BMTA
องค์การขนส่งมวลชนกรุงเทพ

(สำเนา)

ประกาศองค์การขนส่งมวลชนกรุงเทพ

เรื่อง นโยบายและระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูล

และข้อมูลขนาดใหญ่ขององค์กร

.....

เพื่อกำหนดแนวทางการบริหารจัดการข้อมูลขององค์การขนส่งมวลชนกรุงเทพ ให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ กฎหมาย กฎระเบียบ และข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง สอดคล้องกับหลักปฏิบัติสากลในเรื่องการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ โดยการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลที่มีการรวบรวม จัดเก็บ ใช้เผยแพร่ หรือดำเนินการอื่นใด เกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์กับองค์การขนส่งมวลชนกรุงเทพจะต้องมีความมั่นคงปลอดภัย ความน่าเชื่อถือ และมีการคุ้มครองข้อมูลส่วนบุคคล องค์การขนส่งมวลชนกรุงเทพ จึงได้จัดทำนโยบายและระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร ฉบับนี้ขึ้น เพื่อคุ้มครองการดูแลข้อมูลและการบริหารจัดการข้อมูลที่มีการรวบรวม จัดเก็บ ใช้หรือเผยแพร่ในรูปของข้อมูลอิเล็กทรอนิกส์ ซึ่งปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย

อาศัยอำนาจตามความในมาตรา ๖ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ องค์การขนส่งมวลชนกรุงเทพ จึงออกนโยบายฉบับนี้ในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กรโดยมีรายละเอียดดังต่อไปนี้

ข้อ ๑. ประกาศนี้ เรียกว่า “ประกาศองค์การขนส่งมวลชนกรุงเทพ เรื่องนโยบายและระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร”

ข้อ ๒. ในประกาศนี้

(๑) “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลซึ่งสามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

(๒) “ผู้ใช้บริการ” หมายถึง ผู้ใช้บริการขององค์การขนส่งมวลชนกรุงเทพทั้งหมดที่เกี่ยวข้อง

(๓) “ผู้ควบคุมข้อมูล” หมายถึง ผู้ที่มีหน้าที่รับผิดชอบในการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล

(๔) “เจ้าของข้อมูล” หมายถึง บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล

(๕) "ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพ ของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ทั้งการจัดเก็บในรูปของ เอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง หรือจัดเก็บการบันทึกในเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

(๖) "ชุดข้อมูล" หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

(๗) "บัญชีข้อมูล" หมายถึง เอกสารแสดงบรรดารายการของชุดข้อมูลที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทชุดข้อมูลที่อยู่ในความครอบครองหรือควบคุมขององค์การขนส่งมวลชนกรุงเทพ

(๘) "การบริหารจัดการข้อมูล" หมายถึง ขั้นตอน วิธีการหรือกระบวนการใด ๆ อันนำไปสู่การสร้างข้อมูล รวบรวมข้อมูล การจัดเก็บ การจัดเก็บถาวร การทำลายข้อมูล การประมวลผลข้อมูล การแลกเปลี่ยน การเชื่อมโยงข้อมูล และการเปิดเผยข้อมูลต่อสาธารณะ

(๙) "นโยบาย" หมายความว่า นโยบายในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กรที่เป็นไปตามพระราชบัญญัติที่เกี่ยวข้อง ดังนี้

ก. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

ข. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ค. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และที่แก้ไขเพิ่มเติม

ง. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

จ. พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. ๒๕๖๒

ฉ. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม

ข้อ ๓. การเก็บรวบรวมชุดข้อมูลและข้อมูลส่วนบุคคล

องค์การขนส่งมวลชนกรุงเทพ จะดำเนินการรวบรวม จัดเก็บข้อมูลอย่างมีขอบเขตจำกัด และใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม และให้เจ้าของข้อมูลทราบหรือได้รับความยินยอมจากเจ้าของข้อมูลตามแต่กรณี

ข้อ ๔. คุณภาพของชุดข้อมูลและข้อมูลส่วนบุคคล

๔.๑. ชุดข้อมูลและข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บ ให้เป็นไปตามภารกิจ อำนาจหน้าที่ ระเบียบและกฎหมายในการดำเนินงานขององค์การขนส่งมวลชนกรุงเทพ โดยข้อมูลดังกล่าวจะได้รับการตรวจสอบความถูกต้อง ครบถ้วนของข้อมูล และปรับปรุงให้ทันสมัยอยู่เสมอ

๔.๒. ชุดข้อมูลที่เก็บรวบรวมจะถูกบันทึกและตรวจสอบโดยเจ้าหน้าที่ขององค์การขนส่งมวลชนกรุงเทพ และผู้ใช้บริการสามารถแจ้งหรือร้องขอปรับปรุงข้อมูลส่วนบุคคลได้ ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ (มาตรา ๒๕)

๔.๓. กรณีที่เป็นข้อมูลเรื่องเดียวกันแต่มีหลายแหล่งที่มา องค์การขนส่งมวลชนกรุงเทพ จะยึดจากแหล่งที่น่าเชื่อถือได้มากที่สุด เช่น ข้อมูลชื่อบริษัท (ภาษาไทย) องค์การขนส่งมวลชนกรุงเทพ จะยึดถือตามเอกสารที่ได้รับการรับรองจากกรมพัฒนาธุรกิจการค้า เป็นต้น

๔.๔. วิธีการรับ-ส่ง ประมวลผล และจัดเก็บชุดข้อมูลและข้อมูลส่วนบุคคล ถูกดำเนินการตามขั้นตอนระเบียบที่องค์การขนส่งมวลชนกรุงเทพได้ประกาศกำหนดไว้

ข้อ ๕. วัตถุประสงค์ในการเก็บรวบรวมข้อมูล

๕.๑ เพื่อนำไปใช้งานตามภารกิจ อำนาจหน้าที่ ระเบียบและกฎหมายในการดำเนินงานขององค์การขนส่งมวลชนกรุงเทพ

๕.๒ เพื่อเป็นส่วนหนึ่งในการพิจารณาอนุมัติ การให้บริการข้อมูล การจัดทำรายงานสรุปและการประมวลผลสถิติภายใต้ภารกิจขององค์การขนส่งมวลชนกรุงเทพ

๕.๓. เพื่อความสะดวกในการให้บริการแก่ผู้ใช้บริการที่สมัครสมาชิก หรือเพื่อใช้บริการอย่างใดอย่างหนึ่ง

๕.๔ เพื่อสำรวจความคิดเห็นหรือความพึงพอใจในการใช้บริการ อันจะเป็นประโยชน์ในการนำไปใช้ปรับปรุงคุณภาพในการให้บริการขององค์การขนส่งมวลชนกรุงเทพ ซึ่งอาจจำเป็นต้องจัดเก็บรวบรวมข้อมูลของผู้ใช้บริการบางอย่างเพิ่มเติมด้วย เช่น หมายเลขไอพี (IP Address) ชนิดของโปรแกรมค้นดูเว็บ (Browser Type) ชื่อโดเมน (Domain Name) หน้าเว็บไซต์ที่ผู้ใช้เข้าเยี่ยมชม เป็นต้น

๕.๕. เพื่อการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐ หรือหน่วยงานอื่น ซึ่งองค์การขนส่งมวลชนกรุงเทพ กำหนดให้มีการปฏิบัติตามคู่มือการปฏิบัติงาน (Procedure Manual) และ/หรือ วิธีปฏิบัติงาน (Work Instruction) ตามมาตรฐาน ISO/IEC27001 โดยข้อมูลนั้นต้องได้รับการอนุญาตเป็นลายลักษณ์อักษรก่อนทำการแลกเปลี่ยนระหว่างกัน

๕.๖. เพื่อใช้ทำสถิติข้อมูลผู้ติดต่อ และ/หรือ ผู้ใช้บริการข้อมูลขององค์การขนส่งมวลชนกรุงเทพ

๕.๗. หากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูล องค์การขนส่งมวลชนกรุงเทพจะทำการบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน

ข้อ ๖. ข้อจำกัดในการนำชุดข้อมูลและข้อมูลส่วนบุคคลไปใช้

๖.๑. องค์การขนส่งมวลชนกรุงเทพ จะไม่เปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดของชุดข้อมูลและข้อมูลส่วนบุคคล ที่ไม่สอดคล้องกับวัตถุประสงค์ของการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นไปตามภารกิจ อำนาจหน้าที่ ระเบียบและกฎหมายในการดำเนินงานขององค์การขนส่งมวลชนกรุงเทพ ที่กำหนดให้กระทำได้ หรือตามคำสั่งของศาล

๖.๒. องค์การขนส่งมวลชนกรุงเทพ จะปรับปรุง แก้ไข และใช้ชุดข้อมูลและข้อมูลส่วนบุคคลของผู้ใช้บริการ เพื่อให้เป็นไปตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูล ในข้อ ๕.

๖.๓. ในกรณีที่องค์การขนส่งมวลชนกรุงเทพ ได้ว่าจ้างบริษัท/หน่วยงานอื่นดำเนินการเกี่ยวกับชุดข้อมูลและข้อมูลส่วนบุคคลของผู้ใช้บริการ เช่น การจัดส่งไปรษณีย์ การวิเคราะห์ข้อมูลเชิงสถิติการปรับปรุงและดูแลระบบฐานข้อมูล เป็นต้น องค์การขนส่งมวลชนกรุงเทพ ได้กำหนดให้บริษัท/หน่วยงานที่ว่าจ้างดังกล่าวเก็บรักษาความลับและความปลอดภัยของชุดข้อมูลและข้อมูลส่วนบุคคลของผู้ใช้บริการ และกำหนดข้อห้ามมิให้มีการนำชุดข้อมูลและข้อมูลส่วนบุคคลดังกล่าวไปใช้นอกเหนือจากกิจกรรมของสำนักงานโดยกำหนดให้มีการลงนามในบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) และเอกสารอื่น ๆ ที่เกี่ยวข้องกับองค์การขนส่งมวลชนกรุงเทพ อย่างเหมาะสมทุกครั้งก่อนอนุญาตให้เริ่มปฏิบัติงานหรือเข้าถึงและใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ

ข้อ ๗. การรักษาความมั่นคงปลอดภัย

องค์การขนส่งมวลชนกรุงเทพ กำหนดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของชุดข้อมูลและข้อมูลส่วนบุคคลเพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ โดยให้ปฏิบัติตามประกาศองค์การขนส่งมวลชนกรุงเทพ เรื่องนโยบายและระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร และนโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐาน ISO/IEC27001 โดยมีคู่มือการปฏิบัติงาน (Procedure Manual) และ/หรือ วิธีปฏิบัติงาน (Work Instruction) กำกับการปฏิบัติงานตามลำดับ

ข้อ ๘. การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับชุดข้อมูลและข้อมูลส่วนบุคคล

