายชื่อมีการเปลี่ยนแปลง และพื่อการแก้ไขให้ถูกต้อง

(๔) ผู้บังคับชาของหน่วยงานแจ้งรายชื่อหรืออนุมัติรายชื่อของผู้มีสิทธิ์ใช้งานระบบสารสนเทศที่ได้รับการแก้ไขให้ถูกต้องส่งให้ สำนักเทคโนโลยีสารสนเทศ

(๕) ผู้ดูแลระบสารสนเทศ ต้องกำหนดให้อุปกรณ์ต่อพ่วงและคอมพิวเตอร์ทุกประเภทต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที และมีการใช้รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

๙. แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet)

๙.๑ ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่สำนักเทคโนโลยีสารสนเทศจัดสรรไว้เท่านั้น และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็น และทำการขออนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษรแล้ว

๙.๒ ผู้ใช้งานต้องเข้าถึงระบบเทคโนโลยีสารสนเทศ ตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเท่านั้น และเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลขององค์การ ต้องไม่ใช้ระบบอินเทอร์เน็ต (Internet) ขององค์การเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันมีผลกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์การ

๙.๓ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงาน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๙.๔ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๙.๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

๙.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น ใช้ข้อความที่ยั่วยุ ให้ร้าย อันจะก่อให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์การ หรือการทำลายความสัมพันธ์กับบุคลากรขององค์การขนส่งมวลชนกรุงเทพ

๙.๗ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้งานต้องทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๑๐. แนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail Policy) แบ่งออก ๒ ส่วน

๑๐.๑ ผู้ดูแลระบบ

(๑) ต้องจัดทำขึ้นเพื่อให้เป็นแนวปฏิบัติสำหรับการบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการจดหมายอิเล็กทรอนิกส์ขององค์การ

(๒) สำหรับผู้ใช้งานจดหมายอิเล็กทรอนิกส์ขององค์การ เพื่อให้มีความปลอดภัยจากการคุกคามทางอินเตอร์เน็ต

(๓) เครื่องคอมพิวเตอร์ที่เปิดให้บริการจดหมายอิเล็กทรอนิกส์ต้องเป็นเครื่องให้บริการขององค์การที่ดูแลบริหารจัดโดยสำนักเทคโนโลยีสารสนเทศเท่านั้น

(๔) ผู้ดูแลระบบต้องจัดให้มีระบบตรวจสอบจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ผ่านเข้า-ออกเครื่องให้บริการจดหมายอิเล็กทรอนิกส์ขององค์การเพื่อป้องกันไวรัสและสแปม (SPAM)

(๕) ผู้ดูแลระบบต้องจัดทำรายงานสถานะของเครื่องให้บริการจดหมายอิเล็กทรอนิกส์ขององค์การอย่างน้อยไตรมาสละ ๑ ครั้ง

๑๐.๒ ผู้ใช้งาน

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบบัญชีที่ได้รับจากองค์การ ต้องระวังมิให้ผู้อื่นสามารถเข้าถึงรหัสผ่านเพื่อใช้งานบัญชีจดหมายอิเล็กทรอนิกส์ของตนโดยมิชอบ

(๒) ผู้ใช้งานต้องรักษารหัสผ่านและไม่อนุญาตให้ผู้อื่นใช้รหัสผ่านของตน

(๓) ผู้ใช้งานพึงทราบว่าผู้ดูแลระบบไม่มีสิทธิ์ถามหรือร้องขอผู้ใช้ให้เปิดเผยรหัสผ่านเพื่อเข้าใช้งานบัญชี

(๔) ผู้ใช้งานต้องไม่ใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

(๕) ห้ามเผยแพร่ หรือส่งต่อจดหมายลูกโซ่

(๖) ห้ามเผยแพร่ข้อมูลที่เป็นความลับขององค์การ

(๗) ห้ามปลอมแปลงหรือดัดแปลงชื่อผู้ส่งเพื่อให้บุคคลอื่นเข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้นมาจากบุคคลอื่น

(๘) ห้ามปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง

(๙) ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่เผยแพร่ ข้อความ ภาพ วิดีโอ หรือเสียงที่ให้ร้ายต่อบุคคลหรือกลุ่มบุคคล หรือในลักษณะที่หยาบคาย หรือลามก อนาจาร

(๑๐) ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อเผยแพร่โปรแกรมหรือรหัสผ่านสำหรับการเข้าโปรแกรมในลักษณะที่ละเมิดลิขสิทธิ์

(๑๑) ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อกระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้ที่ไม่ต้องการ

(๑๒) ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อกระจายไวรัส หรือโปรแกรมที่เป็นอันตรายกับความมั่นคงปลอดภัยของระบบครือข่าย

(๑๓) ห้ามมิให้ผู้ใช้งานนำบัญชีจดหมายอิเล็กทรอนิกส์ที่ได้รับจากองค์การไปสมัครสมาชิกตามเว็บไซต์ต่างๆ เพื่อประโยชน์ส่วนตน และไม่เกี่ยวข้องกับภารกิจขององค์การ

(๑๔) เมื่อได้รับรหัสผ่านครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที

(๑๕) ผู้ใช้งานควรเปลี่ยนรหัสผ่านทุกๆ ๓ – ๖ เดือน

(๑๖) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องลงบันทึกออก (Logout) ทุกครั้ง

(๑๗) ผู้ใช้งานควรหลีกเลี่ยงการส่งจดหมายอิเล็กทรอนิกส์ที่มีการแนบไฟล์ขนาดใหญ่สำหรับระบบขององค์การอนุญาตให้แนบไฟล์ขนาดไม่เกิน ๑๐ MB

(๑๘) ห้ามส่งข้อมูลที่เป็นความลับผ่านทางจดหมายอิเล็กทรอนิกส์โดยมิได้เข้ารหัสลับ

(๑๙) องค์การขอสงวนสิทธิ์ในการระงับการใช้งานบัญชีผู้ใช้ได้ทันทีโดยไม่ต้องแจ้งให้ทราบล่วงหน้าหากผู้ดูแลระบบตรวจพบความผิดปกติซึ่งอาจจะเกิดจากบัญชีผู้ใช้นั้น

๑๑. แนวปฏิบัติให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยมีรายละเอียด ดังนี้

๑๑.๑ กำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๑๑.๒ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๑๑.๓ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๑๑.๔ กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๑๑.๕ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๑๑.๖ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๑๑.๗ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๑๑.๘ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๑๑.๙ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๑๑.๑๐ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๑๑.๑๑ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๑๑.๑๒ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องทำการสำรองข้อมูลก่อนและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๑๑.๑๓ มาตรการควบคุมอุปกรณ์คอมพิวเตอร์และระบบสื่อสารเคลื่อนที่ต้องมีการจำกัดสิทธิ์ให้ใช้ได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยผู้ที่ได้รับอนุญาตจะได้รับ Username และ Password เฉพาะการเท่านั้น

๑๑.๑๔ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

(๑) การเข้าระบบสารสนเทศและแอพพลิเคชั่นขององค์การได้ดังนี้

- การใช้ระบบสารสนเทศและแอพพลิเคชั่นที่อนุญาตเปิดให้ใช้งานจากภายนอกได้โดยตรง คือ ระบบเว็ปไซต์ ระบบอีเมลล์
- การเข้าใช้ระบบสารสนเทศและแอพพลิเคชั่นผ่านระบบ SSL VPN

(๒) ผู้ใช้งานระบบสารสนเทศและแอพพลิเคชั่นจากภายนอกตามช่องทางในข้อ ๑๑.๑๔ (๑) ที่กำหนดรายละเอียดในแนวปฏิบัติ ส่วนที่ ๓ ข้อ ๕ แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบสารสนเทศ โดยใช้ Username และ Password ที่ได้รับจากสำนักเทคโนโลยีสารสนเทศมอบให้

(๓) กรณีเป็น Outsource ต้องได้รับอนุญาตโดยการอนุมัติจาก ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ ก่อนการเข้าใช้ระบบ โดยสามารถใช้ระบบได้ตามสิทธิ์ที่ได้รับอนุญาตการใช้ Username และ Password ที่ได้รับอนุญาตเท่านั้น

(๔) ผู้ดูแลระบบต้องกำหนดหน้าที่และสิทธิ์ที่เข้าใช้งานระบบและแอพพลิเคชั่นให้ใช้งานระบบได้เพียงสิทธิ์ที่ได้รับ ตามที่อนุญาตเท่านั้น

(๕) มีการจำกัดสิทธิ์ในการใช้งานระบบสารสนเทศและมีกำหนดระยะเวลาให้ใช้งานได้เท่าที่จำเป็นและตามลำดับความสำคัญ

๑๑.๑๕ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๑) ผู้ใช้งานห้ามนำโปรแกรมต่างๆ มาติดตั้งหรือใช้งานในเครื่องคอมพิวเตอร์ในหน่วยงานองค์การ โดยมิได้รับอนุญาตจาก สำนักเทคโนโลยีสารสนเทศ โดยเด็ดขาด

(๒) หากฝ่าฝืนตามมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ ถือเป็นความผิดวินัยร้ายแรง ให้หน่วยงาน สำนักเทคโนโลยีสารสนเทศ ตั้งคณะกรรมการสอบสวน เสนอผู้มีอำนาจพิจารณาโทษตามระเบียบข้อบังคับองค์การ

(๓) กรณีมีความจำเป็นต้องใช้งานโปรแกรมนอกเหนือจากที่หน่วยงานองค์การอนุญาตให้ใช้จะต้องแจ้งเป็นหนังสือขออนุญาตต่อ สำนักเทคโนโลยีสารสนเทศ พิจารณาอนุญาตก่อนการใช้งานทุกครั้ง

(๔) การใช้ซอฟต์แวร์สำหรับเครื่องคอมพิวเตอร์ขององค์การจะต้องมี License หรือลิขสิทธิ์ถูกต้องเท่านั้น หากมีการฝ่าฝืนหรือ เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ ตรวจพบ ผู้ใช้งานจะต้องรับผิดทางวินัยตามระเบียบองค์การกำหนด

๑๑.๑๖ การใช้อุปกรณ์คอมพิวเตอร์และคอมพิวเตอร์พกพา

(๑) อุปกรณ์คอมพิวเตอร์ที่ได้รับอนุญาตให้ผู้ใช้งาน เป็นอุปกรณ์หรือทรัพย์สินขององค์การ ผู้ใช้งานจำต้องใช้งานอย่างมีประสิทธิภาพสูงสุดเพื่อประโยชน์ขององค์การ เท่านั้น

(๒) โปรแกรมต่างๆ หรือซอฟต์แวร์ที่ติดตั้งบนคอมพิวเตอร์ขององค์การเป็นซอฟต์แวร์ลิขสิทธิ์ที่องค์การได้จัดหามาถูกต้องตามกฎหมาย ห้ามผู้ใช้งานทำการคัดลอกไม่ว่าด้วยวิธีการใดๆ หรือนำไปติดตั้งบนคอมพิวเตอร์ส่วนตัวหรือจำหน่ายจ่ายแจก โดยเด็ดขาด

(๓) องค์การไม่อนุญาตให้ผู้ใช้งานเปลี่ยนแปลงแก้ไข หรือติดตั้ง ซอฟต์แวร์ในอุปกรณ์คอมพิวเตอร์ส่วนบุคคลขององค์การ ต้องได้รับการอนุญาตเป็นลายลักษณ์อักษรจาก สำนักเทคโนโลยีสารสนเทศ ก่อนทุกครั้ง

(๔) องค์การไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งคอมพิวเตอร์เพื่อการเชื่อมต่อระบบเน็ตเวิร์คขององค์การ

(๕) การเปลี่ยนแปลงการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ รวมถึงการตรวจซ่อมจะต้องแจ้งให้เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ เป็นผู้ดำเนินการเท่านั้น

(๖) ผู้ใช้งานต้องตรวจสอบอุปกรณ์เชื่อมต่อทุกประเภท รวมทั้ง Thumbdrive ที่นำมาเชื่อมต่อคอมพิวเตอร์ ต้องทำการตรวจสอบไวรัสทุกครั้งก่อนการใช้งาน

(๗) เครื่องคอมพิวเตอร์เป็นทรัพย์สินขององค์การ พนักงาน ผู้ใช้งานมีหน้าที่ดูแลรักษาให้ทรัพย์สินขององค์การมีความปลอดภัยทุกด้าน

ส่วนที่ ๓
การควบคุมการเข้าถึงและการจัดการระบบเครือข่าย

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายขององค์การ และป้องกันการบุกรุกผ่านระบบเครือข่าย หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายขององค์การได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ สำนักเทคโนโลยีสารสนเทศ