องค์การขนส่งมวลชนกรุงเทพ มีการเปิดเผยการดำเนินการ นโยบาย และแนวปฏิบัติที่เกี่ยวกับชุดข้อมูลและข้อมูลส่วนบุคคล และจัดให้มีวิธีการที่สามารถตรวจดูความมีอยู่ ลักษณะของข้อมูลส่วนบุคคล วัตถุประสงค์ของการนำข้อมูลไปใช้ ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคลได้จากเว็บไซต์ http://www.bmta.co.th

ข้อ ๙. การมีส่วนร่วมของเจ้าของข้อมูล

๙.๑ เจ้าของข้อมูล สามารถตรวจสอบถึงความมีอยู่หรือรายละเอียดของชุดข้อมูลและข้อมูลส่วนบุคคล ตามช่องทางที่องค์การขนส่งมวลชนกรุงเทพ กำหนด หรือยื่นคำร้องขอแก้ไข ปรับปรุง ยกเลิกข้อมูล ให้เป็นไปตามข้อเท็จจริงในปัจจุบันได้ โดยผู้ควบคุมข้อมูลจะดำเนินการตามคำร้องขอโดยเร็ว หรือภายในระยะเวลาตามคู่มือปฏิบัติงานที่องค์การขนส่งมวลชนกรุงเทพ กำหนด โดยช่องทางในการติดต่อองค์การขนส่งมวลชนกรุงเทพ ให้เป็นไปตามประกาศองค์การขนส่งมวลชนกรุงเทพ เรื่องนโยบายและระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร

๙.๒ เจ้าของข้อมูลหรือผู้แทนโดยชอบธรรมตามกฎหมาย สามารถขอรับคำชี้แจงหรือข้อมูลตามคำร้องขอได้

๙.๓ ข้อมูลบางอย่างซึ่งองค์การขนส่งมวลชนกรุงเทพ กำหนดให้ผู้ใช้งานกรอกผ่านแบบฟอร์มของเว็บไซต์ เช่น ฟอร์มลงทะเบียนผู้ใช้บริการสามารถเลือกได้ว่าจะให้ข้อมูลนั้นหรือไม่ ทั้งนี้หากผู้ใช้บริการไม่สะดวกที่จะให้ข้อมูลผ่านทางเว็บไซต์ สามารถเข้ามาติดต่อเจ้าหน้าที่องค์การขนส่งมวลชนกรุงเทพได้ตามที่อยู่ แนบท้ายนี้

๙.๔ ในกรณีที่องค์การขนส่งมวลชนกรุงเทพ ปฏิเสธการให้ข้อมูลส่วนบุคคลใด ๆ องค์การขนส่งมวลชนกรุงเทพ จะจัดทำคำชี้แจงให้ผู้ร้องขอทราบภายใน ๓๐ วัน

ข้อ ๑๐. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

๑๐.๑. ให้ผู้ควบคุมข้อมูล ทำการบันทึก และ/หรือ จัดเก็บเอกสารรายละเอียดของการปรับปรุงแก้ไขชุดข้อมูลและข้อมูลส่วนบุคคล จัดทำบันทึกคำคัดค้านการจัดเก็บ หรือการกระทำใด ๆ เกี่ยวกับข้อมูลของเจ้าของข้อมูลไว้เป็นหลักฐาน

๑๐.๒ ให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามมาตรการที่กำหนดไว้ข้างต้น เพื่อให้การดำเนินงานตามนโยบายและระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร เป็นไปตามมาตรฐานของประกาศฉบับนี้

๑๐.๓ กรณีการเปลี่ยนแปลงข้อมูลส่วนบุคคลมีผลกระทบกับผู้ใช้บริการ องค์การขนส่งมวลชนกรุงเทพ จะดำเนินการแจ้งผู้ที่ได้รับผลกระทบจากการเปลี่ยนแปลงได้รับทราบโดยเร็ว

ข้อ ๑๑. การปรับปรุงนโยบายการคุ้มครองข้อมูลส่วนบุคคล

องค์การขนส่งมวลชนกรุงเทพ อาจทำการปรับปรุงหรือแก้ไขนโยบายในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร โดยจะแจ้งให้ผู้ใช้บริการทราบล่วงหน้าอย่างน้อย ๗ วัน ที่หน้าเว็บไซต์ของสำนักงาน http://www.bmta.co.th หรือแจ้งให้ทราบทางจดหมายอิเล็กทรอนิกส์ หรือช่องทางอื่น ๆ แล้วแต่กรณี ทั้งนี้เพื่อความเหมาะสมและมีประสิทธิภาพในการให้บริการ โดยจะแจ้งวัตถุประสงค์ของการปรับปรุงหรือแก้ไขนโยบายฯ ให้ทราบอย่างชัดเจน

ข้อ ๑๒. การติดต่อกับองค์การขนส่งมวลชนกรุงเทพ

ในกรณีที่ผู้ใช้บริการมีข้อสงสัย ข้อเสนอแนะ หรือข้อติชมใด ๆ เกี่ยวกับนโยบายและระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร อันจะเป็นประโยชน์ต่อการพัฒนาปรับปรุงการให้บริการขององค์การขนส่งมวลชนกรุงเทพ สามารถติดต่อองค์การขนส่งมวลชนกรุงเทพได้ตามที่ องค์การขนส่งมวลชนกรุงเทพ เลขที่ ๑๓๑ ถนนวัฒนธรรม ห้วยขวาง กทม. ๑๐๓๑๐ โทรศัพท์: Call Center ๑๓๔๘ สำนักงานใหญ่ ๐๒-๒๔๖-๐๓๓๙, ๐๒-๒๔๖-๐๗๔๑-๔ โทรสาร: ๐๒-๒๔๗-๒๑๘๙ เว็บไซต์: http://www.bmta.co.th, อีเมล์: 1348@bmta.co.th

ระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูล และข้อมูลขนาดใหญ่ขององค์กร

องค์การขนส่งมวลชนกรุงเทพ ได้จัดทำระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กรนี้ขึ้น เพื่อกำหนดขั้นตอนและวิธีการดำเนินงานในการปฏิบัติกับชุดข้อมูลและข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามนโยบายคุ้มครองข้อมูลส่วนบุคคลและตามกฎหมาย สอดคล้องกับหลักปฏิบัติสากลในเรื่องการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร โดยการดำเนินการใด ๆ เกี่ยวกับการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กรที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ หลักการสำคัญว่า ข้อมูลต้องได้รับการคุ้มครองที่เหมาะสมในทุกขั้นตอน ตั้งแต่การเก็บรวบรวม การเก็บรักษา และการเปิดเผย ต้องถูกนำมากำหนดเป็นนโยบายในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กรเช่นกัน

๑. ข้อมูลเบื้องต้น

(ก) ชื่อ : ระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร จัดทำขึ้นเพื่อบังคับใช้ตามนโยบายในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร และตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.๒๕๔๐

(ข) ขอบเขต : องค์การขนส่งมวลชนกรุงเทพจะดำเนินการรวบรวม จัดเก็บ หรือใช้ข้อมูลส่วนบุคคล เพื่อนำไปใช้งานตามภารกิจ อำนาจหน้าที่ ระเบียบและกฎหมายในการดำเนินงานขององค์การขนส่งมวลชนกรุงเทพ ซึ่งครอบคลุมตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลของนโยบายในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร

(ค) กรณีมีการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร องค์การขนส่งมวลชนกรุงเทพจะแจ้งให้ทราบล่วงหน้าอย่างน้อย ๗ วัน ที่หน้าเว็บไซต์ขององค์การขนส่งมวลชนกรุงเทพ หรือแจ้งให้ทราบทางจดหมายอิเล็กทรอนิกส์หรือช่องทางอื่น ๆ แล้วแต่กรณี โดยจะแจ้งวัตถุประสงค์ของการเปลี่ยนแปลงนโยบาย ๆ ให้ทราบอย่างชัดเจน

๒. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลและข้อมูลขนาดใหญ่ขององค์กร

ข้อมูลที่องค์การขนส่งมวลชนกรุงเทพ จัดเก็บ จะถูกระบุอยู่ในแบบฟอร์ม คำร้องหรือระบุในเอกสารคำขอของหน่วยงานที่ประกาศกำหนดไว้ เป็นลายลักษณ์อักษรเท่านั้น โดยเจ้าหน้าที่ผู้ดำเนินการได้รับทราบและปฏิบัติตามอำนาจหน้าที่ ระเบียบและกฎหมายในการดำเนินงานขององค์การขนส่งมวลชนกรุงเทพ โดยข้อมูลใด ๆ ที่องค์การขนส่งมวลชนกรุงเทพ ไม่จัดเก็บ จะไม่ถูกระบุอยู่ในแบบฟอร์มใด ๆ

องค์การขนส่งมวลชนกรุงเทพ จะเก็บรวบรวมชุดข้อมูลและข้อมูลส่วนบุคคลของ ผู้ติดต่อ/ผู้ใช้บริการ ที่เป็นพื้นฐานทั่วไป เช่น

๑. ข้อมูลบุคคล ได้แก่ ชื่อ-นามสกุล ที่อยู่ ตำแหน่ง โทรศัพท์ โทรสาร และ E-Mail เป็นต้น

๒. ข้อมูลบริษัท ได้แก่ ชื่อบริษัท ที่อยู่ โทรศัพท์ โทรสาร เลขทะเบียนนิติบุคคล เป็นต้น

กรณีที่องค์การขนส่งมวลชนกรุงเทพ มีการเก็บรวบรวมข้อมูลตามแบบฟอร์ม คำร้องหรือเอกสารคำขอ ที่ประกาศกำหนดไว้ องค์การขนส่งมวลชนกรุงเทพจะแจ้งให้เจ้าหน้าที่ทราบว่าจะต้องจัดเก็บตามรูปแบบใดเพื่อความเข้าใจที่ถูกต้องตรงกัน

(ก) การติดต่อระหว่างหน่วยงานของรัฐ

องค์การขนส่งมวลชนกรุงเทพ จะติดต่อกับหน่วยงานอื่น หรือผู้มาใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ ผ่านระบบต่าง ๆ เช่น ระบบ Internet , Website , E-Mail หรือตามที่ผู้ใช้บริการแจ้งไว้

(ข) การใช้คุกกี้ (Cookies)

องค์การขนส่งมวลชนกรุงเทพ มีการใช้งาน “คุกกี้” (Cookies) เพื่อช่วยอำนวยความสะดวกของผู้ใช้บริการในการเข้าถึงบริการขององค์การขนส่งมวลชนกรุงเทพ แต่ไม่ได้ใช้เชื่อมโยงกับข้อมูลส่วนบุคคลโดย “คุกกี้” เป็นไฟล์ข้อมูลขนาดเล็กซึ่งจะถูกส่งไปเก็บไว้ที่ Web Browser ของผู้ใช้บริการ ทำหน้าที่ในการเก็บข้อมูลสถานะการใช้งานต่าง ๆ ของผู้ใช้บริการ

ข้อดีของคุกกี้ คือ กรณีที่ผู้ใช้บริการเคยเข้าเว็บไซต์ที่มีการบันทึกข้อมูล หรือมีการลงทะเบียนไว้แล้ว ในการใช้งานครั้งต่อไป ผู้ใช้บริการจะสามารถเข้าไปยังเว็บไซต์นั้น ๆ ได้ทันที โดยไม่ต้องบันทึกข้อมูลหรือลงทะเบียนใหม่ ทั้งนี้เนื่องจาก Web Browser ของผู้ใช้บริการจะทำการส่งข้อมูลภายในคุกกี้ ไปยังเว็บไซต์นั้น ๆ โดยอัตโนมัติทำให้เว็บไซต์นั้น ๆ ทราบว่าผู้ใช้บริการคือใคร เคยบันทึกข้อมูลหรือลงทะเบียนแล้วหรือไม่ หรือมีความต้องให้องค์การขนส่งมวลชนกรุงเทพดำเนินการปรับปรุงในเรื่องอะไร เป็นต้น

(ค) การเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information)

ในกรณีที่ผู้ใช้บริการสมัครสมาชิก ระบบจะเก็บรวบรวมข้อมูลพื้นฐานส่วนบุคคล เช่น ชื่อ - นามสกุล เพศ อายุ อาชีพ และที่อยู่ในการติดต่อ เพื่อใช้เป็นข้อมูลในการติดต่อและให้บริการข้อมูลข่าวสารต่าง ๆ เช่น การเปลี่ยนแปลงข้อกำหนด เงื่อนไข หรือนโยบายต่าง ๆ การส่งเอกสารประชาสัมพันธ์ต่าง ๆ รวมถึงใช้เป็นข้อมูลสนับสนุนในการปฏิบัติตามภารกิจของหน่วยงาน เช่น การตรวจสอบ การวิเคราะห์ข้อมูล การจัดเก็บสถิติผู้เข้าเยี่ยมชมเว็บไซต์ รวมถึงการสำรวจความพึงพอใจในการใช้บริการ เป็นต้น อันจะเป็นประโยชน์ในการนำสถิติไปใช้ เพื่อการปรับปรุงคุณภาพในการให้บริการขององค์การขนส่งมวลชนกรุงเทพ

(ง) บันทึกผู้เข้าชมเว็บ (Log Files)

การให้บริการเว็บไซต์ขององค์การขนส่งมวลชนกรุงเทพ ต้องมีการเก็บบันทึกการเข้า-ออก และระหว่างการเข้าใช้บริการของผู้ใช้บริการโดยอัตโนมัติ ที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลที่ระบุตัวบุคคล เช่น หมายเลข IP Address ซึ่งใช้เป็นข้อมูลที่เชื่อมโยงกลับไปที่ข้อมูลการเชื่อมต่ออินเตอร์เน็ตซึ่งอาจระบุถึงแหล่งที่มาการโพสต์หรือบุคคลที่โพสต์ได้ รวมถึงเว็บไซค์ที่เข้า-ออกก่อนและหลัง และประเภทของ

โปรแกรมบราวเซอร์ (Browser) ทั้งนี้ เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๒๖ ที่กำหนดให้ผู้ให้บริการต้องเก็บข้อมูลจราจรคอมพิวเตอร์ ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

(จ) การจัดเก็บข้อมูลผ่านทางหน้าเว็บไซต์

ชุดข้อมูลและข้อมูลส่วนบุคคลบางรายการ ผู้ใช้บริการมีสิทธิเลือกที่จะ "ให้หรือไม่ให้" ข้อมูลผ่านทางหน้าเว็บไซต์ได้ ผู้ใช้บริการสามารถให้ชุดข้อมูลและข้อมูลส่วนบุคคลผ่านช่องทางอื่น ๆ ได้แก่ E-Mail โทรศัพท์ โทรสาร หรือมาติดต่อด้วยตนเอง ณ สถานที่ทำการ

๓. การระบุความเชื่อมโยงให้ชุดข้อมูลและข้อมูลส่วนบุคคลกับหน่วยงาน หรือองค์กรอื่น

ในการเก็บชุดข้อมูลและข้อมูลส่วนบุคคล องค์การขนส่งมวลชนกรุงเทพ มีการระบุชื่อผู้เก็บรวมรวมข้อมูล หรือชื่อผู้มีสิทธิในข้อมูลทั้งหมด รวมถึงประเภทของข้อมูล ที่ได้มีการเก็บรวบรวม (Data Subject) และชื่อผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวทั้งที่จะใช้ร่วมกับหน่วยงานหรือองค์กรที่เกี่ยวข้อง ตลอดจนชื่อผู้มีหน้าที่ปฏิบัติตามนโยบายในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร โดยแจ้งให้ผู้ใช้บริการทราบและให้ความยินยอมล่วงหน้า ก่อนทำการเชื่อมโยงให้ข้อมูลแก่หน่วยงานหรือองค์กรอื่น หรือดำเนินการอื่นเพื่อให้เป็นไปตามภารกิจ อำนาจหน้าที่ ระเบียบและกฎหมายในการดำเนินงานขององค์การขนส่งมวลชนกรุงเทพ

๔. การรวบรวมข้อมูลจากที่มาหลายแหล่ง

ในการรวบรวมชุดข้อมูลและข้อมูลส่วนบุคคลของผู้ใช้งานจากหลายแหล่งที่มา องค์การขนส่งมวลชนกรุงเทพจะแจ้งให้ทราบถึงเจตนา และวัตถุประสงค์ของการนำข้อมูลนั้นไปใช้ ในกรณีที่เป็นข้อมูลเรื่องเดียวกันแต่มีหลายแหล่งที่มา องค์การขนส่งมวลชนกรุงเทพจะยึดจากแหล่งที่น่าเชื่อถือได้มากที่สุด เช่น ข้อมูลชื่อบริษัท (ภาษาไทย) องค์การขนส่งมวลชนกรุงเทพจะยึดถือตามเอกสารที่ได้รับการรับรองจากกรมพัฒนาธุรกิจการค้า เป็นต้น เพื่อให้เป็นไปตามภารกิจ อำนาจหน้าที่ ระเบียบและกฎหมายในการดำเนินงานขององค์การขนส่งมวลชนกรุงเทพ

๕. การให้บุคคลอื่นใช้หรือการเปิดเผยชุดข้อมูลและข้อมูลส่วนบุคคล

องค์การขนส่งมวลชนกรุงเทพ จะไม่เปิดเผยชุดข้อมูลและข้อมูลส่วนบุคคลให้กับหน่วยงานหรือบุคคลอื่นใด เว้นแต่จะเป็นไปตามภารกิจ อำนาจหน้าที่ ระเบียบและกฎหมายในการดำเนินงานขององค์การขนส่งมวลชนกรุงเทพ

๖. การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

องค์การขนส่งมวลชนกรุงเทพ จะดำเนินการรวบรวม จัดเก็บ ใช้ หรือเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ เพื่อวัตถุประสงค์ตามที่ได้ระบุไว้ตามนโยบายในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร และ/หรือ ตามภารกิจอำนาจหน้าที่ ระเบียบและกฎหมายในการดำเนินงานขององค์การขนส่งมวลชนกรุงเทพเท่านั้น

๗. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

หากผู้ใช้งานประสงค์ขอปรับปรุง เปลี่ยนแปลง หรือแก้ไขข้อมูลให้ถูกต้อง องค์การขนส่งมวลชนกรุงเทพได้จัดให้มีช่องทางในการติดต่อ ดังนี้

(ก) ส่งจดหมายมายังองค์การขนส่งมวลชนกรุงเทพ เพื่อขอแก้ไขข้อมูล

(ข) ส่ง E-Mail โดยต้องส่งจาก E-Mail เดิมที่เคยให้ไว้กับองค์การขนส่งมวลชนกรุงเทพเพื่อให้ง่ายต่อการตรวจสอบ

(ค) ดำเนินการตามที่ระบุไว้ในเอกสารหรือคู่มือขององค์การขนส่งมวลชนกรุงเทพ

(ง) มาติดต่อด้วยตนเอง ณ สถานที่ทำการ

๘. การรักษาความมั่นคงปลอดภัยของชุดข้อมูลและข้อมูลส่วนบุคคล

เพื่อให้การรักษาความมั่นคงปลอดภัยของชุดข้อมูลและข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพ องค์การขนส่งมวลชนกรุงเทพ จึงกำหนดระเบียบภายในหน่วยงานเพื่อกำหนดสิทธิในการเข้าถึงหรือใช้ข้อมูลส่วนบุคคล ทั้งนี้เพื่อรักษาสถานภาพด้านความลับ (Confidentiality) ด้านความถูกต้องสมบูรณ์ (Integrity) และด้านความพร้อมใช้งาน (Availability) โดยกำหนดให้มีมาตรการที่เหมาะสมตั้งแต่การรวบรวมและจัดเก็บข้อมูลส่วนบุคคล เพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวโดยมิชอบ รวมถึงการป้องกันการกระทำใดที่จะมีผลทำให้ข้อมูลไม่อยู่ในสภาพพร้อมใช้งาน ซึ่งมีการดำเนินการรักษาความมั่นคงปลอดภัย ดังนี้

(ก) สร้างเสริมความสำนึกในการรับผิดชอบ ด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงาน ด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรขององค์การขนส่งมวลชนกรุงเทพเป็นประจำ

๑. องค์การขนส่งมวลชนกรุงเทพมีการจัดอบรมให้แก่พนักงานและผู้เกี่ยวข้องด้านข้อมูลและ ด้านความมั่นคงปลอดภัยเป็นประจำทุกปี

๒. องค์การขนส่งมวลชนกรุงเทพมีการตรวจประเมิน ISO/IEC27001 ทั้ง Internal Audit และ External Audit อย่างน้อยปีละ ๑ ครั้ง

๓. องค์การขนส่งมวลชนกรุงเทพ มีการปฏิบัติตามคู่มือระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Manual) และนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ตามมาตรฐาน ISO/IEC27001 โดยมีคู่มือการปฏิบัติงาน (Procedure Manual) และวิธีปฏิบัติงาน (Work Instruction) กำกับการปฏิบัติงานตามลำดับ

(ข) กำหนดสิทธิและข้อจำกัดสิทธิ ในการเข้าถึงชุดข้อมูลและข้อมูลส่วนบุคคลของบุคลากร พนักงาน หรือลูกจ้าง อย่างชัดเจน และมีการบันทึก รวมทั้งการสำรองข้อมูลของการเข้าถึง หรือการเข้าใช้งานชุดข้อมูลและข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสม

(ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือระบบสารสนเทศทั้งหมดอย่างน้อยปีละ ๑ ครั้ง

๑. องค์การขนส่งมวลชนกรุงเทพมีการทดสอบเจาะระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบงานที่เป็น Web Base อย่างน้อยปีละ ๑ ครั้ง