๒.๒ ผู้ดูแลระบบสารสนเทศและ Out Source

๓. แนวปฏิบัติการกำหนดมาตรการปรับปรุงและควบคุมการเข้าถึงระบบสารสนเทศ ปฏิบัติดังนี้

๓.๑ แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยประเภทข้อมูล

๓.๑.๑ ชนิดของข้อมูลแบ่งได้ดังนี้ ๒ ชนิด

(๑) ข้อมูลเอกสาร

(๒) ข้อมูลอิเล็กทรอนิกส์, ฐานข้อมูล (Data Base)

๓.๑.๒ การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล โดยใช้ตามแนวทางระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๓.๑.๓ การรับส่งเอกสารข้อมูลที่มีความสำคัญและเป็นความลับ ผ่านระบบเน็ตเวิร์ค ต้องได้รับการป้องกันโดยการเข้ารหัสที่เป็นมาตรฐานสากล โดยให้ส่งเป็นประเภทไฟล์ PDF และมีการเข้ารหัสสำหรับการเปิดไฟล์ โดยส่งรหัสการเปิดไฟล์ ไปให้ผู้รับทางอื่น

๓.๑.๔ ประเภทของข้อมูลแบ่งเป็น ๒ ประเภท

(๑) ข้อมูลภายใน หมายถึง ข้อมูลทั้งที่เป็นความลับและไม่เป็นความลับ สำหรับที่ใช้ในการดำเนินการภายในภารกิจขององค์การ หรือที่สามารถเปิดเผยแก่บุคคลภายนอกได้เฉพาะที่ได้รับอนุญาตจากผู้มีอำนาจลงนาม และข้อมูลภายในจะเปิดเผยเพื่อการดำเนินการสำหรับภารกิจขององค์การเท่านั้น

(๒) ข้อมูลทั่วไปเพื่อการเปิดเผย หมายถึง ข้อมูลที่สามารถเปิดเผยได้แก่บุคคลทั่วไป โดยไม่ก่อให้เกิดความเสียหายหรือที่ส่งผลกระทบกับภารกิจขององค์การ

๓.๑.๕ ลำดับชั้นความลับของข้อมูลแบ่งได้ ๓ ระดับ ดังนี้

(๑) ข้อมูลลับ

(๒) ข้อมูลลับมาก

(๓) ข้อมูลลับที่สุด

๓.๑.๖ หลักเกณฑ์การจัดชั้นระดับความลับของข้อมูล อาศัยความสำคัญดังนี้

(๑) ข้อมูลที่สามารถเปิดเผยได้ทั้งหมด หรือบางส่วนจะส่งผลกระทบให้เกิดความเสียหาย กำหนดให้ข้อมูลนั้นเป็นชั้นระดับข้อมูลลับ

(๒) ข้อมูลที่สามารถเปิดเผยได้ทั้งหมดหรือบางส่วนจะส่งผลกระทบให้เกิดความเสียหายร้ายแรง กำหนดให้ข้อมูลเป็นชั้นระดับข้อมูลลับมาก

(๓) ข้อมูลที่สามารถเปิดเผยได้ทั้งหมดหรือบางส่วนจะส่งผลกระทบให้เกิดความเสียหายร้ายแรง กำหนดให้ข้อมูลเป็นชั้นระดับข้อมูลลับที่สุด

๓.๑.๗ ระดับชั้นของการเข้าถึงข้อมูล

(๑) เอกสารกระดาษ มีระบบการจัดเก็บในตู้เอกสารพร้อมป้องกันการเข้าถึง รวมทั้งจัดทำแฟ้มเอกสารระบุแฟ้มให้ชัดเจน เพื่อความสะดวกรวดเร็วในการค้นหาและการให้บริการ

(๒) ข้อมูลอิเล็กทรอนิกส์ (ฐานข้อมูล) จัดเก็บในระบบเครื่องแม่ข่าย (SERVER) โดยกำหนดระดับชั้นการเข้าถึงระบบและสิทธิ์ในการใช้ระบบที่กำหนดระยะเวลาตามลำดับชั้น

๓.๑.๘ เวลาที่ได้เข้าถึงข้อมูลและอุปกรณ์มวลผล

(๑) แฟ้มข้อมูลอิเล็กทรอนิกส์ สามารถเข้าถึงได้ตลอดเวลา ตามระดับชั้นของผู้ใช้งาน User/Password

(๒) ข้อมูลเอกสารกระดาษ สามารถเข้าถึงได้ตามวันเวลาราชการ เฉพาะที่ได้รับอนุญาตจากผู้มีอำนาจลงนามอนุญาตตามระเบียบองค์การ

๓.๑.๙ การรักษาความลับของข้อมูล

(๑) ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ.๒๕๔๔ เว้นแต่องค์การจะประกาศไว้เป็นอย่างอื่น

(๒) การรับ-ส่งข้อมูลสารสนเทศที่มีระดับชั้นความลับ ผ่านระบบเครือข่ายองค์การหรือเครือข่ายอื่นๆ จะต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล

๓.๒ จัดให้มีการอบรม การสร้างความตระหนักและความรู้ความเข้าใจถึงผลกระทบต่อความรู้เท่าไม่ถึงการณ์ เรื่องความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ผู้รับการฝึกอบรมมีความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้สอดคล้องกับภารกิจและข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัย

๓.๓ บริหารจัดการ การเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ด้วยการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓.๔ กำหนดแบ่งแยก การใช้งานระบบเครือข่ายที่สำคัญ เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ระบบอินทราเน็ต (Intranet) โดยต้องมีการควบคุมให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และได้รับความเห็นชอบจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอให้สอดคล้องกับข้อปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย

๓.๕ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย

๓.๖ ทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งานผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๓.๗ ผู้ดูแลระบบ (System Administrator) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๓.๘ ดำเนินการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงานเพื่อใช้ในการกำหนดว่า หมายเลขระบุอุปกรณ์ใดจะสามารถเข้าถึงเครือข่ายส่วนใดขององค์กร

๓.๙ ผู้ดูแลระบบ (System Administrator) การควบคุม ซอฟต์แวร์หรือฮาร์ดแวร์ เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมายทราบทันที

๓.๑๐ การนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายขององค์การขนส่งมวลชนกรุงเทพต้องได้รับอนุญาตจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย และต้องปฏิบัติตามนโยบายอย่างเคร่งครัด

๓.๑๑ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่องค์การขนส่งมวลชนกรุงเทพรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

๓.๑๒ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่อพ่วงอุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๓.๑๓ ระบบเครือข่ายทั้งหมดขององค์การขนส่งมวลชนกรุงเทพที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย และต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๓.๑๔ การเข้าสู่ระบบเครือข่ายภายในองค์การขนส่งมวลชนกรุงเทพโดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ ซึ่งเลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๓.๑๕ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก มีการแยกวงของเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ ซึ่งการใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมายและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๓.๑๖ การบริหารและควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (System Software)

๓.๑๗ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ โดยควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อบันทึกข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อบันทึกดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแล

ระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่องค์การขนส่งมวลชนกรุงเทพ มอบหมาย

๓.๑๘ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง และควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ อีกทั้งต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๓.๑๙ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยบุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ขององค์การขนส่งมวลชนกรุงเทพจะต้องทำเรื่องขออนุญาตจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย

๓.๒๐ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และการปิดพอร์ทที่ไม่จำเป็น รวมถึงวิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลหรือจากบุคคลภายนอกต้องได้รับการอนุญาตผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย ซึ่งการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงาน

๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

๔.๑ องค์การกำหนดให้มีมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศเพื่อดูแลรักษาความปลอดภัยโดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรตามสายงานต่อหัวหน้าหน่วยงานที่ควบคุมดูแลรับผิดชอบการเข้าถึงระบบสารสนเทศ

๔.๒ จัดให้มีการอบรมการปฏิบัติหน้าที่ผู้ใช้งาน เพื่อเพิ่มความรู้ความเข้าใจถึงผลกระทบต่อความรู้เท่าไม่ถึงการณ์เรื่องความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้รับการฝึกอบรมมีความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านระบบสารสนเทศ และสอดคล้องกับการใช้งานตามภารกิจขององค์การ

๔.๓ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างน้อยปีละ ๑ ครั้ง

๔.๔ ผู้ดูแลระบบจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศที่มีต่อระบบข้อมูลสารสนเทศ

๔.๕ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ

๔.๖ ผู้ดูแลระบบต้องจัดให้มีการตรวจสอบการกำหนดสิทธิตามลำดับความสำคัญของระบบสารสนเทศ

๔.๗ ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร และกำหนดสิทธิ์การเข้าใช้งานระบบสารสนเทศจากภายนอก

๔.๘ ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการเข้าใช้งานระบบสารสนเทศจากภายนอกองค์การ ผู้ดูแลระบบต้องกำหนดความสำคัญของระบบสารสนเทศ และมีการควบคุมอุปกรณ์คอมพิวเตอร์ และการปฏิบัติงานภายนอกองค์กรเพื่อให้ระบบสารสนเทศที่มีความสำคัญสูงปลอดภัยมากที่สุด

๔.๙ ผู้ดูแลระบบต้องมีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่อื่นใดในการเข้าใช้ระบบสารสนเทศ

๔.๑๐ การจัดระบบสารสนเทศที่มีความสำคัญสูงขององค์การ

(๑) จัดให้มีระบบการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมตามแนวปฏิบัติส่วนที่ ๑ การรักษาความมั่นคงทางกายภาพและสิ่งแวดล้อม

(๒) การจัดการระบบสารสนเทศที่มีความสำคัญสูงต่อองค์การ ต้องดำเนินการแยกออกจากระบบสารสนเทศอื่น

(๓) ผู้ดูแลระบบสารสนเทศต้องมีเครื่องมือ ที่ใช้ในการตรวจสอบสภาพพร้อมใช้งานของระบบสารสนเทศขององค์การ

(๔) ต้องจัดให้มีการทำระบบสำรองสารสนเทศที่มีความสำคัญสูงต่อองค์การ ตามแนวปฏิบัติส่วนที่ ๕ การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

๕. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบสารสนเทศ

สำนักเทคโนโลยีสารสนเทศ ผู้ดูแลระบบ (System Administrator) ได้กำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญเช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งได้มีการทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ ผู้ดูแลระบบได้บริหารจัดการสิทธิ์ของผู้ใช้งาน ดังต่อไปนี้

๕.๑ กำหนดจำแนกประเภทสิทธิ์ของผู้ใช้งาน

(๑) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ ระดับผู้บริหาร CIO/Administrator

(๒) ผู้ช่วยผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ ระดับผู้บริหาร Administrator

(๓) หัวหน้ากลุ่มงานปฏิบัติการคอมพิวเตอร์และเครือข่าย ระดับ Administrator

(๔) หัวหน้ากลุ่มงานวางแผนและพัฒนาระบบเทคโนโลยีสารสนเทศ ระดับ Administrator

(๕) หัวหน้างานปฏิบัติการคอมพิวเตอร์ ระดับ User

(๖) หัวหน้างานบริการระบบคอมพิวเตอร์และเครือข่าย ระดับ User

(๗) หัวหน้างานพัฒนาระบบสารสนเทศ ระดับ User

(๘) หัวหน้างานแผนและเผยแพร่ความรู้เทคโนโลยีสารสนเทศ ระดับ User

๕.๒ ในกรณีผู้ใช้งานมีความจำเป็นต้องใช้สิทธิ์สูงกว่าปกติ ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงข้อมูลระดับใดได้บ้าง โดยกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติเพื่อผู้ดูแลระบบจะได้ดำเนินการปรับค่าหรือแก้ไขต่อไป

๕.๓ ทำการยกเลิกรหัสผ่าน (Password) เมื่อได้รับการแจ้งจากหน่วยงานบริหารงานบุคคลหรือผู้เกี่ยวข้อง เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่งหรือยกเลิกอำนาจหน้าที่

๕.๔ ระบบการบริหารสิทธิ์และวิธีการเข้าใช้งานระบบสารสนเทศ

ผู้ใช้งานระบบ	ผู้บริหาร	พนักงาน	ลูกจ้าง	บุคคลภายนอก
	GIS/EIS	ระบบงาน ๑, ๒	ระบบสารบรรณ	www.bmta.co.th

ผู้ใช้งานระบบ	ผู้บริหาร	พนักงาน	ลูกจ้าง	บุคคลภายนอก
ระบบ สารสนเทศ	MIS	ระบบสารบรรณ	Internet	Call Center ๑๓๔๘
	ระบบสารบรรณ	MIS	Intranet bmta	
	Internet	Internet	www.bmta.co.th	
	VPN	Intranet bmta		
	Wireless HO	www.bmta.co.th		
	E-mail			
	www.bmta.co.th			