๒. องค์การขนส่งมวลชนกรุงเทพมีการระบุเงื่อนไขใน TOR การว่าจ้างพัฒนาระบบสารสนเทศ โดยระบบที่พัฒนาขึ้นจะต้องผ่านเกณฑ์มาตรฐานในเรื่องช่องโหว่ OWASP ตามที่กำหนด

๓. องค์การขนส่งมวลชนกรุงเทพมีการใช้โปรแกรมตรวจสอบประสิทธิภาพการทำงานของระบบโปรแกรมทั้งในลักษณะ Web Base และ Application ต่าง ๆ โดยสามารถบอกถึงประสิทธิภาพ ตั้งแต่ ต้นทางที่ผู้ใช้งานทำงาน จนไปถึงระบบโปรแกรมปลายทางต่าง ๆ ในลักษณะ End-to-End Monitoring ได้ทั้งปัญหาและสาเหตุ (Root Cause)

๔. องค์การขนส่งมวลชนกรุงเทพมีการบริหารจัดการเรื่องสินทรัพย์สารสนเทศทั้งหมด ได้แก่ ทะเบียนสินทรัพย์ การประเมินความเสี่ยงสินทรัพย์ แผนจัดการความเสี่ยงสินทรัพย์ และการจัดการความเสี่ยงสินทรัพย์ที่ยังเหลืออยู่

๕. องค์การขนส่งมวลชนกรุงเทพมีการบริหารจัดการเรื่องความเสี่ยง ได้แก่ การประเมินความเสี่ยง แผนจัดการความเสี่ยง รายงานผลการประเมินความเสี่ยง และการจัดการความเสี่ยงที่หลงเหลือ อย่างน้อยปีละ ๑ ครั้ง

(ง) กำหนดให้มีมาตรการที่เหมาะสม และเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของชุดข้อมูลและข้อมูลส่วนบุคคลที่มีความสำคัญ หรือเป็นข้อมูลที่อาจกระทบกับความรู้สึก ความเชื่อ ความสงบเรียบร้อยและศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการขององค์การขนส่งมวลชนกรุงเทพ หรืออาจก่อให้เกิดความเสียหายหรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน

๑. องค์การขนส่งมวลชนกรุงเทพมีการรักษาชุดข้อมูลและข้อมูลส่วนบุคคล โดยปฏิบัติตามนโยบายในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร

๒. สิทธิในการเข้าถึงข้อมูลหรือระบบสารสนเทศใด ๆ ต้องปฏิบัติตามคู่มือการปฏิบัติงาน (Procedure Manual) หรือวิธีปฏิบัติงาน (Work Instruction) กำกับการปฏิบัติงานในเรื่องนั้น ๆ ตามมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC27001

๓. กรณีที่มีการนำชุดข้อมูลและข้อมูลส่วนบุคคลที่มีความสำคัญ ไปก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เจ้าของข้อมูลสามารถแจ้ง หรือร้องเรียน ให้องค์การขนส่งมวลชนกรุงเทพรับทราบโดยองค์การขนส่งมวลชนกรุงเทพจะดำเนินการสอบสวนและลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ ระเบียบปฏิบัติขององค์การขนส่งมวลชนกรุงเทพ แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุในแต่ละข้อกฎหมายนั้น ๆ

๔. องค์การขนส่งมวลชนกรุงเทพมีการรักษาความมั่นคงปลอดภัยของชุดข้อมูลและข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งยวด เช่น หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เป็นต้น

๕. องค์การขนส่งมวลชนกรุงเทพมีการรักษาความมั่นคงปลอดภัยของข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชน ซึ่งเป็นผู้ใช้บริการขององค์การขนส่งมวลชนกรุงเทพ เช่น เชื้อชาติ ศาสนา ความเชื่อความคิดเห็นทางการเมือง สุขภาพ เป็นต้น

๖. องค์การขนส่งมวลชนกรุงเทพไม่มีการเก็บข้อมูลที่อาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพ ของผู้เป็นเจ้าของข้อมูล เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต เป็นต้น

๙.การติดต่อกับองค์การขนส่งมวลชนกรุงเทพ

ในกรณีที่ผู้ใช้บริการมีข้อสงสัย ข้อเสนอแนะ หรือข้อติชมใดๆ เกี่ยวกับนโยบายและระเบียบปฏิบัติในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลและข้อมูลขนาดใหญ่ขององค์กร องค์การขนส่งมวลชนกรุงเทพยินดีที่จะตอบข้อสงสัย รับฟังข้อเสนอแนะ และคำติชมทั้งหลาย อันจะเป็นประโยชน์ต่อการพัฒนาปรับปรุงการให้บริการขององค์การขนส่งมวลชนกรุงเทพต่อไป โดยผู้ใช้บริการสามารถติดต่อองค์การขนส่งมวลชนกรุงเทพได้ตามที่ องค์การขนส่งมวลชนกรุงเทพ เลขที่ ๑๓๑ ถนนวัฒนธรรม ห้วยขวาง กทม. ๑๐๓๑๐ โทรศัพท์: Call Center ๑๓๔๘ สำนักงานใหญ่ ๐๒-๒๔๖-๐๓๓๙, ๐๒-๒๔๖-๐๗๔๑-๔ โทรสาร: ๐๒-๒๔๗-๒๑๘๙ เว็บไซต์: http://www.bmta.co.th, อีเมล์: 1348@bmta.co.th

ประกาศ ณ วันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๕

(นายกิตติกานต์ จอมดวง จารุวรพลกุล)
ผู้อำนวยการองค์การขนส่งมวลชนกรุงเทพ

สำเนาถูกต้อง

(นางสาวอัญชลี กังวาล)
ห.ธก.(สบจ.)
๓๑ พ.ค. ๖๕

/สำเนาเรียน....

สำเนาเรียน ผอก.

รอง ผอก.ฝบร., รอง ผอก.ฝรอ., รอง ผอก. ฝรร.

ช.ผอก.ฝบร., ช.ผอก.ฝรอ. ๑, ๒, ช.ผอก.ฝรร.

- เพื่อโปรดทราบ

ผอ.ขดร. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘

สบส. สผอ. สตส. สทส. สผง. สกม. สบก. สบจ. สจท. สบด. สพบ. สปร. ๑, ๒ สตง.

ช.ผอ.สบส. ช.ผอ.สผอ. ช.ผอ.สตส. ช.ผอ.สทส. ช.ผอ.สผง. ช.ผอ.สกม. ช.ผอ.สบก.

ช.ผอ.สปร. ๑, ๒ ช.ผอ.สบจ. ช.ผอ.สจท. ช.ผอ.สบด. ช.ผอ.สพบ. ผตก. ๗

ช.ผอ.ขดร. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘

กลป. กบส. กคน. กปส. กตพ. กตป. กตบ. กวพ. กวผ. กวป. กวท. กปค. กงก.

กคด. กนก. กบช. กบง. กรร. ๑, ๒, ๓, ๔ กจช. กบก. กบค. กบท. กคว. กวก. กฝอ.

กสส. กพส. กซบ. กสต. ผตก.๖

กบท. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘

กบง. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘

กปด. ๑๑, ๒๑, ๓๑, ๑๒, ๒๒, ๓๒, ๑๓, ๒๓, ๓๓, ๑๔, ๒๔, ๓๔,
๑๕, ๒๕, ๓๕, ๑๖, ๒๖, ๓๖, ๑๗, ๒๗, ๓๗, ๑๘, ๒๘, ๓๘

กง. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘ บม. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘

ตส. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘ บค. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘

บส. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘ บก. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘

ผข. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘ อบ. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘

ตก. ๑, ๒, ๓, ๔, ๕, ๖, ๗, ๘

ธป. ๑๑, ๒๑, ๓๑, ๑๒, ๒๒, ๓๒, ๑๓, ๒๓, ๓๓, ๑๔, ๒๔, ๓๔
๑๕, ๒๕, ๓๕, ๑๖, ๒๖, ๓๖, ๑๗, ๒๗, ๓๗, ๑๘, ๒๘, ๓๘

บส. คน. ปส. ปช. ลก. ตพ. วม. วพ. บป. วป. งป. ผผ. พร. ปค. บร. ผค. คด. อบ. รจ.

ปบ. ตจ. บง. บด. ๑, ๒, ๓, ๔ กท. ๑, ๒, ๓, ๔ ขผ. ตบ. รบ. ขบ. วน. รส. ธก.

ผด. กช. วบ. บผ. บง. สก. ปอ. พท. กช. สส. สต.

ธก.(ฝบร.) ธก.(ฝรร.) ธก.(ฝรอ.) ธก.(สบจ.) ธก.(กซบ.) มธ.(สบส.) มธ.(สผอ.) มธ.(สตส.)

มธ.(สทส.) มธ.(สผง.) มธ.(ช.ผอก.ฝบร.) มธ.(สกม.) มธ.(สบก.) มธ.(ช.ฝรร.) มธ.(สปร. ๑, ๒)

มธ.(สจท.) มธ.(ช.ผอก.ฝรอ. ๑, ๒) มธ.(สพบ.)

สหภาพแรงงานรัฐวิสาหกิจองค์การขนส่งมวลชนกรุงเทพ

- เพื่อโปรดทราบ และแจ้งพนักงานในสังกัดเพื่อทราบด้วย

(นางสาวอัญชลี กังวาล)

ห.ธก.(สบจ.)

๓๑ พ.ค. ๖๕

BMTA

องค์การขนส่งมวลชนกรุงเทพ

นโยบายและแนวปฏิบัติในการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
องค์การขนส่งมวลชนกรุงเทพ

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้องกับภารกิจขององค์การขนส่งมวลชนกรุงเทพ จึงจำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์เพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ นั้น

เพื่อให้การบริหารจัดการระบบความมั่นคงปลอดภัยไซเบอร์ สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความน่าเชื่อถือได้และให้บริการได้อย่างต่อเนื่อง สามารถป้องกันภัยคุกคามไซเบอร์ซึ่งอาจก่อนให้เกิดความเสียหายแก่องค์การขนส่งมวลชนกรุงเทพ จึงประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า "ประกาศองค์การขนส่งมวลชนกรุงเทพ เรื่อง นโยบายการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์"

ข้อ ๒ ในประกาศนี้

(๑) "ขสมก." หมายความว่า องค์การขนส่งมวลชนกรุงเทพ

(๒) "ผู้บริหารระดับสูงสุด" หมายความว่า ผู้อำนวยการองค์การขนส่งมวลชนกรุงเทพ

(๓) "ผู้บริหารเทคโนโลยีสารสนเทศ" หมายความว่า รองผู้อำนวยการฝ่ายบริหาร หรือผู้ซึ่งได้รับมอบหมายให้รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ ขสมก.

(๔) "คณะกรรมการ" หมายความว่า คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ ขสมก.

(๕) "นโยบาย" หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่เป็นไปตามพระราชบัญญัติที่เกี่ยวข้อง ดังนี้

ก. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม

ข. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ค. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ง. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

จ. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

(๖) "แนวปฏิบัติ" หมายความว่า ขั้นตอน วิธีการหรือข้อกำหนดให้ผู้ใช้งาน (User) และผู้ดูแลระบบ (Administrator) รวมทั้งบุคคลภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ขสมก. ได้ถือปฏิบัติตามนโยบาย ข้อ ๒ (๕)

(๗) "เจ้าของระบบ" (System Owner) หมายความว่า สำนัก/กอง/กลุ่ม/กลุ่มงาน/ศูนย์ ที่เป็นเจ้าของระบบคอมพิวเตอร์ หรือ ระบบสารสนเทศ

(๘) "ผู้ดูแลระบบ" (System Administrator) หมายความว่า บุคลากร ขสมก. ผู้ซึ่งได้รับมอบหมายจากเจ้าของระบบ (System Owner) หรือจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และการบริหารจัดการระบบเทคโนโลยีสารสนเทศ ขสมก.

(๙) "ผู้ใช้งาน" (User) หมายความว่า บุคลากร ขสมก. ทุกระดับ ซึ่งเป็น พนักงาน ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานจ้างเหมาและบุคคลภายนอก ที่ได้รับอนุญาตให้ใช้ระบบเทคโนโลยีสารสนเทศ ขสมก.

(๑๐) "สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ขสมก.

(๑๑) "สินทรัพย์" (asset) หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งอื่นใดก็ตามที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของ ขสมก. ประกอบด้วย

ก. ฮาร์ดแวร์ (Hardware) หมายความว่า อุปกรณ์คุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้

i. เครื่องคอมพิวเตอร์แม่ข่าย (Server) ทั้งแบบเครื่องแม่ข่ายปกติ (Rack Server) และเครื่องแม่ข่ายแบบชุด (Blade Server)

ii. เครื่องคอมพิวเตอร์ลูกข่าย (Client) ได้แก่ เครื่องคอมพิวเตอร์ (PC) และคอมพิวเตอร์พกพา (Laptop)

iii. เครื่องพิมพ์ (Printer/Scanner) และอุปกรณ์สำรองข้อมูลของ ขสมก.

iv. อุปกรณ์โครงข่าย (Network) หรืออุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) หรืออุปกรณ์สำหรับเชื่อมต่อระบบสื่อสาร (Router, Switch, Access Point) หรืออุปกรณ์จัดเก็บบันทึกการใช้งาน (Log File)

ข. โปรแกรมประยุกต์หรือแอปพลิเคชัน (Program or Application) หมายความว่า ระบบคุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้ ระบบ, System Software,

Database, Software, Software Tool และ Application Software ที่ใช้งานร่วมกับอุปกรณ์ฮาร์ดแวร์

(๑๒) "ศูนย์ข้อมูลและสารสนเทศ" หมายความว่า พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะเพื่อติดตั้งอุปกรณ์ในการประมวลผลข้อมูล (Process Devices) ระบบเครือข่ายคอมพิวเตอร์ ระบบจัดเก็บข้อมูล ระบบรักษาความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศและระบบป้องกันอัคคีภัย ซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์ ระบบข้อมูลและระบบสารสนเทศแก้ผู้ใช้งาน ประกอบด้วย

ก. "ศูนย์ข้อมูล" (Data Center) หมายความว่า ศูนย์ข้อมูลและสารสนเทศของ ขสมก. ตั้งอยู่ที่ 131 ถนนวัฒนธรรม ห้วยขวาง กทม. 10310

ข. "ศูนย์สำรองข้อมูล" (DR Site: Disaster Recovery Site) หมายความว่า ศูนย์สำรองข้อมูลของ ขสมก. ตั้งอยู่ที่ 131 ถนนวัฒนธรรม ห้วยขวาง กทม. 10310

(๑๓) "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

(๑๔) "ความมั่นคงปลอดภัยด้านสารสนเทศ" (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (Reliability)

(๑๕) "เหตุการด้านความมั่นคงปลอดภัย" (Information Security Event) หมายความว่ากรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๖) "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๓ ขสมก. ได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยไซเบอร์และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร ตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๔ นโยบายสนการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

(๑) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบ

(๒) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติฯ ดังกล่าวให้ชัดเจน

(๓) ต้องทบทวนและปรับปรุงนโยบาย อย่างน้อย ปีละ ๑ ครั้ง

ข้อ ๕ ขสมก. ได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งได้กำหนดให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเป็นผู้กำกับ ดูแล และติดตามผู้ใช้งาน (User) ปฏิบัติตามโนยบายและแนวปฏิบัติดังกล่าวอย่างชัดเจน ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้ระบบสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

(๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๓) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

(๔) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๕) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

(๗) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ (Data Recovery)

(๘) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment and Risk Management)

(๙) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

ข้อ ๖ ขสมก. ได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ผู้ที่เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติด้วยวิธีการใดวิธีการหนึ่ง ให้ผู้ใช้งาน (User) และบุคคลภายนอกทราบ เพื่อให้สามารถเข้าใจ เข้าถึง และปฏิบัติตามด้วยหนังสือเวียนภายในองค์กร ระบบ เครือข่ายภายใน (Intranet) หนังสือเวียนอิเล็กทรอสิกส์ หรือเว็บไซต์ภายในและภายนอก ขสมก.

ข้อ ๗ หน่วยงานภายใน ขสมก. ที่ต้องบริหารจัดการระบบเทคโนโลยีสารสนเทศ สามารถกำหนดแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานได้เอง ทั้งนี้ต้องให้สอดคล้องกับ “ประกาศองค์การขนส่งมวลชนกรุงเทพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๔”

ข้อ ๘ หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของ ขสมก. เกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ ต้องรายงานต่อผู้บริหารเทคโนโลยีสารสนเทศสั่งการตรวจสอบผู้ละเลยที่ก่อนให้เกิดความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของ ขสมก. เพื่อรายงานต่อผู้บริหารระดับสูงสุด

ข้อ ๙ ขสมก. กำหนดให้ผู้บริหารระดับสูงสุด เป็นผู้รับผิดชอบในการบริหารความเสี่ยง ควบคุมความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขสมก.

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๔
องค์การขนส่งมวลชนกรุงเทพ

หมวดที่ ๑
การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control)

วัตถุประสงค์

เพื่อให้บุคลากรองค์การขนส่งมวลชนกรุงเทพ และบุคคลภายนอก ให้มีความรู้ ความเข้าใจและสามารถปฏิบัติตามแนวทางปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control) พร้อมทั้งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ นโยบายบุคลากรองค์การขนส่งมวลชนกรุงเทพ และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุน การรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูล ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้

๑.๑. การเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ต้องสอดคล้อง และเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติหน้าที่และคำสั่งมอบอำนาจ

๑.๒. เจ้าของระบบมีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน

๑.๓. ผู้ดูแลระบบมีหน้าที่กำหนดสิทธิ์ให้แก่ผู้ใช้งานตามที่เจ้าของระบบอนุมัติ

๑.๔. ผู้ดูแลระบบมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน สำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๕. ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

๑.๖. เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ ต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากเจ้าของระบบ และต้องรักษาความลับขององค์การขนส่งมวลชนกรุงเทพ ในกรณีที่เกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

๑.๗. การเข้าถึงห้องศูนย์ข้อมูล (Data Center) ให้ดำเนินการ ดังนี้

๑.๗.๑. สำนักเทคโนโลยีสารสนเทศต้องกำหนดข้อปฏิบัติสำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center)

๑.๗.๒. การติดตั้ง ซ่อมเซม และนำอุปกรณ์ใด ๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๑.๗.๓. ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับอนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)

๑.๗.๔. ห้ามนำอาหาร เครื่องดื่ม เข้ามาในห้องศูนย์ข้อมูล (Data Center)

๑.๗.๕. ห้ามถ่ายรูป อุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ก่อนได้รับอนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)

๒. การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนด ดังนี้

๒.๑. สิทธิของผู้ใช้งาน (User) ประกอบด้วย

๒.๑.๑. อ่านอย่างเดียว

๒.๑.๒. สร้างข้อมูล

๒.๑.๓. แก้ไขข้อมูล

๒.๑.๔. ลบข้อมูล

๒.๒. สิทธิผู้ดูแลระบบ (Administrator)กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การกำหนดประเภทของข้อมูล ลำดับความสำคัญ ลำดับชั้นความลับ รวมถึงระดับชั้น การเข้าถึง เวลาที่เข้าถึง และช่องทางการเข้าถึง ดังนี้

๓.๑. ประเภทของข้อมูล แบ่งเป็น ๓ ประเภท อังนี้

๓.๑.๑. ข้อมูลสารสนเทศสำหรับการบริหาร

๓.๑.๒. ข้อมูลสารสนเทศสำหรับการสนับสนุนการปฏิบัติงาน

๓.๑.๓. ข้อมูลสารสนเทศสำหรับการเผยแพร่แก่ประชาชนทั่วไปและผู้ที่สนใจ

๓.๒. ลำดับความสำคัญของข้อมูล แบ่งเป็น ๓ ระดับ ดังนี้

๓.๒.๑. สำคัญมากที่สุด

๓.๒.๒. สำคัญมาก

๓.๒.๓. ปกติ

๓.๓. ลำดับชั้นความลับของข้อมูล แบ่งเป็น ๔ ระดับ ดังนี้

๓.๓.๑. ลับที่สุด ความลับที่มีความสำคัญที่สุด เกี่ยวกับข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหากความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายหรือเป็นภยันตรายต่อความมั่นคงความปลอดภัย หรือความสงบเรียบร้อยของประเทศชาติหรือพันธมิตร หรือการดำเนินงานของหน่วยงานที่เกี่ยวข้องอย่างร้ายแรงที่สุด

๓.๓.๒. ลับมาก ความลับที่มีความสำคัญมาก เกี่ยวกับข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหากความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือเป็นภยันตรายต่อความมั่นคงความปลอดภัยของประเทศชาติหรือพันธมิตร หรือความสงบเรียบร้อยภายในราชอาณาจักร หรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้องได้อย่างร้ายแรง

๓.๓.๓. ลับ ความลับที่มีความสำคัญเกียวกับ ข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหากความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายหรือเป็นภยันตราย หรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้องได้

๓.๓.๔. ปกปิด ความลับซึ่งไม่พึ่งเปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบ โดยสงวนไว้ให้ทราบเฉพาะบุคคลที่มีหน้าที่ต้องทราบเพื่อประโยชน์ในการปฏิบัติภารกิจองค์กรเท่านั้น

๓.๔. ระดับชั้นการเข้าถึง แบ่งเป็น ๓ ระดับ ดังนี้

๓.๔.๑. กลุ่มผู้บริหาร

๓.๔.๒. กลุ่มผู้ปฏิบัติงาน

๓.๔.๓. กลุ่มประชาชนทั่วไปและผู้ที่สนใจ

๓.๕. เวลาที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถเข้าถึงได้ตลอด ๒๔ x ๗ วัน