๖. แนวปฏิบัติกำหนดให้ผู้ดูแลระบบ (System Administrator) ปฏิบัติดังนี้

๖.๑ ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายขององค์การขนส่งมวลชนกรุงเทพให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข ป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้น พร้อมทั้งรายงานต่อผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย ทราบในทันที

๖.๒ กรณีเกิดสิ่งผิดปกติขึ้นจากการใช้งานของผู้ใช้ที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่อาจจะเกิดขึ้นแก่องค์การขนส่งมวลชนกรุงเทพ ให้ผู้ดูแลระบบพิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

๖.๓ ดำเนินการติดตั้ง ตรวจสอบและปรับปรุงโปรแกรมคอมพิวเตอร์ระบบสารสนเทศ และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและถูกต้อง ทันสมัยอยู่เสมอ

๖.๔ ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที รวมถึงดูแลรักษาและปรับปรุงบัญชีผู้ใช้งาน (Account) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์การใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

๖.๕ ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้บริการให้มีการกำหนดรหัสผ่าน (Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password) และไม่ใช้อำนาจหน้าที่ของผู้ดูแลระบบ (System Administrator) ในการเข้าถึงข้อมูลของผู้ใช้ที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร และไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร รวมถึงไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

๖.๖ เมื่อผู้ดูแลระบบ (System Administrator) พ้นจากหน้าที่จะต้องคืนสินทรัพย์ของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และรหัสให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายดำเนินการตรวจสอบ

๖.๗ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวัน

นับตั้งแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องใช้วิธีการที่มั่นคงปลอดภัย โดยเก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ (System Administrator) สามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ ซึ่งในการเก็บข้อมูลจราจรนั้นต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

๖.๘ การบริหารจัดการรหัสผ่าน (Password Management System)

(๑) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนโดยลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศขององค์การ

(๒) การมอบบัญชีผู้ใช้งานให้กับผู้ใช้งานครั้งแรก ให้กำหนดรหัสผ่านชั่วคราวจากการสุ่มให้กับผู้ใช้งานเมื่อผู้ใช้งานได้รับรหัสผ่านแล้ว ให้เปลี่ยนรหัสผ่านนั้นเป็นรหัสผ่านของตนเองที่เป็นไปตามแนวปฏิบัติการใช้งานรหัสผ่านมาตรฐานความปลอดภัย

(๓) การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัยโดยให้ใช้วิธีการใส่ซองปิดผนึกหรือกระดาษสลิปคาร์บอนด์ จากนั้นส่งมอบให้ผู้กับใช้งานระบบโดยตรง

(๔) ผู้ใช้งานต้องตอบรับการยืนยันการได้รับรหัสผ่าน ผ่านระบบอีเมลล์

(๕) กรณีที่ผู้ใช้ระบบสารสนเทศลาออก หรือไม่มีหน้าที่ความรับผิดชอบเกี่ยวกับระบบสารสนเทศ ที่ขอสิทธิ์ในการใช้งาน ให้หัวหน้าหน่วยงานแจ้ง สำนักเทคโนโลยีสารสนเทศทันที เพื่อเปลี่ยนสิทธิ์หรือถอนออกจากระบบผู้ใช้งานระบบสารสนเทศ ทันที

(๖) ผู้ดูแลระบบสารสนเทศ จัดระบบที่สนองความต้องการของผู้ใช้ระบบให้สามารถเปลี่ยนรหัสผ่านของตนเองได้โดยเปลี่ยนรหัสผ่านทุกๆ ๑๘๐ วัน

(๗) ผู้ดูแลระบบสารสนเทศ สามารถกำหนดความเหมาะสมจำนวนครั้งที่ยอมให้ User ผู้ใช้งานใส่รหัสผิดพลาดได้ไม่เกิน ๓ ครั้ง ในการเข้าใช้งานระบบสารสนเทศ

๖.๙ การใช้รหัสผ่านอย่างปลอดภัย (Password use)

(๑) รหัสผ่าน (Password) มีความยาวไม่น้อยกว่า ๖ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัว พิมพ์เล็ก หรือตัว พิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆ โดยใช้อักขระพิเศษประกอบ

(๒) กำหนดรหัสผ่าน (Password) จากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์ และไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน

(๓) ทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์ของสำนักงานทุก ๓-๖ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่ามีการรั่วไหล

(๔) ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่กำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

(๕) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ต้องเปลี่ยนรหัสผ่านนั้นโดยทันที

(๖) ผู้ใช้งานเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

(๗) หากมีการนำอุปกรณ์สื่อสารสนเทศอื่นๆเข้ามาต่อพวงอย่างเช่น แฟลชไดร์ฟ, สมาร์ทโฟน, กล้องดิจิตอล ผู้ใช้งานจะต้องแน่ใจว่าอุปกรณ์เหล่านั้นไม่ก่อให้เกิดความเสียหายต่ออุปกรณ์คอมพิวเตอร์ภายในองค์การหากจำเป็นต้องมีการเชื่อมต่อ ต้องแจ้งเจ้าหน้าที่ สำนักเทคโนโลยีสารสนเทศ เพื่อทำการตรวจสอบก่อนการใช้งาน

๗. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Management)

๗.๑ การจัดการเครือข่ายไร้สาย (Wireless Management) จัดทำขึ้นเพื่อเป็นแนวปฏิบัติสำหรับการบริหารจัดการระบบเครือข่ายไร้สาย WISE (Wireless Service for Education) ขององค์การให้มีความเหมาะสมและสอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์การ

๗.๒ ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) ไม่ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุดเพื่อความปลอดภัย

๗.๓ ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ตามที่ได้ถูกกำหนดเป็นค่าเริ่มต้นไว้ (default setting) โดยผู้ผลิต ทันทีที่นำอุปกรณ์กระจายสัญญาณมาติดตั้งใช้งาน

๗.๔ ผู้ดูแลระบบ (System Administrator) ดำเนินการกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สายตามความเหมาะสมในกรณีต่างๆ

๗.๕ ผู้ดูแลระบบ (System Administrator) ใช้วิธีการควบคุมผ่านระบบ AD (Active Directory) โดยกำหนดชื่อผู้ใช้ (Username) รหัสผ่าน (Password) สำหรับพนักงานและใช้วิธีการควบคุมผ่านระบบ Firewall Authentication โดยกำหนดชื่อผู้ใช้ (Username) รหัสผ่าน (Password) สำหรับบุคคลภายนอก

๗.๖ ผู้ดูแลระบบ (System Administrator) ได้กำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๗.๗ อุปกรณ์กระจายสัญญาณที่มีคุณสมบัติตามข้อกำหนดมาตรฐานขององค์การ จะต้องถูกติดตั้งระบบการยืนยันการพิสูจน์ตัวตนการเข้าใช้งานเครือข่ายขององค์การ

๗.๘ กรณีอุปกรณ์กระจายสัญญาณที่จัดหาไม่สามารถติดตั้งระบบการยืนยันการพิสูจน์ตัวตนการเข้าใช้งานเครือข่ายได้นั้น ผู้ดูแลระบบจะต้องดำเนินการติดตั้งให้เป็นแบบ Bridge เท่านั้นเพื่อให้ผู้ใช้งานยืนยันตัวตนผ่านระบบขององค์การ

๗.๙ ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๗.๑๐ ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์ หรือ ฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยติดตามและบันทึกเหตุการณ์น่าสงสัยในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจพบความผิดปกติในการใช้งาน ผู้ดูแลระบบต้องรายงานต่อผู้บริหารของหน่วยงานให้ทราบทันที

๗.๑๑ ผู้ดูแลระบบ ต้องควบคุมดูแลมิให้บุคคล หรือ หน่วยงานภายนอกที่มิได้รับอนุญาตใช้งานระบบเครือข่ายไร้สาย ขององค์การขนส่งมวลชนกรุงเทพ เพื่อการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในขององค์การ

๘. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๘.๑ สำนักเทคโนโลยีสารสนเทศได้กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ไม่ใช่เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ โดยต้องลงทะเบียนขออนุญาต ระบุ วัน-เวลา เข้าออกและเหตุผลความจำเป็น

๘.๒ ผู้ใช้งานภายนอกที่จะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงาน ต้องได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๘.๓ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๘.๔ ผู้ดูแลระบบ (System Administrator) ควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๘.๔.๑ ใช้วิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๘.๔.๒ มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๘.๔.๓ มีการกำหนดให้จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ของผู้ใช้งานไปยังเครื่องคอมพิวเตอร์แม่ข่าย

๘.๔.๔ ระบบเครือข่ายทั้งหมดของสำนักงาน ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นภายนอกสำนักงาน ได้ถูกเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก และมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware)

๘.๔.๕ การเข้าสู่ระบบเครือข่ายภายในสำนักงาน ผ่านทางระบบอินเทอร์เน็ตได้กำหนดให้ลงบันทึกเข้า (Login) โดยระบุชื่อผู้ใช้งานและรหัสผ่านผู้ใช้งานผ่านระบบพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้งาน

๘.๔.๖ กำหนดเลขที่อยู่ไอพี (IP Address) ของระบบเครือข่ายให้กับอุปกรณ์ ที่เชื่อมต่อกับระบบเครือข่ายให้สามารถระบุถึงอุปกรณ์นั้นได้อย่างถูกต้อง กรณีที่ไม่สามารถใช้เลขที่อยู่ไอพี แอดเดรสในการระบุอุปกรณ์บนเครือข่ายได้ กำหนดให้ใช้เลขแม็คแอดเดรส ในการระบุอุปกรณ์บนเครือข่ายแทน

๘.๔.๗ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก ที่สามารถระบุบนระบบเครือข่ายและอุปกรณ์บนเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอและการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) มีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๘.๔.๘ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย จะต้องได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๘.๔.๙ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ควบคุมการเข้าถึง

(๑) ตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่ใช้งาน สำหรับพอร์ตที่ใช้ในการตรวจสอบและปรับแต่งระบบ ต้องมีการยืนยันตัวตนและอนุญาตให้เฉพาะผู้มีสิทธิ์เท่านั้น

๘.๔.๑๐ มีการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

(๑) ผู้ดูแลระบบเครือข่ายต้องกำหนดตารางการใช้งานบนระบบเครือข่าย (Network routing table) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ (Switch) เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานได้เฉพาะที่ได้รับอนุญาต

(๒) ผู้ดูแลระบบเครือข่ายต้องจำกัดการใช้เส้นทางบนระบบเครือข่ายจากอุปกรณ์คอมพิวเตอร์ของผู้ใช้งานไปยังเครื่องแม่ข่ายที่ให้บริการต่างๆ โดยกำหนดให้ใช้เส้นทางตามที่กำหนดให้เท่านั้น

(๓) ผู้ดูแลระบบเครือข่ายต้องจำกัดการใช้เส้นทางบนระบบเครือข่ายจากอุปกรณ์คอมพิวเตอร์ที่ใช้งานไปยังเครื่อง (Server) โดยในการเชื่อมต่อเข้าสู่เครื่องแม่ข่ายหลัก ที่ให้บริการเพื่อบริหารระบบ กำหนดชุดไอพีแอดเดรส (IP Address) สำหรับผู้ดูแลระบบสารสนเทศเท่านั้นที่สามารถเข้าถึงเครื่องแม่ข่ายนั้นได้

(๔) ผู้ดูแลระบบเครือข่ายจะต้องบริหารจัดการอุปกรณ์ Firewall เพื่อควบคุมการเข้าถึงระบบเครือข่าย

๘.๔.๑๑ การควบคุมการเชื่อมต่อทางระบบเครือข่าย (Network Connection Control)

(๑) ใช้ Mornitoring Tools เพื่อการตรวจสอบการเชื่อมต่อระบบเครือข่าย

(๒) ติดตั้งระบบการตรวจสอบผู้บุกรุกทั้งบนระบบเครือข่ายและระดับเครื่องแม่ข่าย

(๓) ควบคุมการไม่ให้มีการเปิดการให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

๘.๕ ผู้ดูแลระบบ (System Administrator) ทำหน้าที่บริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

๘.๖ สำนักเทคโนโลยีสารสนเทศได้กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๘.๖.๑ ความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ กำหนดชั้นความลับในการเข้าถึงข้อมูลซึ่งผู้ดูแลระบบไม่ได้รับอนุญาตให้แก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศขององค์การ (Internal IT Auditor) หรือบุคคลที่สำนักเทคโนโลยีสารสนเทศ มอบหมาย

๘.๖.๒ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๘.๖.๓ ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๘.๖.๔ วิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๘.๗ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

๘.๗.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย (Server) ขององค์การ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๘.๗.๒ ผู้ดูแลระบบได้ควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๘.๗.๓ วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๘.๗.๔ การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๘.๗.๕ การเข้าใช้งานต้องผ่านระบบการพิสูจน์ตัวตนจากระบบขององค์การ