๓.๖. ช่องทางการเข้าถึงสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ได้ ๒ ช่องทาง ดังนี้

๓.๖.๑. ระบบเครือข่ายภายใน (Intranet)

๓.๖.๒. ระบบเครือข่ายภายนอก (Internet)

๔. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Business Requirements For Access Control) ดังนี้

๔.๑. เจ้าของระบบอนุมัติสิทธิให้ผู้ใช้งาน ตามภารกิจเพื่อให้สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ เฉพาะในส่วนที่ได้รับมอบหมาย ตามความเป็นจำในการใช้งาน

๔.๒. ผู้ดูแลระบบกำหนดสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งานตามที่เจ้าของระบบอนุมัติ

หมวดที่ ๒
การบริหารจัดการเข้าถึงของผู้ใช้งาน
(User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งานที่ได้รับอนุญาตแล้วและสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยไซเบอร์และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนบุคลากรใหม่ (User Registration) เพื่อรับสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

๒. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อไม่ได้ปฏิบัติงานที่องค์การขนส่งมวลชนกรุงเทพ

๓. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการควบคุมจำกัด และเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้

๑.๑. ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ อย่างน้อยประกอบด้วยชื่อ นามสกุล ตำแหน่ง สังกัด และหมายเลขโทรศัพท์

๑.๒. การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

๑.๒.๑. กรณีบุคลากรองค์การขนส่งมวลชนกรุงเทพ

(๑) ให้บุคลากรกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๒) ให้หน่วยงานส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้เจ้าของระบบที่ขอใช้งาน

(๓) ให้เจ้าของระบบอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิ ตามที่เจ้าของระบบอนุมัติ พร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๒.๒. กรณีบุคคลภายนอก

(๑) ให้บุคคลภายนอกกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมระบุเหตุผลในการเข้าใช้งาน หรือหนังสือขอเข้าใช้งานจากบริษัท/หน่วยงานต้นสังกัด

(๒) ให้หน่วยงานพิจารณาเหตุผล และดำเนินการส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้เจ้าของระบบที่ขอใช้งาน

(๓) ให้เจ้าของระบบอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิตามที่เจ้าของระบบ อนุมัติพร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๓. การสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๑.๓.๑. การสร้างบัญชีผู้ใช้งาน (Username) ให้เจ้าของระบบ กำหนด เช่น ชื่อภาษาอังกฤษหรือบัตรประจำตัวประชาชนตามด้วยเครื่องหมาย “_” หรือ “.” ตามด้วยอักษรนามสกุลตัวแรก หรือลักษณะอื่นใดตามที่เจ้าของระบบ ที่มีการตกลงร่วมกัน

๑.๓.๒. การกำหนดรหัสผ่าน (Password) ชุดของตัวอักษรภาษาอังกฤษ ตัวเลข และอักขระพิเศษ อย่างน้อย ๘ ตัวขึ้นไป และยากต่อการคาดเดา

๑.๓.๓. ให้ผู้ดูแลระบบ แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ผู้ใช้งาน ทราบโดยตรง

๑.๓.๔. เมื่อผู้ใช้งาน มีการเปลี่ยนข้อมูลให้แจ้งเจ้าของระบบ เพื่อปรับปรุงข้อมูลผู้ใช้งาน

๒. การยกเลิกสิทธิการใช้งานของบุคลากร หรือบุคคลภายนอกให้ดำเนินการ ดังนี้

๒.๑. ให้หน่วยงานแจ้งเจ้าของระบบ เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก ให้โอน หรือสิ้นสุดการจ้าง

๒.๒. ผู้ดูแลระบบ จะดำเนินการปิดบัญชีผู้ใช้งาน (Username) และแจ้งกลับไปยังหน่วยงานรับทราบ

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้ใช้งาน ให้ดำเนินการ ดังนี้

๓.๑. ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้หน่วยงานแจ้งเจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๓.๒. ในกรณีที่ผู้ใช้งาน ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สูงกว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อเจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการ ตามหลักเกณฑ์ ดังนี้

๔.๑. ในกรณีที่ผู้ใช้งาน ลืมรหัสผ่าน (Password) ให้ขอรับรหัสผ่านใหม่ วิธีการของเจ้าของระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนด เช่น โทรศัพท์ หรือ ออนไลน์

๔.๒. ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๑ ปี และรหัสผ่าน (Password) ใหม่ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

๕. ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสุดสิ้นการจ้าง เพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่คณะกรรมการกำหนด

หมวดที่ ๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลับลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

๑. กำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)

๒. กำหนดแนวปฏิบัติในการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) ดูแล

๓. กำหนดแนวปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ได้แก่ เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศเพื่อไม่ให้สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งาน (User) ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔. กำหนดให้ผู้ใช้งาน (User) อาจนำการ์ดเข้ารหัสข้อมูล (Encryption) มาใช้กับการรับส่งข้อมูล ที่สำคัญหรือข้อมูลที่เป็นความลับขององค์การขนส่งมวลชนกรุงเทพ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

แนวปฏิบัติ

๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้

๑.๑. ผู้ใช้งานต้องกำหนดรหัสผ่าน (Password) ตามหมวดที่ ๒ ข้อ ๑.๓ และต้องเปลี่ยนรหัสผ่านตาม ข้อ ๔.๒.

๑.๒. ผู้ใช้งานต้องไม่ใช้รหัสผ่าน (Password) ร่วมกับบุคคลอื่น และไม่ควรให้ระบบคอมพิวเตอร์หรือระบบสารสนเทศจำรหัสผ่าน (Password) ในการเข้าใช้งานโดยอัตโนมัติ

๑.๓. ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่าน (Password) สำหรับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเก็บเป็นความลับเสมือนเป็นสมบัติส่วนตัว ห้ามจดหรือเขียนรหัสผ่าน (Password) ที่ใช้งานไว้ในที่เปิดเผย

๑.๔. หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็น ในการเข้าถึงหลังจากดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

๑.๕. หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของบัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดแล้ว

๒. ผู้ใช้งานต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๓.๑. ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ในการประมวลผลข้อมูล (Process Device) มีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานขององค์การขนส่งมวลชนกรุงเทพเท่านั้น

๓.๒. ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ (Asset) ขององค์การขนส่งมวลชนกรุงเทพ และให้ใช้งานด้วยความระมัดระวังเสมือนเป็นทรัพย์สินส่วนตน

๓.๓. ผู้ใช้งานต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใด ๆ ที่เครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์พกพา หรือระบบคอมพิวเตอร์และระบบสารสนเทศ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลต่อผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัด

๓.๔. ผู้ใช้งานต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา หรือการ์ดความจำในโทรศัพท์มือถือ เพื่อป้องกันการรั่วไหลของข้อมูล

๓.๕. บุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานด้านสารสนเทศ ต้องขออนุมัติเป็นลายลักษณ์อักษรก่อนเข้าปฏิบัติงาน

๓.๖. การทำลายอุปกรณ์บันทึกข้อมูลหรือการนำอุปกรณ์บันทึกข้อมูลกลับมาใช้งานใหม่ให้ดำเนินการ ดังนี้

๓.๖.๑. การทำลายอุปกรณ์บันทึกข้อมูล เช่น Flash Drive CD/DVD ฮาร์ดดิสก์ เทป เป็นต้น ให้ใช้วิธีการทุบ หรือบดให้เสียหาย หรือเผาทำลายด้วยวิธีการทำลายตามมาตรฐานสากล หรือตามที่คณะกรรมการกำหนด

๓.๖.๒. การนำอุปกรณ์บันทึกข้อมูลไปใช้งานใหม่ ให้ฟอร์แมต (Format) อุปกรณ์บันทึกข้อมูลนั้นโดยใช้วิธีการฟอร์แมต (Format) ตามมาตรฐานสากล หรือตามที่คณะกรรมการกำหนด

หมวดที่ ๔
การควบคุมการเข้าถึงเครือข่าย
(Network Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายให้มีความมั่นคงปลอดภัย

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึง

๒. กำหนดแนวปฏิบัติในการยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาต ให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถใช้งานเครือข่าย ระบบคอมพิวเตอร์และระบบสารสนเทศขององค์การขนส่งมวลชนกรุงเทพได้

๓. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดยต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๔. กำหนดแนวปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) โดยต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕. กำหนดแนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

๖. กำหนดแนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศและการส่งข้อมูลสารสนเทศสอดคล้องกับแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

๑. การเข้าถึงเครือข่ายของผู้ใช้งาน

๑.๑. การใช้งานระบบเครือข่ายภายนอก (internet) ให้ดำเนินการ ดังนี้

๑.๑.๑. กำหนดให้ใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองสำหรับเข้าใช้งานระบบเครือข่ายภายนอก (Internet)

๑.๑.๒. ห้ามใช้งานระบบเครือข่ายภายนอก (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) สูงที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ ได้แก่ รายการบันเทิงต่าง ๆ ในเวลาทำการ

๑.๑.๓. ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดศิลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์เสื่อมเสีย

๑.๑.๔. ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับขององค์การขนส่งมวลชนกรุงเทพเว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๕. ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเคร่งครัด

๑.๑.๖. ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่าง ๆ เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ โดยแจ้งให้ผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัดทราบก่อนติดตั้งใช้งาน

๑.๒. การใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) โดเมนเนม (Domain Name) ขององค์การขนส่งมวลชนกรุงเทพ (@bmta.co.th) ให้ดำเนินการดังนี้

๑.๒.๑. ห้ามใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ในทางที่ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศิลธรรม

๑.๒.๒. ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจด้วยการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ส่งโดยโดเมนเนม (Domain Name) ขององค์การขนส่งมวลชนกรุงเทพ

๑.๒.๓. ต้องตรวจสอบชื่อผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender) ก่อนเปิดจดหมายอิเล็กทรอนิกส์ (E-Mail) เพื่อป้องกันการเปิดไฟล์อันตรายที่อาจมีไวรัสคอมพิวเตอร์ โดยเฉพาะ Executable File ได้แก่ ไฟล์ที่มีนามสกุล .exe, .com, .bat และ .inf ที่อาจนำสู่ระบบเครือข่ายองค์การขนส่งมวลชนกรุงเทพ

๑.๒.๔. หลังกจาใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องออกจากระบบ (Log Out) ทันที

๑.๓. การใช้งานเครือข่ายไร้สาย (WiFi) ให้ดำเนินการ ดังนี้

๑.๓.๑. ผู้ดูแลระบบต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดเป็นค่ามาตรฐานมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้งเพื่อใช้งาน

๑.๓.๒. ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (WiFi)

๑.๓.๓. ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็นทรัพย์สินขององค์การขนส่งมวลชนกรุงเทพไปใช้งานเครือข่ายไร้สาย (WiFi) ที่ไม่น่าเชื่อถือ