๙. แนวปฏิบัติการจัดการไฟล์วอลล์ (Firewall Management)

๙.๑ สำนักเทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการและกำหนดค่าการใช้งานของอุปกรณ์รักษาความปลอดภัย (firewall) ส่วนกลางบนเครือข่ายขององค์การ

๙.๒ บริการต่างๆ จะถูกปฏิเสธทั้งหมด ยกเว้นแต่บริการที่ทางสำนักเทคโนโลยีสารสนเทศเปิดให้บริการเท่านั้น

๙.๓ ก่อนการใช้งานอินเทอร์เน็ตทุกครั้ง ผู้ใช้งานจะต้องทำการล็อกอินโดยใช้ไอดีที่กำหนดให้ใช้เท่านั้น

๙.๔ การเปลี่ยนแปลงการกำหนดค่าต่างๆ บนอุปกรณ์รักษาความปลอดภัยจะต้องดำเนินการโดยผู้ที่ได้รับมอบหมายเท่านั้น โดยทุกครั้งที่มีการเปลี่ยนแปลงต้องมีการบันทึกข้อมูล และสำรองข้อมูลค่าต่างๆ ไว้ก่อนเสมอ

๙.๕ การให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายจะมีการเปิดพอร์ตที่เป็นการใช้งานพื้นฐานโปรแกรมทั่วไปเท่านั้น กรณีที่ผู้ใช้ต้องการเชื่อมต่อผ่านพอร์ตอื่นนอกเหนือจากที่กำหนดต้องได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศก่อน

๙.๖ พอร์ตที่ใช้สำหรับตรวจสอบและการปรับแต่งระบบจะต้องเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๙.๗ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายจะต้องกำหนดค่าการให้บริการที่จำเป็นต่อการให้บริการ

๙.๘ ให้บริการตามแบบบันทึกลงในสมุดขอเปิดใช้บริการเครื่องคอมพิวเตอร์แม่ข่ายเท่านั้นอุปกรณ์รักษาความปลอดภัยต้องกำหนดให้มีการบันทึกและจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ที่ผ่านเข้าออกอุปกรณ์นั้นไม่น้อยกว่า ๙๐ วัน

๙.๙ เส้นทางการเชื่อมต่อระบบเครือข่ายจะต้องมีการควบคุมเพื่อป้องกันข้อมูลสารสนเทศที่มีความสำคัญสูง

๙.๑๐ ในกรณีตรวจพบว่าเครื่องคอมพิวเตอร์ลูกข่ายใดที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบายหรือมีการใช้งานอันจะก่อให้เกิดปัญหาต่อระบบเครือข่าย สำนักเทคโนโลยีสารสนเทศ ขอสงวนสิทธิ์ในการระงับหรือ บล็อกการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายนั้นจนกว่าจะดำเนินการแก้ไขเสร็จสิ้น

๙.๑๑ ผู้ละเมิดนโยบายด้านความปลอดภัยของระบบเครือข่ายขององค์การจะถูกระงับการใช้งานทันทีโดยมิต้องแจ้งให้ทราบล่วงหน้า

๑๐. แนวปฏิบัติการป้องกันไวรัสคอมพิวเตอร์ (การจัดการระบบเครือข่าย)

๑๐.๑ การป้องกันไวรัสคอมพิวเตอร์ (Computer Virus Prevention) เพื่อให้เกิดความปลอดภัยจากภัยคุกคามที่เกิดจากการแพร่ระบาดของไวรัสคอมพิวเตอร์และสามารถแก้ไขปัญหาได้ทันท่วงที

๑๐.๒ Update Patch ของระบบปฏิบัติการของเครื่องคอมพิวเตอร์ เพื่อลดความเสี่ยงในการถูกโจมตีผ่านช่องโหว่ของระบบสารสนเทศ

๑๐.๓ จัดหาและติดตั้งระบบป้องกันไวรัสที่สามารถควบคุมการทำงานของโปรแกรมป้องกันไวรัสได้จากศูนย์กลางของระบบคอมพิวเตอร์องค์การ

๑๐.๔ ดำเนินการติดตั้งโปรแกรมป้องกันไวรัสบนเครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่อง

๑๐.๕ ตรวจสอบการปรับปรุงฐานข้อมูล Virus Signature บนเครื่องคอมพิวเตอร์ลูกข่ายทุกครั้งที่มีการเปิดเครื่อง

๑๐.๖ ตรวจสอบการปรับปรุง Virus Signature บนเครื่องคอมพิวเตอร์ลูกข่ายทุกๆ ๔ ชั่วโมงเป็นอย่างน้อย

๑๐.๗ จัดทำขั้นตอนการจัดการกับปัญหาเมื่อพบว่ามีการแพร่ระบาดของไวรัสคอมพิวเตอร์

๑๐.๘ จัดทำรายงานไวรัสที่ตรวจจับได้ภายในองค์การขนส่งมวลชนกรุงเทพ และจำนวนเครื่องที่ติดไวรัสชนิดนั้น เดือนละ ๑ ครั้ง และรายงานผู้เกี่ยวข้องทราบ

๑๑. แนวการปฏิบัติการบริหารจัดการเครื่องแม่ข่ายสำหรับเว็บ (Web Server Management)

๑๑.๑ จัดทำ Web server checklist เช่น Apache และ IIS

๑๑.๒ ทบทวนและปรับปรุง Web server checklist อย่างสม่ำเสมอและทันต่อสถานการณ์ที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา

๑๑.๓ กำหนด Version ของเอกสาร Security Checklist เพื่อป้องกันการสับสนในการนำไปใช้งาน

๑๑.๔ ตรวจสอบในส่วนของการ Update หรือ Service Pack หรือ Patch หรือ Hot Fix เวอร์ชั่นล่าสุดและนำมาติดตั้งเพื่อใช้งาน

๑๑.๕ ภายหลังที่มีการติดตั้ง Web Server จะต้องดำเนินการให้มีการเก็บบันทึกการเรียกใช้งานของ Web Server (Log) ทั้งในส่วนที่พบข้อผิดพลาดและส่วนของการเรียกใช้งานทั่วไป

๑๑.๖ ทดสอบการใช้งานของ Web Server โดยสำรองข้อมูลก่อนดำเนินการนำไปใช้งาน

๑๑.๗ คอมพิวเตอร์แม่ข่ายที่ให้บริการเว็บหลักขององค์การต้องติดตั้งอยู่ภายในห้องคอมพิวเตอร์ขององค์การเท่านั้น

๑๒. แนวปฏิบัติการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

สำนักเทคโนโลยีสารสนเทศได้กำหนดมาตรการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ขององค์การ ในขณะที่ไม่มีผู้ดูแล ดังต่อไปนี้

๑๒.๑ ผู้ใช้งานต้องออกจาก (Log out) ระบบสารสนเทศโดยทันทีเมื่อเสร็จสิ้นการใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานๆ

๑๒.๒ ป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบสารสนเทศของตน

๑๒.๓ สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกันการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

๑๒.๔ เมื่อผู้ใช้งานระบบสารสนเทศทิ้งไว้โดยไม่ใช้งานต่อเนื่องเป็นเวลานานเกิน ๒๕ นาที ระบบจะยุติการใช้งานระบบ หรือตามความเหมาะสมขึ้นอยู่กับระบบสารสนเทศนั้นๆ

๑๓. แนวปฏิบัติการลงทะเบียนผู้ใช้งาน

ผู้ดูแลระบบ (System Administrator) ต้องจัดทำขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานในการเข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว ดังต่อไปนี้

๑๓.๑ ทำการลงทะเบียนผู้ใช้งาน สำหรับระบบสารสนเทศขององค์การ ตามเอกสารหรือจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ได้รับแจ้งเป็นลายลักษณ์อักษรจากหน่วยงานต้นสังกัดนั้นๆ

๑๓.๒ ตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๑๓.๓ ตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามข้อกำหนดของหน่วยงานต้นสังกัด

๑๓.๔ แสดงเอกสารเป็นบันทึกหรือจดหมายอิเล็กทรอนิกส์ (e-mail) แจ้งให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศ

๑๓.๕ กำหนดให้มีการถอดถอนสิทธิ์การเข้าถึงระบบสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๑๓.๖ การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่รับอนุญาต

๑๔. แนวปฏิบัติการจัดการด้านวินัยเมื่อมีการละเมิดหรือละเลยต่อหน้าที่

๑๔.๑ กำหนดบทลงโทษเมื่อมีการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัย

๑๔.๒ กำหนดกระบวนการเกี่ยวกับการลงโทษต่อผู้ที่ฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัย

๑๔.๓ กำหนดขั้นตอนการปฏิบัติเกี่ยวกับการลงโทษต่อผู้ที่ฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยดังนี้

- การว่ากล่าวตักเตือน
- การตักเตือนอย่างเป็นทางการ
- การระบุโทษและพิจารณาลงโทษ
- การลงโทษ

๑๕. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy)

๑๕.๑ ผู้ดูแลระบบสารสนเทศจัดทำบัญชีสินทรัพย์สารสนเทศ โดยระบุผู้รับผิดชอบในสินทรัพย์สารสนเทศองค์การ อย่างชัดเจน

๑๕.๒ กรณีผู้ใช้งานมีการใช้งานสินทรัพย์สารสนเทศ ต้องมีการลงบันทึกการใช้งานที่ผู้ดูแลระบบจัดทำขึ้น เพื่อป้องกันการสูญหายของสินทรัพย์สารสนเทศขององค์การ

๑๕.๓ ผู้ใช้งานต้องไม่ละทิ้ง หรือปล่อยปละละเลยให้สินทรัพย์สารสนเทศที่มีความสำคัญ ข้อมูล, สื่อบันทึกข้อมูล อยู่ในภาวะหรือสถานที่ที่ไม่ปลอดภัย หรืออยู่ในสถานที่สาธารณะในสภาพที่พบเห็นได้โดยง่าย

๑๕.๔ ผู้ใช้งานต้องเก็บรักษาสินทรัพย์ที่ตนใช้งานในที่ที่กำหนดไว้หลังจากการใช้งานเสร็จเรียบร้อยแล้ว หากเป็นการใช้งานระบบสารสนเทศต้องทำการออกจากระบบทุกครั้ง

๑๕.๕ ในกรณีที่สินทรัพย์อยู่ในรูปแบบสื่ออิเล็กทรอนิกส์และสินทรัพย์สารสนเทศนั้นมีการกำหนดชั้นความลับไว้ และหากมีการส่งสินทรัพย์สารสนเทศผ่านเน็ตเวิร์คระบบอีเมลล์จำต้องเปิดระบบหรือฟังชั่นห้ามการส่งต่ออีเมลล์นั้น

๑๕.๖ การทำลายสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ของหน่วยงานองค์การ

(๑) ผู้ดูแลระบบหรือเจ้าของข้อมูลอิเล็กทรอนิกส์ต้องเป็นผู้ทำลายข้อมูลอิเล็กทรอนิกส์นั้น

(๒) ลักษณะการทำลายสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

ชนิดสื่อข้อมูล	CD/DVD /RW	Thumb Drive	Tape Library	Hard Drisk
ลักษณะการทำลายสื่อบันทึกนั้นก่อนนำมาใช้ใหม่	Delete/Format	Format	Delete/RW	Format
การดำเนินการทำลายสื่อ	ทำลายก่อนนำมาใช้	ทำลายก่อนนำมาใช้	ทำลายก่อนนำมาใช้	ทำลายก่อนนำมาใช้
การทำลายสื่อบันทึกที่ไม่ให้นำกลับมาใช้ได้อีก	เผา/ทุบ/เครื่องย่อยทำลาย	เผา/ทุบ/เครื่องย่อยทำลาย	เผา/ทุบ/เครื่องย่อยทำลาย	เผา/ทุบ/เครื่องย่อยทำลาย
ระยะเวลาที่กำหนดการทำลายสื่อบันทึก	เก็บไว้ ๑ ปี ก่อนทำลาย	เก็บไว้ ๑ ปี ก่อนทำลาย	เก็บไว้ ๑ ปี ก่อนทำลาย	เก็บไว้ ๑ ปี ก่อนทำลาย

๑๖. แนวปฏิบัติการบริหารจัดการสิทธิใช้งานระบบและการแบ่งแยกเครือข่าย

๑๖.๑ แบ่งแยกและควบคุมเครือข่ายด้วยอุปกรณ์ไฟร์วอลล์ (Firewall) และทำงานร่วมกันกับอุปกรณ์เครือข่ายสวิทช์ ซึ่งสามารถกำหนด VLAN ได้

๑๖.๒ การจัดแบ่งเครือข่ายผู้ใช้งานภายในให้ทำการจัดแบ่งตามภารกิจ และหน้าที่ โดยจำกัดการเข้าถึงข้ามส่วนงาน หรือกลุ่มงาน เพื่อป้องกันข้อมูลรั่วไหล หรือการโจมตีในเครือข่าย

๑๖.๓ การแบ่งแยกบนเครือข่ายหลักต้องมีพื้นที่หรือกลุ่มต่างๆ อย่างน้อยดังนี้

๑๖.๓.๑ กลุ่มผู้ใช้งาน (Intranet)

๑๖.๓.๒ กลุ่มเครือข่ายไร้สาย (Wireless)

๑๖.๓.๓ กลุ่มเจ้าหน้าที่ภายนอก (Out Source)

๑๖.๓.๔ กลุ่มเจ้าหน้าที่ดูแลระบบ (Administrator)

๑๖.๓.๕ กลุ่มเครื่องคอมพิวเตอร์แม่ข่ายให้บริการสาธารณะ (Public Server)

๑๖.๓.๖ กลุ่มเครื่องคอมพิวเตอร์แม่ข่ายและโปรแกรมประยุกต์ (Application Server)

๑๖.๓.๗ กลุ่มเครื่องคอมพิวเตอร์แม่ข่ายให้บริการเฉพาะภายในสำนักงานใหญ่เท่านั้น (Internal Server) กลุ่มผู้ใช้งาน (Intranet) มีสิทธิ์ในการเข้าใช้งานบนระบบเครือข่ายดังนี้

(๑) สามารถใช้งาน Internet ที่เป็นประโยชน์ต่อองค์การเท่านั้น

(๒) สามารถเข้าใช้งานบนระบบสารสนเทศภายในได้โดยไม่มีการจำกัดเวลา

(๓) สามารถใช้งาน Internet ได้ต่อเมื่อมีการ login โดยใช้ไอดีเท่านั้น

(๔) กลุ่มเครือข่ายไร้สาย (Wireless) มีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้ (ให้ถือปฏิบัติตามที่องค์การกำหนด)

(๕) สามารถใช้งาน Internet ที่เป็นประโยชน์ต่อองค์การเท่านั้น

(๖) สามารถใช้งาน Internet ได้ต่อเมื่อมีการ login โดยใช้ไอดีเข้าเท่านั้น

๑๖.๓.๘ กลุ่มเจ้าหน้าที่ภายนอก (Out Source) กำหนดให้เป็นกลุ่มของผู้รับจ้างดูแลระบบเครือข่ายขององค์การขนส่งมวลชนกรุงเทพ โดยมีสิทธิ์ในการเข้าใช้งานบนระบบเครือข่ายดังนี้

ไม่สามารถเชื่อมต่อไปยังภายนอกกลุ่มของตนเอง เว้นแต่มีการขออนุญาตเป็นกรณีพิเศษ ซึ่งจะต้องได้รับความเห็นชอบจากสำนักเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๑๖.๓.๙ กลุ่มเจ้าหน้าที่ดูแลระบบ (Administrator) มีสิทธิ์ในการเข้าใช้งานบนระบบเครือข่ายดังนี้

(๑) สามารถเชื่อมต่อเข้าไปยังระบบเครือข่ายขององค์การได้ทุกที่และตลอดเวลา

(๒) กลุ่มเครื่องคอมพิวเตอร์แม่ข่าย (Server) โดยให้มีการกำหนดระดับความสำคัญ และความต้องการเพื่อจำแนกเครื่องแม่ข่ายไปยังตำแหน่งที่เหมาะสม ไม่ว่าจะเป็นกลุ่มของเครื่องแม่ข่ายที่ให้บริการสาธารณะ ระบบโปรแกรมประยุกต์ และเครื่องแม่ข่ายที่ให้บริการเฉพาะภายในเท่านั้น

๑๖.๔ สามารถเชื่อมต่อจากกลุ่มต่างๆ ขององค์การที่ได้กำหนดไว้ เพื่อเข้ามาใช้บริการบนเครื่องคอมพิวเตอร์แม่ข่าย ดังนี้

๑๖.๔.๑ เครื่องคอมพิวเตอร์ภายนอกเครือข่ายจะต้องไม่สามารถติดต่อเข้ามายังเครื่องแม่ข่ายที่อยู่ในกลุ่มเพื่อให้บริการภายในเท่านั้น

๑๖.๔.๒ เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถเรียกออกไปยัง Internet ได้เว้นแต่มีเหตุจำเป็นที่จะต้องเชื่อมต่อ เช่น การใช้งาน DNS ของเครื่องคอมพิวเตอร์แม่ข่ายการปรับปรุงเรื่อง Virus เป็นต้น

๑๖.๕ สำนักเทคโนโลยีสารสนเทศสามารถทักท้วง หรือไม่อนุญาตให้มีการใช้งานของเครื่องคอมพิวเตอร์ลูกข่าย หรือเครื่องคอมพิวเตอร์แม่ข่ายได้ หากพบว่าความผิดปกติที่อาจก่อให้เกิดความเสียหาย หรือมีความไม่เหมาะสมต่อระบบเครือข่าย ขององค์การได้

๑๖.๖ สำนักเทคโนโลยีสารสนเทศต้องปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ในฐานะผู้ให้บริการการเข้าถึงเครือข่ายอินเทอร์เน็ต

๑๗. การใช้งานระบบเครือข่ายองค์การ

๑๗.๑ ผู้ใช้งานระบบสารสนเทศต้องได้รับอนุญาตจากผู้ดูแลระบบเครือข่ายขององค์การ หรือได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศ ซึ่งสามารถเข้าใช้งานระบบสารสนเทศได้เพียงระบบที่ได้รับอนุญาตเท่านั้น

๑๗.๒ ผู้ดูแลระบบเครือข่ายและสำนักเทคโนโลยีสารสนเทศ มีหน้าที่ตรวจสอบการขออนุมัติและกำหนดหลักเกณฑ์การขออนุญาตในการเข้าสู่ระบบเครือข่ายสารสนเทศขององค์การ ตามสิทธิ์และการปฏิบัติงานในหน้าที่ เท่านั้น

๑๗.๓ ผู้ดูแลระบบเครือข่าย หรือสำนักเทคโนโลยีสารสนเทศต้องจัดให้มีระบบการบันทึกการเข้าใช้งานระบบสารสนเทศองค์การ รวมถึงการเฝ้าระวังการใช้งานระบบต่างๆ ไม่ให้ผู้ใช้งานระบบล่วงละเมิดความปลอดภัยและสิทธิ์การในการใช้งานของผู้ใช้งานอื่นๆ

๑๗.๔ สำหรับการใช้งารระบบอินเตอร์เน็ต (Internet) ผู้ใช้งานจำต้องทำการพิสูจน์ตัวตนในระบบด้วยการใส่ Username และ Password ตามที่ได้รับจากผู้ดูแลระบบ ทุกครั้ง และการใช้งานอินเตอร์เน็ตจะถูกระบบทำการบันทึกการใช้งานไว้ Log file เป็นระยะเวลา ๙๐ วัน ตามข้อกำหนดองค์การ

๑๘. การพิสูจน์ตัวตนผู้ใช้งานระบบจากภายนอกองค์การ

๑๘.๑ การตรวจสอบตัวตนผู้ใช้งานระบบ (Identification) ด้วยชื่อผู้ใช้งานระบบ (Username)

๑๘.๒ การตรวจพิสูจน์ตัวตนของผู้ใช้งานระบบ (Authentication) ด้วยรหัสผ่าน (Password)

๑๘.๓ การเข้าสู่ระบบสารสนเทศขององค์การจากภายนอกด้วยระบบอินเทอร์เน็ต จะมีการตรวจสอบโดยระบบจากหน้าเว็ปไซต์ทุกครั้ง

๑๘.๔ การเข้าใช้งารระบบสารสนเทศองค์การจากระยะไกล โดยมีการป้องกันเพื่อความปลอดภัย จะต้องมีการตรวจพิสูจน์ตัวตนของผู้ใช้งานระบบและผู้ใช้งานระบบโปรโตคอลสำหรับที่มีการเข้ารหัสข้อมูลตามมาตรฐานองค์การเช่น SSL VPN

๑๙. แนวทางการปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๙.๑ จัดฝึกอบรมแนวการปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมและส่งเสริมทางด้านเทคนิคใหม่ๆ สนับสนุนการปฏิบัติตามแนวนโยบายให้สอดคล้องกับหลักสูตรการอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน (เอกสารแนบ ๓)

๑๙.๒ จัดสัมนาเชิงปฏิบัติการเพื่อเผยแพร่แนวนโยบายและแนวทางปฏิบัติให้กับบุคลากร โดยการจัดสัมนาอย่างน้อยปีละ ๑ ครั้งหรือมากกว่า โดยร่วมกับส่วนราชการอื่นหรือหน่วยงานเอกชน และรวมถึงการเชิญวิทยากรที่มีความรู้มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้แก่บุคลากรของหน่วยงาน

๑๙.๓ ติดประกาศเพื่อการประชาสัมพันธ์ ให้เผยแพร่ความรู้เกี่ยวกับแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย ในลักษณะเกร็ดความรู้ ข้อควรระวังในรูปแบบที่สามารถเข้าใจได้ง่าย และสามารถนำไปปฏิบัติได้จริง โดยมีการปรับเปลี่ยนการนำเสนอเกร็ดความรู้ใหม่ๆ อย่างต่อเนื่องและสม่ำเสมอ

๑๙.๔ ระดมความคิดเพื่อการมีส่วนร่วมของพนักงานภายในหน่วยงาน และการนำแนวคิดที่ดีเพื่อสู่การปฏิบัติได้เป็นอย่างรูปธรรม และส่งผลต่อการกำกับ ควบคุม ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

ส่วนที่ ๔
การปฏิบัติของผู้ดูแลระบบ

๑. วัตถุประสงค์

เพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ดูแลระบบ (System Administrator) ในการบริหารจัดการกำกับดูแลเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย (Network) ให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งการสอดส่องดูแลผู้ใช้งานให้เป็นไปตามแนวนโยบาย

๒. ผู้รับผิดชอบ

๒.๑ สำนักเทคโนโลยีสารสนเทศ

๒.๒ ผู้ดูแลระบบสารสนเทศและ Out Source

๓. แนวปฏิบัติกำหนดให้ผู้ดูแลระบบ (System Administrator) ปฏิบัติดังนี้

๓.๑ ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายขององค์การขนส่งมวลชนกรุงเทพให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข ป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้น พร้อมทั้งรายงานต่อผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) หรือผู้ที่ได้รับมอบหมาย ทราบในทันที

๓.๒ กรณีเกิดสิ่งผิดปกติขึ้นจากการใช้งานของผู้ใช้ที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่อาจจะเกิดขึ้นแก่

องค์การขนส่งมวลชนกรุงเทพให้ผู้ดูแลระบบพิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

๓.๓ ดำเนินการติดตั้ง ตรวจสอบและปรับปรุงโปรแกรมคอมพิวเตอร์ระบบสารสนเทศและระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและถูกต้อง ทันสมัยอยู่เสมอ

๓.๔ ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที รวมถึงดูแลรักษาและปรับปรุงบัญชีผู้ใช้งาน (Account) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์การใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

๓.๕ ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้บริการให้มีการกำหนดรหัสผ่าน (Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password) และไม่ใช้อำนาจหน้าที่ของผู้ดูแลระบบ (System Administrator) ในการเข้าถึงข้อมูลของผู้ใช้ที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร และไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร รวมถึงไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

๓.๖ เมื่อผู้ดูแลระบบ (System Administrator) พ้นจากหน้าที่จะต้องคืนสินทรัพย์ของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และนำรหัสให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายดำเนินการตรวจสอบ

๓.๗ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องใช้วิธีการที่มั่นคงปลอดภัย โดยเก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ (System Administrator) สามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ ซึ่งในการเก็บข้อมูลจราจรนั้นต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

๔. กำหนดให้ผู้ดูแลระบบงานวางแผนและพัฒนาระบบเทคโนโลยีสารสนเทศ ปฏิบัติดังนี้

๔.๑ กำหนดเป็นมาตรการการเข้าถึงระบบงานของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบงาน โดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ์ในการเข้าถึงระบบงาน เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบขององค์การได้

๔.๒ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบงานขององค์การ

๔.๓ ผู้ดูแลระบบงานต้องตรวจสอบบัญชีผู้ใช้งาน ที่ไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๔.๔ ผู้ดูแลระบบงานต้องตรวจสอบและให้สิทธิ์การเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๔.๕ ผู้ดูแลระบบงานต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบงาน รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๔.๖ ผู้ดูแลระบบงานต้องกำหนดให้มีการถอดถอนสิทธิ์การเข้าถึงระบบงานโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๔.๗ การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบงานต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