๑.๓.๔. ผู้ใช้งานไม่ควรทำธุรกรรมทางการเงินอิเล็กทรอนิกส์ระหว่างการใช้งานเครือข่ายไร้สาย (WiFi) เนื่องจากอาจเกิดความไม่ปลอดภัยและอาจขาดการเชื่อมต่อของสัญญาณ

๑.๓.๕. ห้ามผู้ใช้งานติดตั้งและเปิดการทำงานโปรแกรมดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายขององค์การขนส่งมวลชนกรุงเทพ และมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

๑.๔.๑. การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ภายใต้หน่วยงานขององค์การขนส่งมวลชนกรุงเทพ ควรนำเสนอเกี่ยวกับภารกิจของหน่วยงาน เช่น ผลการดำเนินงานและข่าวสาร โดยการนำเข้าข้อมูลต้องเป็นผู้ที่ได้รับมอบหมายจากหน่วยงานและต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๔.๒. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับขององค์การขนส่งมวลชนกรุงเทพผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าข้องข้อมูล

๑.๔.๓. กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงต่อไป

๑.๔.๔. ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากองค์การขนส่งมวลชนกรุงเทพ และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑.๔.๕. หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งานต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทัน

๒. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ให้ดำเนินการ ดังนี้

๒.๑. ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องจัดทำผังระบบเครือข่าย (Network Diagram) พร้อมรายละเอียดอุปกรณ์บนเครือข่ายที่เห็นว่าจำเป็นต่อการใช้งาน ได้แก่ กลุ่มอุปกรณ์ เลขที่อยู่ไอพ (IP Address) และหมายเลขเฉพาะอุปกรณ์ (MAC Address) โดยให้ปรับปรุงทุก ๒ ปี หรือตามความเหมาะสม

๒.๒. การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ มาใช้งานบนเครือข่ายต้องได้รับอนุญาตจากผู้รับผิดชอบด้านสารสนเทศของหน่วยงาน

๓. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) ให้ดำเนินการ ดังนี้

๓.๑. สำนักเทคโนโลยีสารสนเทศดูแล/ตรวจสอบ พอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) รวมทั้งการควบคุมการเข้าถึงพอร์ตทางกายภาพและเครือข่าย

๓.๒. สำนักเทคโนโลยีสารสนเทศต้องเปิดใช้งานเฉพาะพอร์ตที่จำเป็นสำหรับการใช้งานเท่านั้น และต้องตรวจสอบพอร์ตที่เปิดให้บริการ อย่างน้อยปีละ ๑ ครั้ง

๔. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้ดำเนินการ ดังนี้

๔.๑. สำนักเทคโนโลยีสารสนเทศต้องติดตั้งระบบป้องกันการบุกรุกโจมตีทางเครือข่าย (Firewall) เพื่อใช้เป็นจุดควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๔.๒. ผู้ดูแลระบบต้องไม่เปิดเผยข้อมูลการเชื่อมต่อทางเครือข่าย ก่อนได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศ

๔.๓. ผู้ดูแลระบบมีหน้าที่ในการควบคุมการเชื่อมต่อสัญญาณหรือยกเลิก การเชื่อมต่อสัญญาณตามที่ได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศ ทั้งนี้ หากพบข้อผิดพลาดหรือเห็นว่า หมดความจำเป็นในการเชื่อมต่อสัญญาณให้รายงานสำนักเทคโนโลยีสารสนเทศทันที

๔.๔. การเชื่อมต่อเครือข่ายสารสนเทศระหว่างองค์การขนส่งมวลชนกรุงเทพกับหน่วยงานภายนอกต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศ และเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ของผู้ให้บริการที่มีความน่าเชื่อถือ

๕. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ให้ดำเนินการ ดังนี้

๕.๑. ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ และการรับ-ส่งหรือการไหลเวียนของข้อมูลหรือสารสนเทศเป็นไปอย่างรวดเร็ว

๕.๒. ผู้ดูแลระบบต้องเก็บข้อมูลค่าจราจรคอมพิวเตอร์ (Log File) ของผู้ใช้งานเป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน ความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

หมวดที่ ๕
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการโดยต้องมีการควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวตนที่ปลอดภัย

๒. กำหนดแนวปฏิบัติใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการ ความมั่นคงปลอดภัยที่ได้กำหนดไว้

แนวปฏิบัติ

๑. ผู้ใช้งานต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าถึงระบบปฏิบัติการ

๒. ผู้ใช้งานไม่มีสิทธิ์เปลี่ยนแปลงแก้ไขค่าต่าง ๆ ของระบบปฏิบัติการ เช่น

๒.๑. Product Key หรือ License ของระบบปฏิบัติการ

๒.๒. ค่าคอนฟิกกูเรชัน (Configuration) ต่าง ๆ เช่น Computer Name, IP Address เป็นต้น

๓. การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) กำหนด ดังนี้

๓.๑. ผู้ใช้งานต้องไม่ดัดแปลงหรือติดตั้งโปรแกรมอรรถประโยชน์ใด ๆ บนระบบปฏิบัติการทั้งนี้ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์ต่อผู้รับผิดชอบด้านสารสนเทศของหน่วยงาน

๓.๒. การใช้งานโปรแกรมอรรถประโยชน์อื่น ๆ นอกเหนือจากที่ติดตั้งมากับระบบปฏิบัติการ เช่น โปรแกรมดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทพดักจับรหัสผ่าน (Password Sniffer) และโปรแกรม Formatter กำหนดให้ผู้ดูแลระบบหรือ(ที่ได้รับมอบหมายเท่านั้นที่มีสิทธิใช้งาน

หมวดที่ ๖
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
(Application and Information Access Control)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control) โดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อองค์การขนส่งมวลชนกรุงเทพ โดยต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)

๒. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศจากความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๓. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) โดยต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกสำนักงาน

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการดังนี้

๑.๑. ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งานที่เข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศผ่านเครือข่ายภายนอก ให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN)

๑.๒. การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) รายละเอียดปรากฏตามภาคผนวก.

๒. ระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์การขนส่งมวลชนกรุงเทพให้ดำเนินการ ดังนี้

๒.๑. ระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ดังนี้

๒.๑.๑. ระบบการบริหารจัดการความมั่นคงปลอดภัยและเครือข่าย ได้แก่ ระบบ Antivirus ระบบ Backup System ระบบ Domain Name Server ระบบ Dynamic Host Configuration Protocol ระบบ Network Management ระบบ Network Monitoring และระบบจัดเก็บข้อมูลกลาง

๒.๒ ระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อองค์การขนส่งมวลชนกรุงเทพ ต้องได้รับการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกออกจากระบบอื่น ๆ

๒.๓. ผู้ดูแลระบบต้องแบ่งพื้นที่สำหรับการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายตามระดับความสำคัญและความปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์การขนส่งมวลชนกรุงเทพ เพื่อควบคุมสภาพแวดล้อมโดยเฉพาะ

๒.๔. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking) เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องเข้าถึงในสถานที่ที่มีความปลอดภัยและต้องได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศ

๓. การควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ให้ดำเนินการ ดังนี้

๓.๑. อุปกรณ์สื่อสารเคลื่อนที่ ได้แก่ Smart Phone และ Tablet ต้องได้รับการยืนยันตัวตัน โดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของผู้ใช้งานสำหรับการเข้าใช้งาน

๔. การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) กำหนด ดังนี้

๔.๑. ผู้ใช้งานต้องปฏิบัติตามหมวด ๖ แนวปฏิบัติ ข้อ ๑ การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

๔.๒. เมื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศแล้ว ผู้ใช้งานต้องระมัดระวังไมให้ผู้ไม่มีส่วนเกี่ยวข้องเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ สื่อสารเคลื่อนที่ได้และต้องออกจากระบบ (Log Out) ทันทีเมื่อปฏิบัติเลิกใช้งาน

หมวดที่ ๗
การจัดทำระบบสำรองของระบบสารสนเทศ
(Disaster Recovery Site)

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศและการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมฉุกเฉิน และการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่องแม้ในสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่าง ๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสมและสามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง

นโยบาย

๑. พิจารณาคัดเลือกระบบสารสนเทศที่หมาะสมในการจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน

๒. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ เพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ

แนวปฏิบัติ

๑. ผู้ดูแลระบบจะต้องจัดทำการสำรองของระบบสารสนเทศโดยมีขั้นตอน ดังนี้

๑.๑. ผู้ดูแลระบบจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูล และการกู้คืนข้อมูลสารสนเทศ

๑.๒. กำหนดรูปการสำรองข้อมูลระบบสารสนเทศ ดังนี้

๑.๒.๑. คัดเลือกระบบสารสนเทศในการสำรองข้อมูล

๑.๒.๒. กำหนดรูปแบบการสำรองข้อมูล เช่น เฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) แบบสมบูรณ์ (Full Backup)

๑.๒.๓. กำหนดความถี่ในการสำรองข้อมูลตามความเหมาะสมของระบบสารสนเทศ

๑.๓. ผู้ดูแลระบบดำเนินการสำรองของระบบสารสนเทศ ตามข้อที่ ๑.๒.

๒. ผู้ดูแลระบบต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศที่สำรองไว้ อย่างน้อย ๑ ระบบ โดยอย่างน้อยปีละ ๑ ครั้ง

๓. สำนักเทคโนโลยีสารสนเทศดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศขององค์การขนส่งมวลชนกรุงเทพ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่องโดยกำหนดให้ปรับปรุงแผนดังกล่าวทุก ๑ ปี

๔. มีการทบทวนระบบสารสนเทศในการระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๘
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Risk Assessment and Risk Management)

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยด้านสารสนเทศ ทำให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนด มีความมั่นคงปลอดภัยและหน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

นโยบาย

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

แนวปฏิบัติ

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒. กำหนดให้มีผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๒.๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศประจำปีงบประมาณ ให้ดำเนินการโดยกลุ่มตรวจสอบภายใน (Internal Auditor)

๒.๒. หากมีความประสงค์ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศเชิงเทคนิค ให้ดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๓. กำหนดแนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๓.๑. ผู้ตรวจสอบต้องจัดการทำรายงานพร้อมข้อเสนอแนะในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๒. สำนักเทคโนโลยีสารสนเทศต้องอำนวยความสะดวกแก่ผู้ตรวจสอบในการตรวจสอบข้อมูลที่สำคัญ

๓.๓. ในกรณีที่ผู้ตรวจสอบจำเป็นต้องเข้าถึงข้อมูลสำคัญให้สำนักเทคโนโลยีสารสนเทศ สร้างสำเนาสำหรับข้อมูลนั้น โดยให้ผู้ตรวจสอบใช้งานและทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือหากประสงค์จัดเก็บข้อมูลนั้นเป็นหลักฐานให้แจ้งสำนักเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๓.๔. ในกรณีการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบประเมินความเสี่ยงระบบคอมพิวเตอร์และระบบสารสนทศ ให้แยกการติดตั้งเครื่องมือออกจากระบบที่ให้บริการจริง หรือระบบที่ใช้ในการพัฒนาและกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว (Read Only)