๔.๘ ผู้ดูแลระบบงานต้องกำหนดสิทธิ์การใช้ระบบงาน โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๔.๙ ผู้ดูแลระบบต้องกำหนดระดับสิทธิ์ในการเข้าถึงที่เหมาะสมสำหรับระบบงาน

๔.๑๐ ผู้ดูแลระบบงานต้องมอบหมายสิทธิ์ให้มีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

๔.๑๑ ผู้ดูแลระบบงานต้องจัดเก็บเอกสารการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน นโยบายการรักษาความมั่นคงปลอดภัยของระบบงานขององค์การ

๔.๑๒ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ ได้รับว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๔.๑๓ ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

๔.๑๔ ระบบบริหารจัดการรหัสผ่านต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเองและมีขั้นตอนปฏิบัติ เพื่อยืนยันรหัสผ่านใหม่

๔.๑๕ ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเลือกรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

๔.๑๖ ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุกๆ ๖ เดือน

๔.๑๗ ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชีผู้ใช้งานและทำการล็อกอินเข้าใช้งานระบบงานเป็นครั้งแรก

๔.๑๘ ระบบบริหารจัดการรหัสผ่านต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน เช่น ให้แสดงเป็นเครื่องหมายดอกจัน (*) บนหน้าจอ เป็นต้น

๔.๑๙ ระบบบริหารจัดการรหัสผ่านต้องป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้ หรือที่จำเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๔.๒๐ ผู้ดูแลระบบงานต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๔.๒๑ ผู้ดูแลระบบงานต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

๔.๒๒ ผู้ดูแลระบบงานต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและควรกำหนดรหัสผ่านที่แตกต่างกัน

๔.๒๓ ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่งและกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

๔.๒๔ ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ๑ ครั้ง / ปี เป็นอย่างน้อย

๔.๒๕ ผู้ดูแลระบบงานทบทวนสิทธิ์สำหรับผู้ที่มีสิทธิ์ในระดับสูง เช่น สิทธิ์ในระดับผู้ดูแลระบบงานด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๔.๒๖ ผู้ดูแลระบบงานทบทวนสิทธิ์ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

๔.๒๗ ผู้ดูแลระบบงานต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิ์ในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

๕. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๕.๑ ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนโดยลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศขององค์การ

๕.๒ การมอบบัญชีผู้ใช้งานให้กับผู้ใช้งานครั้งแรก ให้กำหนดรหัสผ่านชั่วคราวจากการสุ่มให้กับผู้ใช้งานเมื่อผู้ใช้งานได้รับรหัสผ่านแล้ว ให้เปลี่ยนรหัสผ่านนั้นเป็นรหัสผ่านของตนเองที่เป็นไปตามแนวปฏิบัติการใช้งานรหัสผ่านมาตรฐานความปลอดภัย

๕.๓ การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัยโดยให้ใช้วิธีการใส่ซองปิดผนึกหรือกระดาษสลิปคาร์บอนด์ จากนั้นส่งมอบให้ผู้กับใช้งานระบบโดยตรง

๕.๔ ผู้ใช้งานต้องตอบรับการยืนยันการได้รับรหัสผ่าน ผ่านระบบอีเมลล์

๕.๕ กรณีที่ผู้ใช้ระบบสารสนเทศลาออก หรือไม่มีหน้าที่ความรับผิดชอบเกี่ยวกับระบบสารสนเทศที่ขอสิทธิ์ในการใช้งาน ให้หัวหน้าหน่วยงานแจ้ง สำนักเทคโนโลยีสารสนเทศทันที เพื่อเปลี่ยนสิทธิ์หรือถอนออกจากระบบผู้ใช้งานระบบสารสนเทศ ทันที

๕.๖ ผู้ดูแลระบบสารสนเทศ จัดระบบที่สนองความต้องการของผู้ใช้ระบบให้สามารถเปลี่ยนรหัสผ่านของตนเองได้โดยเปลี่ยนรหัสผ่านทุกๆ ๖ เดือน

๕.๗ ผู้ดูแลระบบสารสนเทศ สามารถกำหนดความเหมาะสมจำนวนครั้งที่ยอมให้ User ผู้ใช้งานใส่รหัสผิดพลาดได้ไม่เกิน ๔ ครั้ง ในการเข้าใช้งานระบบสารสนเทศ

๖. ผู้ดูแลระบบต้องทำหน้าที่เก็บข้อมูลจราจรดังนี้

ผู้ดูแลระบบ (System Administrator) ทำหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้บริการและเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วันนับตั้งแต่การใช้บริการสิ้นสุดลงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ใช้วิธีการที่มั่นคงปลอดภัยดังต่อไปนี้

๖.๑ เก็บในสื่อบันทึกข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อบันทึกดังกล่าวได้

๖.๒ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ (System Administrator) สามารถแก้ไขข้อมูลที่เก็บรักษาไว้เว้นแต่ ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์การ (Internal IT Auditor) หรือบุคคลที่ได้รับมอบหมาย

๖.๓ ในการเก็บข้อมูลจราจรนั้น สามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

๖.๔ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริง ผู้ดูแลระบบได้ตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum ๐) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

หมวดที่ ๒ ระบบสารสนเทศและระบบสำรองของสารสนเทศ

ส่วนที่ ๕
การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

๑. บทนำ

เพื่อกำหนดเป็นมาตรการในการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายหลัก (Server) ณ อาคาร ขสมก. ชั้น ๔ และเครื่องคอมพิวเตอร์แม่ข่ายสำรองที่ อาคารกลุ่มงานสื่อสาร ชั้น ๑ เป็นอุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมในกรณีเกิดเหตุฉุกเฉินหรือไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ หรือมีผลกระทบด้วยประการใดๆ ทำให้เครื่องคอมพิวเตอร์แม่ข่ายหลักไม่สามารถใช้การได้ และให้สามารถใช้งานเครื่องคอมพิวเตอร์แม่ข่ายสำรองได้ทันท่วงที รวมถึงการกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติอย่างต่อเนื่อง เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจขององค์การขนส่งมวลชนกรุงเทพ

๒. วัตถุประสงค์

๒.๑ เพื่อให้เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ ใช้เป็นแนวทางการปฏิบัติงาน เมื่อต้องเผชิญเหตุการณ์ ที่ส่งผลกระทบต่อระบบ และให้การสนับสนุนการบริการจัดการเดินรถโดยสารเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพตามระเบียบปฏิบัติ

๒.๒ เพื่อเตรียมความพร้อมรองรับกับสถานการณ์ฉุเฉิน กรณีไฟฟ้าดับ หรือการเกิดภัยพิบัติต่างๆ สามารถทำให้ระบบต่างๆ ดำเนินการได้อย่างต่อเนื่องตามมาตรฐาน

๓. ผู้รับผิดชอบ

๓.๑ ผู้รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่ายหลัก (Server HO) อาคาร ขสมก. สำนักงานใหญ่

๓.๑.๑ สำนักเทคโนโลยีสารสนเทศ

(๑) นายยงยุทธ พันธ์สวัสดิ์ ห.กปค. (ระดับ ๖)
(๒) นายประวัติ สุขพันธ์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔
(๓) นายสมยศ อินทรศิลป์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔
(๔) นายชานนทร์ แก้วพรายตา เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔

๓.๑.๒ Out Source บริษัท สตรีม ไอ.ที.คอนซัลติ้ง จำกัด

๓.๒ ผู้รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่ายสำรอง (Server Clicent) อาคาร ขดร.๘ สวนสยาม

๓.๒.๑ สำนักเทคโนโลยีสารสนเทศ

(๑) นายประวัติ สุขพันธ์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔
(๒) นายวราราช ชื่อดี เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔
(๓) นายปิยะสิทธิ์ พูลสุข เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔

๓.๒.๒ Out Source บริษัท สตรีม ไอ.ที.คอนซัลติ้ง จำกัด

๔. แนวปฏิบัติแผนการเตรียมความพร้อมภัยพิบัติการปฏิบัติ ดังนี้

๔.๑ การปฏิบัติการตามแผน

๔.๑.๑ การเตรียมความพร้อมรองรับสถานการณ์

(๑) ดำเนินการเตรียมพร้อมของระบบคอมพิวเตอร์แม่ข่ายหลัก (Server HO) ที่อาคาร ขสมก. สำนักงานใหญ่ ชั้น ๔ โดยการเชื่อมต่อระบบเครือข่าย MPLS (Fiber Obtic)วงจร ๔๕๑๕ ของบริษัท อินเตอร์ลิ้ง เทเลคอม จำกัด สำหรับ Run ห้องคอมพิวเตอร์แม่ข่ายสำหรับเก็บข้อมูลสำรอง (DR Server) เขตการเดินรถที่ ๘

(๒) ผู้รับผิดชอบสำนักเทคโนโลยีสารสนเทศ

(๒.๑) นายยงยุทธ พันธ์สวัสดิ์ ห.กปค. (ระดับ ๖)

(๒.๒) นายประวัติ สุขพันธ์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔

(๒.๓) นายชานนทร์ แก้วพรายตา เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔

(๒.๔) นายสมยศ อินทรศิลป์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔

(๒.๕) Out Source บริษัท สตรีม ไอ.ที.คอนซัลติ้ง จำกัด

(๓) รวบรวมและจัดเก็บสำรองข้อมูลระบบที่มีความสำคัญและมีการอัพเดสข้อมูล (Server) เพื่อการติดตั้ง และป้องกันการเสียหายของข้อมูลระบบ รวมถึงสามารถ Recovery ข้อมูลระบบได้ถูกต้อง

๔.๑.๒ จัดทำแผนรองรับสถานการณ์ไฟฟ้าดับ

(๑) เครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณ ๑๕ นาที

(๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(๓) กรณีเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและทำการปิดเครื่องคอมพิวเตอร์แม่ข่ายหลัก (Server HO) และอุปกรณ์ต่างๆ ทันที

(๔) ประสานงานไปยังระบบคอมพิวเตอร์แม่ข่ายสำรอง (Server Client) ด้วยวิทยุสื่อสาร เพื่อการ Run ระบบ (Server Client) เต็มระบบเพื่อการ ใช้งานได้ตามปกติ

(๕) ผู้รับผิดชอบสำนักเทคโนโลยีสารสนเทศ

(๕.๑) นายยงยุทธ พันธ์สวัสดิ์ ห.กปค. (ระดับ ๖)

(๕.๒) นายวราราช ชื่อดี เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔

(๕.๓) นายชานนทร์ แก้วพรายตา เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔

(๕.๔) นายปิยะสิทธิ์ พูลสุข เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ระดับ ๔

(๕.๕) Out Source บริษัท สตรีม ไอ.ที.คอนซัลติ้ง จำกัด

ให้มีการ Backup ข้อมูลโดยระบบอัตโนมัติเก็บไว้ทุกวันในเวลา ๒๓.๐๐ น.

๔.๒ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๔.๒.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้

๔.๒.๒ ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบเครือข่ายเพื่อการควบคุมเพลิงในเบื้องต้น

๔.๒.๓ ให้มีการสำรองฐานข้อมูลทั้งหมดเดือนละ ๑ ครั้งเป็นอย่างน้อย

๔.๓ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุอุทกภัย/น้ำรั่ว

เพื่อเป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์อุทกภัย /น้ำรั่ว ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๔.๓.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากอุทกภัย/น้ำรั่ว

๔.๓.๒ มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องควบคุมระบบเครือข่าย เพื่อให้ปลอดภัยต่อการรั่วซึมของน้ำอย่างสม่ำเสมอ

๔.๓.๓ ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๔.๔ การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัส

๔.๔.๑ ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากบุคคลภายนอก

๔.๔.๒ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ขาย (Server) และเครื่องลูกข่าย (Client)

๔.๔.๓ อัพเดตโปรแกรมกำจัดไวรัส ทุก ๑ เดือน เป็นอย่างน้อย (Update Patch)

๔.๔.๔ ให้เจ้าหน้าที่งานปฏิบัติการคอมพิวเตอร์แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่อง สม่ำเสมอรวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น

๕. การเตรียมความพร้อมรับภัยจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๕.๑ กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

๕.๒ หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องควบคุมระบบเครือข่าย จะต้องให้เจ้าหน้าที่ของงานปฏิบัติการคอมพิวเตอร์ผู้ดูแลระบบเครือข่าย เป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออก และคอยกำกับดูแลตลอดการปฏิบัติงานเพื่อป้องกันการโจรกรรม

๕.๓ มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

๕.๔ มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๕.๕ มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตขององค์การเพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕.๖ มีการป้อนชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิ์ก่อนเข้าใช้อินเทอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๖. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติดังนี้

๖.๑ กรณีเครื่องลูกข่าย (Client)

๖.๑.๑ ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศ ของหน่วยงานทราบ หรือในกรณีเกิดจากงานปฏิบัติการคอมพิวเตอร์และงานบริการระบบคอมพิวเตอร์และเครือข่าย ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ หัวหน้ากลุ่มงานปฏิบัติการคอมพิวเตอร์และเครือข่ายต้องประกาศให้ทุกหน่วยงานในองค์การทราบ

๖.๑.๒ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๖.๑.๓ ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถ แก้ไขปัญหาได้แจ้งเหตุขัดข้องให้สำนักเทคโนโลยีสารเทศเพื่อแก้ไขปัญหาต่อไป

๖.๒ กรณีเครื่องแม่ข่ายบริการ (Server)

๖.๒.๑ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการใช้งาน

๖.๒.๒ ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๖.๒.๓ ตัดระบบจ่ายกระแสไฟฟ้า ในกรณีเกิดเหตุเพลิงไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๖.๒.๔ ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

๖.๒.๕ กรณีเพลิงไหม้ให้ใช้น้ำยาดับเพลิง ฉีดควบคุมเพลิงโดยเร็ว

๖.๒.๖ รีบขนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ไปไว้ในที่ปลอดภัย

๖.๒.๗ ประสานขอความช่วยเหลือกับเจ้าหน้าที่บริษัทที่รับผิดชอบด้านการให้บริการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๖.๒.๘ ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำ อุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๖.๒.๙ ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทราบโดยเร็ว

ส่วนที่ ๖
แผนเตรียมความพร้อมกรณีฉุกเฉิน

๑. วัตถุประสงค์

๑.๑ เพื่อป้องกันการสูญเสียข้อมูลสำคัญและทรัพย์สินรวมทั้งลดผลกระทบจากการเกิดสถานการณ์ฉุกเฉิน เช่น ไฟฟ้าดับ น้ำท่วม เป็นต้น

๑.๒ เพื่อพัฒนาระบบบริหารจัดการด้านระบบไฟฟ้าของสำนักเทคโนโลยีสารสนเทศ และแผนการสำรองข้อมูลให้มีประสิทธิภาพสามารถลดอัตราความเสี่ยงต่อการเกิดเหตุ

๑.๓ เพื่อให้เจ้าหน้าที่และบุคลากรเกิดความตระหนักและมีความพร้อมสามารถระงับเหตุรวมทั้งช่วยเหลือตนเองได้อย่างปลอดภัยเมื่อเกิดเหตุ

๒. แนวการปฏิบัติ

๒.๑ การปฏิบัติก่อนเกิดเหตุ ประกอบด้วย แผนป้องกันสถานการณ์ฉุกเฉินกรณีไฟฟ้าดับและแผนสำรองระบบสารสนเทศ คือ ๑) แผนการตรวจตราศูนย์ข้อมูลหลักและศูนย์สำรองสารสนเทศ ๒) แผนการอบรม และ ๓) แผนฝึกซ้อมการป้องกันและเผชิญเหตุ

๒.๒ การปฏิบัติเมื่อเกิดเหตุ ประกอบด้วย ๑) แผนการแก้ไขสถานการณ์และการสวิทซ์ข้อมูล

๒.๓ การปฏิบัติภายหลังเหตุประกอบด้วย ๑) แผนการฟื้นฟูเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์และกู้คืนข้อมูล

๓. รายละเอียดการปฏิบัติ

๓.๑ การปฏิบัติก่อนเกิดเหตุ ประกอบด้วย

๓.๑.๑ แผนการตรวจตราศูนย์ข้อมูลหลักและศูนย์สำรองสารสนเทศและวิเคราะห์สถานการณ์

เพื่อเป็นแผนการเฝ้าระวังป้องกันและสำรวจตรวจตราระบบความปลอดภัยและความเรียบร้อยของอาคาร สำนักงาน วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ เพื่อเตรียมรับมือกับสถานการณ์ โดยดำเนินการดังนี้

(๑) จัดให้มีคณะเจ้าหน้าที่ปฏิบัติหน้าที่เวรฯ ของศูนย์ข้อมูลหลัก (ห้องแม่ข่ายคอมพิวเตอร์ อาคาร ขสมก. ชั้น ๔)

(๒) สำรวจตรวจตราระบบไฟฟ้าของอาคารให้เป็นไปตามที่กฎหมายกำหนดและจัดหาแหล่งสำรองระบบสารสนเทศ กรณีศูนย์หลักมีปัญหา

(๓) แจ้งเส้นทางอพยพขนย้ายทรัพย์สิน การจัดลำดับความสำคัญของทรัพย์สินและแนวทางการสำรองระบบสารสนเทศให้ทุกคนรับทราบ

(๔) จัดทำผังการติดต่อสื่อสาร หมายเลขโทรศัพท์ของฝ่ายบริหาร หน่วยงานผู้ให้บริการด้านระบบไฟฟ้า ผู้ดูแลอาคาร หรือห้องเวรรักษาความปลอดภัย

(๕) จัดทำสัญลักษณ์ของบัญชีทรัพย์สินตลอดจนเอกสารสำคัญที่สามารถขนย้ายได้เมื่อเกิดเหตุ โดยเรียงลำดับความสำคัญ เช่น กำหนดแถบสีแดง หมายถึง มีความสำคัญอันดับ ๑ ให้ขนย้ายก่อน แถบสีเขียว หมายถึง มีความสำคัญอันดับ ๒ ให้ขนย้ายลำดับต่อมา พร้อมแจ้งให้ทุกคนในหน่วยงานรับทราบและเข้าใจร่วมกัน

๓.๒ แผนการอบรม

เพื่อเป็นแผนการฝึกอบรมให้ความรู้เกี่ยวกับการป้องกันเผชิญเหตุ สำหรับเจ้าหน้าที่ในหน่วยงาน ดังนี้

๓.๒.๑ การฝึกอบรมให้ความรู้ เพื่อให้เจ้าหน้าที่ทุกคนมีความรู้ ความเข้าใจสามารถแก้ปัญหาเบื้องต้นได้ รวมถึงทราบตำแหน่งที่ตั้งเมนสวิทช์ (คัทเอาท์) จุดตัดกระแสไฟฟ้า (คัทเอาท์) ภายในหน่วยงานของตนหรือใกล้เคียง

๓.๒.๒ การฝึกซ้อม ฝึกปฏิบัติโดยการฝึกซ้อมการเผชิญเหตุรวมทั้งตรวจสอบศูนย์สารสนเทศสำรองว่ามีความพร้อมหรือไม่

๓.๓ แผนฝึกซ้อมป้องกันการเผชิญเหตุ

โดยเน้นความสำคัญของการป้องกันและเตรียมความพร้อมในการป้องกันการเกิดเหตุให้ทุกหน่วยงานดำเนินการดังนี้

๓.๓.๑ จัดทำแผนสำรองระบบไฟฟ้า กรณีเกิดกระแสไฟฟ้าของการไฟฟ้านครหลวงขัดข้องไม่สามารถจ่ายกระแสไฟฟ้ามายังห้องเครื่องคอมพิวเตอร์แม่ข่าย อาคาร ขสมก. ชั้น ๔ ได้ โดยมีการเตรียมความพร้อมระบบสำรองไฟฟ้า (UPS)

๓.๓.๒ จัดทำแผนสำรองระบบสารสนเทศ โดยมีมาตรการหลักๆ ดังนี้

(๑) การสำรองข้อมูลลงบนฮาร์ดดิสก์

(๒) การสำรองข้อมูลบนเทป ซึ่งจะมีการโปรแกรมการสำรองข้อมูลลงบนเทปในทุกวันเวลา ๑๙.๐๐ น. และจัดเก็บเทปไว้เป็นรายสัปดาห์ (ในกรณีเกิดสถานการณ์ฉุกเฉินสามารถขนย้ายเทปไปยังสถานที่ปลอดภัย)

๓.๓.๓ ดำเนินการทดสอบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง หากตรวจพบปัญหาในการระหว่างกู้คืนระบบ ให้ทำการบันทึกปัญหา และแนวทางขั้นตอนวิธีการแก้ไขเป็นลายลักษณ์อักษร

๓.๔ การปฏิบัติเมื่อเกิดเหตุ ประกอบด้วย

๓.๔.๑ แผนการแก้ไขสถานการณ์และการสวิทช์ข้อมูล

๓.๔.๑.๑ การแจ้งเหตุ

- กรณีเกิดเหตุในเวลาราชการ ให้รายงานเหตุไฟฟ้าขัดข้องกับผู้บังคับบัญชาหรือหัวหน้างาน และแจ้งการไฟฟ้านครหลวง
- กรณีเกิดเหตุนอกเวลาราชการ ให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบ ซึ่งได้มีการจัดเวรฯ การรับแจ้งเหตุของสำนักเทคโนโลยีสารสนเทศ

๓.๔.๑.๒ การแก้ไขสถานการณ์เบื้องต้น

- ระบบเครื่องสำรองไฟฟ้า (UPS) จ่ายกระแสไฟฟ้าให้เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ตลอดเวลา เมื่อเกิดเหตุการณ์ไฟฟ้าดับจากการไฟฟ้าขัดข้องไม่สามารถจ่ายกระแสไฟฟ้าได้
- เจ้าหน้าที่ผู้ดูแล จะต้องทำการ Shutdown เครื่อง Server แม่ข่ายก่อนเครื่องไฟฟ้าสำรองจะหมดกระแสไฟ

๓.๔.๒ การแก้ไขสถานการณ์ขั้นสูงสุด หากไฟฟ้าดับนานเกินต้องรายงานสถานการณ์ให้ผู้บังคับบัญชาทราบตามลำดับชั้นถึงระดับ ผอ.สทส. เพื่อสั่งการในการสวิทช์ระบบจากศูนย์ข้อมูลหลัก โดยกลุ่มงานฯ คอมพิวเตอร์ได้จัดเจ้าหน้าที่เวรฯ ในการดูแลศูนย์สารสนเทศสำรอง (Backup site) ตลอดเวลาพร้อมรับคำสั่งในการสวิทช์การทำงานไปยัง Backup site

๓.๕ การปฏิบัติภายหลังเกิดเหตุ แผนการฟื้นฟูเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์และกู้คืนข้อมูล

๓.๕.๑ เมื่อระบบไฟฟ้าสามารถใช้งานได้ตามปกติให้สำรวจความเสียของอุปกรณ์และข้อมูล เพราะในช่วงระหว่างไฟฟ้าดับอาจเกิดกระแสไฟฟ้าขัดข้องหรือไฟฟ้าไปเลี้ยงอุปกรณ์ต่างๆ ได้ไม่เต็มที่ อาจมีอุปกรณ์บางตัวดับไปโดยไม่ได้ Shut Down อาจส่งผลต่อระบบได้

๓.๕.๒ การกู้คืนข้อมูล ในกรณีที่มีการสวิทช์การทำงานไปยัง Backup Site เมื่อเหตุการณ์ปกติจะต้องมีการกู้คืนข้อมูลมายังระบบงานหลัก ต้องตรวจสอบระบบการทำงานและข้อมูลว่ามีความถูกต้องครบถ้วนหรือไม่

๔. การสำรองข้อมูลและการกู้คืนฐานข้อมูล

๔.๑ การคัดเลือกระบบสำรองและการกู้คืนระบบ

๔.๑.๑ พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำบัญชีของระบบที่มีความสำคัญและมีระบบสำรองข้อมูลระบบสภาพพร้อมใช้งาน

๔.๑.๒ จัดให้มีการสำรองข้อมูลระบบสารสนเทศแต่ละรบบ และกำหนดความถี่ในการสำรองและกรณีมีการเปลี่ยนแปลงบ่อยต้องกำหนดให้มีความถี่ในการสำรองเพิ่มขึ้นโดยมีวิธีการดังนี้

(๑) จัดลำดับความสำคัญของระบบงานที่มีความสำคัญต้องสำรองข้อมูลระบบ

(๒) กำหนดเจ้าหน้าที่ สำนักเทคโนโลยีสานสนเทศรับผิดชอบในการสำรองข้อมูล

(๓) กำหนดชนิดข้อมูลระบบที่มีความสำคัญจำเป็นต้องสำรองข้อมูลไว้ รวมทั้งข้อมูลในฐานข้อมูลระบบ เช่น การอัพเดสคอนฟิกกูเรชั่น และซอฟต์แวร์ระบบปฏิบัติการที่เกี่ยวข้อง