๓.๕. ผู้ตรวจสอบต้องแจ้งความเสี่ยงและระบุความรุนแรงของเครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยง

หมวดที่ ๙
การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
(Information Security Incident Management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพในช่วงระยะเวลาที่เหมาะสม

แนวทางปฏิบัติ

๑. จัดให้มีขั้นตอนหรือกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศที่สำคัญ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถ และประสบการณ์ โดยขั้นมีการกำหนดขั้นตอนและกระบวนการดังต่อไปนี้

๑.๑ การกำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร

๑.๒ การประเมินเหตุการณ์หรือจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ และพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

๑.๓ จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ และรายงานเหตุการณ์ ผู้ที่เกี่ยวข้องให้ทราบและดำเนินการต่อไป

๑.๔ การดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติ

๑.๕ วิเคราะห์ รวบรวมและรายงานเหตุการณ์ต่อผู้บังคับบัญชาทราบ ทั้งนี้ เพื่อระบุถึงสาเหตุและเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต

๒. ต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ ผ่านบุคคล หรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) โดยให้ดำเนินการดังนี้

๒.๑ แจ้งผู้บังคับบัญชา โดยช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ เช่น Social Network, E-mail เป็นต้น ทั้งนี้ เนื้อหาขั้นต่ำ ต้องประกอบด้วย วันเวลา เหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น

๒.๒ รายงานผู้บังคับบัญชาเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น

- การบุกรุกด้านกายภาพ

- การปฏิบัติงานที่ไม่เป็นไปตามโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

- การเปลี่ยนแปลง การเข้าถึงโดยไม่ได้รับอนุญาต

- การทำงานผิดของโปรแกรมและอุปกรณ์คอมพิวเตอร์ หรือการปฏิบัติงาน

จัดให้มีบุคคลหรือหน่วยงานงาน (point of contact) เพื่อทำหน้าที่รายงานเหตุการณ์ที่เกิดขึ้นต่อผู้บังคับบัญชา โดยให้รายงานดังต่อไปนี้

รายงานทันทีเมื่อเกิดเหตุ	ระหว่างดำเนินการแก้ไข	แก้ไขปัญหาได้ และเหตุยุติ
1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้นชื่อผู้ติดต่อ/ประสานงานของบริษัทเพื่อให้ข้อมูล	1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น 4. ดำเนินการแก้ไขปัญหาและระยะเวลาในการแก้ไข 5. ความคืบหน้าในการแก้ไขปัญหา	1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้นโดยประเมินมูลค่าความเสียหายที่อาจเกิดขึ้น 4. ดำเนินการแก้ไขปัญหา 5. ผลการแก้ไขปัญหา และระยะเวลาในการแก้ไข 6. แนวทางป้องกันในอนาคตและการเก็บรวบรวมหลักฐาน เพื่อระบุสาเหตุและแนวทางแก้ไขต่อไป

รายงานทันทีเมื่อเกิดเหตุ

คือการรายงานโดยไม่ชักช้า อาจแจ้งด้วยวาจาหรือช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ เมื่อทราบเหตุการณ์และตรวจสอบในเบื้องต้นแล้ว

ระหว่างดำเนินการแก้ไข

คือการรายงานโดยไม่ชักช้า อาจแจ้งด้วยวาจาหรือช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ เมื่อหราบเหตุการณ์และตรวจสอบในเบื้องต้นแล้ว

แก้ไขปัญหาได้ และเหตุยุติ

คือการรายงานเป็นลายลักษณ์อักษรโดยมีเนื้อหาจากข้อมูลข้างต้น

ภาคผนวก

การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนทศของผู้รับจ้าง (Outsource)

เพื่อให้ระบบคอมหิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศ ศูนย์ข้อมูลและสารสนเทศ และพื้นที่ปฏิบัติงานทั่วไป ซึ่งเป็นทรัพย์สินที่มีค่าขององค์การขนส่งมวลชนกรุงเทพมีความปลอดภัยต่อการถูกบุกรุกโจมตี และลดความเสี่ยงต่อลักลอบเปิดเผยข้อมูลสารสนเทศ จึงกำหนดแนวปฏิบัติการควบคุมการเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศของผู้รับจ้าง (Outsource) ดังนี้

๑. ก่อนปฏิบัติงาน

๑.๑. ผู้รับจ้าง (Outsource) ต้องขออนุญาตหัวหน้าส่วนงานนั้น ๆ เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคคลภายนอก ตามหมวดที่ ๒ ข้อปฏิบัติที่ ๑

๑.๒. หัวหน้าส่วนงานหรือผู้ที่ได้รับมอบหมายพิจารณาเหตุผลการขออนุญาตดังกล่าวและต้องอนุมัติเป็นลายลักษณ์อักษร

๒. ระหว่างปฏิบัติงาน

๒.๑. ผู้รับจ้าง (Outsource) ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน

๒.๒. ผู้รับผิดชอบด้านสารสนเทศหรือผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนงานต้องกำกับดูแลการปฏิบัติงานของผู้รับจ้าง โดยเฉพาะการติดตั้ง ซ่อมแซม หรือการเปลี่ยนอุปกรณ์ประมวลผลข้อมูล ภายในห้องศูนย์ข้อมูล (Data Center) ต้องกำกับดูแลโดยเคร่งครัด

๒.๓. ผู้รับจ้างต้องปฏิบัติตามหน้าที่ที่ได้รับมอบหมายเท่านั้นและต้องคำนึงถึงการรักษาความลับข้อมูลขององค์การขนส่งมวลชนกรุงเทพเป็นสำคัญ หากเกิดปัญหาระหว่างการปฏิบัติงานให้แจ้งผู้รับผิดชอบด้านสารสนเทศหรือผู้ที่ได้รับมอบหมายที่กำกับดูแลการปฏิบัติงานทันที

๓. หลังปฏิบัติงาน

๓.๑. ให้ผู้รับจ้างแจ้งความประสงค์ต่อผู้รับผิดชอบด้านสารสนเทศเพื่อยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศทันทีเมื่อปฏิบัติงานแล้วเสร็จ

๓.๒. ผู้ดูแลระบบ จะยกเลิกสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ และลบข้อมูลสารสนเทศของผู้รับจ้างเป็นการถาวรทันทีเมื่อสิ้นสุดการจ้างงานหรือข้อตกลงร่วมกัน

๔. การรักษาความลับ

ผู้รับจ้างต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงดังกล่าว ต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

ข้อปฏิบัติการเข้าใช้งานห้องศูนย์ข้อมูล (Data Center)

เพื่อให้การเข้าออกห้องศูนย์ข้อมูล (Data Center) เป็นไปด้วยความสะดวก เรียบร้อย มีความปลอดภัย จึงได้มีการกำหนดข้อปฏิบัติ ดังนี้

๑. บุคคลผู้มีสิทธิเข้าใช้งานห้องศูนย์ข้อมูล (Data Center) ประกอบด้วย

๑.๑. ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) หมายถึง เจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ ให้รับผิดชอบดูแลห้องศูนย์ข้อมูล (Data Center)

๑.๒. เจ้าหน้าที่ผู้รับผิดชอบห้องศูนย์ข้อมูล (Data Center) จากบริษัท หมายถึง เจ้าหน้าที่ของบริษัท ที่ได้รับการผู้รับจ้างในการบำรุงรักษาเครือข่าย ห้องศูนย์ข้อมูล (Data Center) องค์การขนส่งมวลชนกรุงเทพ

๑.๓. บุคคลภายนอก หมายถึง ผู้ที่เข้ามาปฏิบัติงานตามภารกิจ โดยต้องการรับการอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ องค์การขนส่งมวลชนกรุงเทพ

๒. การเข้าใช้งานห้องศูนย์ข้อมูล (Data Center) มีขั้นตอนดังนี้

๒.๑. ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) เข้าใช้งานโดยการสแกนลายนิ้วมือ หรือรหัส การใช้งานของอุปกรณ์เปิด - ปิด ประตู หน้าห้องศูนย์ข้อมูล (Data Center)

๒.๒. เจ้าหน้าที่ผู้รับผิดชอบห้องศูนย์ข้อมูล (Data Center) จากบริษัท เข้าใช้งานโดยการสแกนลายนิ้วมือ หรือรหัส การใช้งานของอุปกรณ์เปิด - ปิด ประตู หน้าห้องศูนย์ข้อมูล (Data Center) โดยได้รับการอนุมัติการนำเข้าลายนิ้วมือจากได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center)

๒.๓. บุคคลภายนอกจะต้องทำเป็นหนังสือขอเข้าพื้นที่เป็นลายลักษณ์อักษรเท่านั้น โดยให้หนังสือจะต้องระบุ วัน เวลา ที่ชัดเจน จำนวน หรือรายชื่อบุคลากร พร้อมด้วยเหตุผลความจำเป็นโดยมีผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) เป็นผู้นำพาเข้าและควบคุมตลอดเวลา

๒.๔. บุคคลภายนอก ต้องลงทะเบียนเซ็นชื่อการเข้าในสมุดหน้าห้องทุกครั้ง และเมื่อเสร็จภารกิจต้องเซ็นชื่อออก ทุกครั้งเช่นกัน

๓. ระยะเวลาการเข้าใช้งานห้องศูนย์ข้อมูล (Data Center) มีรายละเอียด ดังนี้

๓.๑. วันและเวลาราชการ ๘.๓๐ - ๑๖.๓๐ น.

๓.๒. กรณีที่มีเหตุฉุกเฉิน หรือนอกวันและเวลาราชการ ที่มีความจำเป็นต้องเข้าห้องศูนย์ข้อมูล (Data Center) ให้แจ้งได้รับมอบหมายให้ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) ทราบถึงเหตุผลและความจำเป็นในการเข้าไปใช้งาน

๔. ห้ามนำอาหาร เครื่องดื่ม เข้ามาในห้องศูนย์ข้อมูล (Data Center)

๕. ห้ามถ่ายรูป อุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ก่อนได้รับอนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)

๖. เมื่อเสร็จภารกิจให้ตรวจสอบความเรียบร้อยก่อนออกจากศูนย์ข้อมูล (Data Center) เช่น ไฟ ประตู

เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) ชั้น ๔ อาคารองค์การขนส่งมวลชนกรุงเทพ ได้แก่

๑. นายปิยะสิทธิ์ พูลสุข เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ๔

๒. นายประวัติ สุขพันธ์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ๔

ผู้ควบคุม

๑. นายยงยุทธ พันธ์สวัสดิ์ หัวหน้างานปฏิบัติการคอมพิวเตอร์

เบอร์ติดต่อ

๐๒-๒๔๘-๔๐๐๗ ต่อ ๑๔๑๗ – ๑๔๑๘