(๔) กำหนดระยะเวลาความถี่ในการสำรองข้อมูลระบบตามที่เหมาะสม

(๕) ดำเนินการสำรองข้อมูลระบบตามความถี่และตรวจสอบความถูกต้องครบถ้วน

(๖) ดำเนินการทดสอบระบบสำหรับการกู้คืนข้อมูลระบบ ไม่น้อยกว่าปีละ ๑ ครั้ง

๔.๒ สำรองข้อมูลฐานข้อมูล (Full Backup) โดยการทำการทุกวันศุกร์และสิ้นเดือน

๔.๒.๑ พนักงานเปิดโปรแกรม PL/SQL Developer ตรวจสอบว่ามีเครื่อง Client ใช้งานระบบฐานข้อมูลหรือไม่ ถ้าไม่มีผู้ใช้งานทำการ Login Database Server

๔.๒.๒ ตรวจสอบว่ามี User ใช้งาน Database Server อยู่หรือไม่ ถ้าไม่มีผู้ใช้ดำเนินการใส่เทปใน Tape Library พิมพ์คำสั่งการ Backup ข้อมูลบนระบบ UNIX รอกระบวนการ Backup เสร็จเรียบร้อยแล้วนำเทปเก็บข้อมูลมาระบุ วัน/เดือน/ปี และจำนวนข้อมูลไว้บนเทป นำไปเก็บในที่ปลอดภัย

๔.๒.๓ พนักงานตรวจสอบการเข้าใช้ระบบงานสารสนเทศว่าสามารถทำงานได้เป็นปกตหรือไม่ หากปกติทำการ Logout ออก ถ้าไม่สามรถใช้งานได้ปกติทำการ Restart Database Server ใหม่

๔.๒.๔ กำหนดการสำรองข้อมูลระบบ พร้อมทั้งสื่อที่ใช้ในการบันทึก รวมถึงรูปแบบการสำรองข้อมูลระบบ ๒ รูปแบบคือ สำรองข้อมูลเต็มระบบ และสำรองข้อมูลแบบเฉพาะส่วน

(๑) การสำรองข้อมูลระบบสารสนเทศ ตามความถี่ดังนี้

ระบบ	ข้อมูลที่จำเป็นต้องสำรองระบบ	ระยะความถี่การสำรองข้อมูลระบบ
E-mail	Delete log ในส่วน Mail box	เดือนละ ๒ ครั้ง
Web Server	ค่าคอนฟิกกุเรชั่นระบบ	ช่วงก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลอัพเดสที่เผยแพร่	๒ ครั้ง/สัปดาห์
Database Server	ค่าคอนฟิกกุเรชั่นระบบ	ช่วงก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลระบบประจำวัน	๑ ครั้ง/วัน (เวลา ๒๔.๐๐ น.)
Firewall	ค่าคอนฟิกกุเรชั่นระบบ	ช่วงก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลระบบ	๑ ครั้ง/เดือน
IP Mangement	ค่าคอนฟิกกุเรชั่นระบบ	ช่วงก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลระบบ	๑ ครั้ง/เดือน

๔.๓ ผู้ดูแลระบบสารสนเทศและระบบเครือข่ายดำเนินการสำรองข้อมูลระบบดังนี้

๔.๓.๑ พนักงานเตรียมเทปบันทึกข้อมูลที่เก็บไว้ชุดล่าสุดให้ Outsource ดำเนินการกู้ข้อมูล

๔.๓.๒ หลังกู้ข้อมูลแล้วให้หัวหน้างานพัฒนาระบบและ User ทำการตรวจสอบข้อมูลและการทำงานทุกระบบว่าสามารถใช้งานได้ปกติและต่อเนื่องหรือไม่

๔.๓.๓ ถ้าไม่ปกติให้ Outsource ดำเนินการแก้ไขจนกว่าจะใช้งานได้ปกติ เมื่อปกติแล้วพนักงานทำการ Logout ออก

๔.๓.๔ ดำเนินการสำรองข้อมูลระบบและทดสอบข้อมูลที่ได้สำรองไว้อย่างสม่ำเสมอ

๔.๓.๕ ดำเนินการบันทึกด้วย Tape Libraly ในการสำรองข้อมูล

๔.๓.๖ ดำเนินการจัดทำรายงานข้อผิดพลาด ที่เกิดจากการสำรองข้อมูลระบบ รวมถึงวิธีการแก้ไขปัญหา

๕. อัตรากำลังบุคลากร

๕.๑ เจ้าหน้าที่ของ สำนักเทคโนโลยีสารสนเทศ

๕.๑.๑ เจ้าหน้าที่ จำนวน ๒๙ อัตรา

๕.๒ เจ้าหน้าที่ภายนอกหน่วยงาน ได้แก่

๕.๒.๑ การไฟฟ้านครหลวง	๐ ๒๓๔๘ ๕๒๒๒, ๐ ๒๓๔๘ ๕๓๓๓
๕.๒.๒ บริษัท สตรีม ไอ.ที.คอนซัลติ้ง จำกัด จำกัด	๐ ๒๖๗๙ ๒๒๓๓
๕.๒.๓ บริษัท อินเตอร์ลิ้งค์ คอมมูนิเคชั่น จำกัด	๐ ๒๖๙๓ ๑๒๒๒

๖. การบังคับบัญชา

๖.๑ กรณีสถานการณ์เบื้องต้น ผอ.สทส. หรือผู้ที่ได้รับ มอบหมายเป็นผู้บังคับบัญชาสั่งการ ได้แก่ ช.ผอ.สทส., ห.กปค., ตามลำดับ

๖.๒ กรณีสถานการณ์ขั้นสูงสุด ผอก.ขสมก. หรือผู้ที่ได้รับมอบหมายเป็นผู้บังคับบัญชาสูงสุด

๗. การติดต่อสื่อสาร

๗.๑ การสื่อสาร กรณีภาวะปกติให้ใช้ระบบโทรศัพท์พื้นฐาน และแอพพลิเคชั่นไลน์

๗.๒ กรณีฉุกเฉินใช้โทรศัพท์เคลื่อนที่

๘. การรายงาน

๘.๑ หน่วยปฏิบัติการทุกหน่วยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชาตามลำดับชั้นพร้อมทั้งข้อสังเกต (ถ้ามี)

๘.๒ หน่วยงานต้องรายงานความเสียหายและการปฏิบัติงานของเจ้าหน้าที่ต่อผู้บังคับบัญชา หมายเลขโทรศัพท์ในการติดต่อสื่อสาร

๘.๓ เจ้าหน้าที่ กลุ่มงานปฏิบัติการคอมพิวเตอร์และเครือข่าย

๘.๓.๑	นายยงยุทธ	พันธ์สวัสดิ์	๐๘ ๖๘๘๑ ๑๖๙๗
๘.๓.๒	นายชานนทร์	แก้วพรายตา	๐๘ ๑๙๘๔ ๕๕๘๔
๘.๓.๓	นายสมยศ	อินทรศิลป์	๐๘ ๙๔๙๕ ๕๓๙๖
๘.๓.๔	นายวราราช	ชื่อดี	๐๘ ๑๖๕๕ ๕๓๕๖
๘.๓.๕	นายประวัติ	สุขพันธ์	๐๘ ๘๕๙๓ ๖๔๖๑
๘.๓.๖	นายปิยะสิทธิ์	พูลสุข	๐๘ ๓๐๐๒ ๓๗๙๓
๘.๓.๗	นางสาวสุนทรี	ฟักขำ	๐๘ ๓๘๕๗ ๒๑๐๐

๘.๓.๘ นางสาวนิตยา ศรีนวลมาก	๐๘ ๗๐๗๓ ๕๗๓๙
๘.๓.๙ นางสาวเสาวนีย์ คงสุวรรณ์	๐๖ ๕๒๕๘ ๑๐๙๕
๘.๓.๑๐ นางสาวรุ่งทิพย์ มาตา	๐๘ ๗๖๗๕ ๘๒๑๕
๘.๓.๑๑ นางสาวรุ่งรวี นาคเฉลิม	๐๖ ๕๕๒๕ ๕๑๕๖
๘.๓.๑๒ นายสมภพ พระทัย	๑๘ ๖๓๓๙ ๕๘๘๘
๘.๓.๑๓ นายทรัพย์ประสิทธิ์ เฉยเมล์	๐๘ ๔๙๗๒ ๗๕๙๘
๘.๓.๑๔ นางสาวจันทิรา พลอยมีทรัพย์	๐๘ ๐๐๙๙ ๔๒๖๗
๘.๓.๑๕ นายเอกสิทธิ์ อิงสันเทียะ	๐๖ ๔๒๖๐ ๘๑๘๑

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๗
การตรวจสอบและประเมินความเสี่ยง

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๒. ผู้รับผิดชอบ

๒.๑ สำนักเทคโนโลยีสารสนเทศ

๒.๒ ผู้ดูแลระบบสารสนเทศและ Auditors

๓. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงของสารสนเทศ

๓.๑ ระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงขององค์การเพื่อการประเมินความเสี่ยงนั้น

๓.๒ กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้นโดยการประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบในด้าน

๓.๒.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๓.๒.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๓.๒.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๓.๓ กำหนดมาตรการจัดการความเสี่ยง

๓.๔ ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan)

๓.๔.๑ กำหนดรอบระยะเวลาการตรวจประเมินจากหน่วยงานภายใน (Internal Audit) ไตรมาสละ ๑ ครั้ง โดย สำนักตรวจสอบ, สำนักบริหารความเสี่ยงและควบคุมภายใน

๓.๔.๒ กำหนดรอบระยะเวลาการตรวจประเมินจากหน่วยงานภายนอก (External Audit) ๖ เดือน / ครั้ง โดยหน่วยงาน สรอ.

๓.๕ ต้องดำเนินการทบทวนนโยบาย แนวปฏิบัติ รวมทั้งกฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของสารสนเทศในการใช้เครื่องคอมพิวเตอร์และเครือข่ายให้ชัดเจน

หมวดที่ ๔ หน้าที่และความรับผิดชอบด้านสารสนเทศ

ส่วนที่ ๘
การจัดการด้านวินัยเมื่อมีการละเมิดหรือละเลยต่อหน้าที่

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ สำนักเทคโนโลยีสารสนเทศ

๒.๒ ผู้ดูแลระบบ

๓. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมขององค์การ

๓.๒ จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

๓.๓ ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๓.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

๔. แนวปฏิบัติการจัดการด้านวินัยเมื่อมีการละเมิดหรือละเลยต่อหน้าที่

๔.๑ จัดทำระเบียบวินัยเมื่อมีการละเมิดหรือละเลย เพื่อเป็นแนวปฏิบัติในการดำเนินการในกรณีที่บุคลากรมีการละเมิดหรือละเลยต่อนโยบายหรือกฎระเบียบที่ใช้ในการควบคุมดูแลในด้านความปลอดภัยของข้อมูลและทรัพยากรขององค์การ

๔.๒ กำหนดบทลงโทษเมื่อมีการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัย

๔.๓ กำหนดกระบวนการเกี่ยวกับการลงโทษต่อผู้ที่ฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัย

๔.๔ กำหนดขั้นตอนการปฏิบัติเกี่ยวกับการลงโทษต่อผู้ที่ฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัย ดังนี้

๔.๔.๑ การว่ากล่าวตักเตือน

๔.๔.๒ การตักเตือนอย่างเป็นทางการ

๔.๔.๓ การระบุโทษและพิจารณาลงโทษ

๔.๔.๔ การลงโทษ

ส่วนที่ ๙
การกำหนดผู้รับผิดชอบ

๑. วัตถุประสงค์

กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนว นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ระดับนโยบาย

ให้ผู้บริหารระดับสูงขององค์การ ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานที่ทำหน้าที่ CEO และผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การ ติดตามและกำกับดูแลควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

๓. แนวทางปฏิบัติของผู้รับผิดชอบ

๓.๑ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบฐานข้อมูลและระบบสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยง และตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและระบบสารสนเทศ พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

๓.๑.๑ ควบคุมการเข้า-ออกห้อง Server ตามการกำหนดสิทธิ์การเข้าถึง Server

๓.๑.๒ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้สามารถใช้ งานได้ตามปกติตลอดเวลา ๒๔ ชม.

๓.๑.๓ กำกับดูแล การติดตั้ง รื้อถอน ดูแล ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN, Internet, Intranet ที่ให้บริการภายในหน่วยงาน

๓.๑.๔ กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของเครื่อง Server ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้

๓.๑.๕ แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

๓.๑.๖ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาระดับสูงทราบสม่ำเสมอ

๓.๑.๗ กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิ์การเข้าถึงระบบ

๓.๑.๘ กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๓.๑.๙ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ในServer ของระบบฐานข้อมูลทั้งหมดที่ให้บริการในเว็บไซต์ ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.

๓.๑.๑๐ กำกับดูแล ตรวจสอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบอื่นๆ