บริษัท วิทยุการบินแห่งประเทศไทย จำกัด

ที่ ปก ๑๐๑ /๒๕๖๔ ๒๗ กันยายน ๒๕๖๔

ประกาศ

เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

ของบริษัท วิทยุการบินแห่งประเทศไทย จำกัด

โดยที่เป็นการสมควรให้มีประกาศ เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท วิทยุการบินแห่งประเทศไทย จำกัด เพื่อให้การดำเนินการสอดคล้องตามแผนรักษาความปลอดภัยในการบินพลเรือนแห่งชาติ ในเรื่องมาตรฐานการรักษาความปลอดภัยด้านสารสนเทศการบริการการเดินอากาศ และเพื่อให้เป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๙ ที่กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงเพื่อให้เป็นไปตามพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ มาตรา ๕ มาตรา ๖ และมาตรา ๗ ที่กำหนดให้หน่วยงานหรือองค์กร ต้องมีมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

อาศัยอำนาจตามความในข้อ ๘ (๖) และข้อ ๘ (๑๑) แห่งระเบียบบริษัทฯ เรื่อง การกำกับดูแลมาตรฐานและความปลอดภัยบริการการเดินอากาศ พ.ศ. ๒๕๖๒ และมติคณะกรรมการกำกับดูแลมาตรฐานและความปลอดภัยบริการการเดินอากาศ (กมป.) ในคราวประชุมครั้งที่ ๑๒/๒๕๖๔ เมื่อวันที่ ๒๓ กันยายน ๒๕๖๔ เห็นชอบให้มีการบูรณาการระบบสารสนเทศของบริษัทฯ ทุกประเภท จึงให้ยกเลิกประกาศบริษัทฯ ที่ ปก ๘๑/๒๕๖๐ เรื่อง “แนวปฏิบัติการรักษาความปลอดภัยระบบสารสนเทศการบริการการเดินอากาศ (Air Traffic Management System ICT Security Standard Operating Procedures)” ฉบับที่ ๑ (พฤษภาคม ๒๕๖๐) ลงวันที่ ๓๑ พฤษภาคม ๒๕๖๐ ประกาศบริษัทฯ ที่ ปก/รวท ๑๐๑/๒๕๖๐ เรื่อง “วิธีปฏิบัติงานการรักษาความปลอดภัยระบบสารสนเทศการบริการการเดินอากาศ ประเภท CNS/ATM Critical IT Infrastructure” ฉบับที่ ๑ (กรกฎาคม ๒๕๖๐) ลงวันที่ ๖ กรกฎาคม ๒๕๖๐ และประกาศบริษัทฯ ที่ ปก ๑๕๓/๒๕๖๒ เรื่อง “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒” ลงวันที่ ๒ สิงหาคม ๒๕๖๒ โดยกำหนดแนวปฏิบัติเพื่อใช้ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ ไว้ดังต่อไปนี้

๒/ข้อ ๑...

ข้อ ๑ แนวปฏิบัตินี้ เรียกว่า “แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท วิทยุการบินแห่งประเทศไทย จำกัด”

ข้อ ๒ ให้กรรมการผู้อำนวยการใหญ่ เป็นผู้รักษาการตามแนวปฏิบัตินี้ รวมทั้งมีอำนาจตีความ วินิจฉัยปัญหาเกี่ยวกับการปฏิบัติตามแนวปฏิบัติ และประกาศที่ออกโดยอาศัยอำนาจตามแนวปฏิบัตินี้

ข้อ ๓ แนวปฏิบัตินี้ให้ใช้บังคับแก่พนักงาน ลูกจ้าง และหน่วยงานหรือบุคคลภายนอกที่เข้าใช้งานหรือดำเนินการเกี่ยวข้องกับระบบสารสนเทศของบริษัทฯ

ข้อ ๔ ในการปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ ให้ยึดถือและปฏิบัติตามแนวปฏิบัติที่แนบท้ายประกาศนี้

ข้อ ๕ ให้มีการทบทวนแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อเกิดการเปลี่ยนแปลงที่มีผลกระทบต่อระบบสารสนเทศของบริษัทฯ และเผยแพร่แนวปฏิบัตินี้ให้ผู้ใช้งานหรือดำเนินการเกี่ยวข้องกับระบบสารสนเทศของบริษัทฯ ทราบ

ข้อ ๖ กรณีที่ระบบสารสนเทศของบริษัทฯ มีข้อจำกัดในการปฏิบัติตามแนวปฏิบัติฉบับนี้ ให้ผู้ดูแลระบบสารสนเทศที่รับผิดชอบดูแลระบบสารสนเทศดังกล่าว กำหนดวิธีปฏิบัติหรือมาตรการทดแทน และนำเสนอคณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร อนุมัติก่อนประกาศใช้งาน

ข้อ ๗ บุคคลใดจงใจฝ่าฝืนหรือไม่ปฏิบัติตามแนวปฏิบัติ วิธีปฏิบัติ หรือมาตรการต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ จะถือว่าเป็นความผิดทางวินัยและให้ดำเนินการตามข้อบังคับเกี่ยวกับพนักงาน ทั้งนี้ หากการกระทำนั้นเป็นเหตุให้บริษัทฯ ได้รับความเสียหาย ผู้กระทำจะได้รับการพิจารณาดำเนินคดีตามกฎหมายอีกทางหนึ่งด้วย

ทั้งนี้ ให้ถือปฏิบัติตามประกาศตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๔ เป็นต้นไป

จึงประกาศมาเพื่อทราบโดยทั่วกัน

(นายทินกร ชูวงศ์)
รองกรรมการผู้อำนวยการใหญ่
รักษาการ กรรมการผู้อำนวยการใหญ่

กองบริหารระบบเทคโนโลยีสารสนเทศ
สำเนาส่ง ทุกหน่วยงาน

แนวปฏิบัติการรักษาความมั่นคงปลอดภัย

ระบบสารสนเทศ

ของ

บริษัท วิทยุการบินแห่งประเทศไทย จำกัด

การอนุมัติเอกสาร

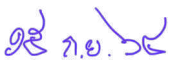
ผู้อนุมัติ

ตำแหน่ง	ชื่อ	ลายมือชื่อ	วัน/เดือน/ปี
ประธานคณะกรรมการกำกับดูแลมาตรฐานและความปลอดภัยบริการการเดินอากาศ (กมป.)	นายทินกร ชูวงศ์		

ผู้ตรวจสอบ

ตำแหน่ง	ชื่อ	ลายมือชื่อ	วัน/เดือน/ปี
ประธานคณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร	นายทินกร ชูวงศ์		

ผู้จัดทำ

ตำแหน่ง	ชื่อ	ลายมือชื่อ	วัน/เดือน/ปี
หัวหน้าคณะทำงานจัดทำแนวปฏิบัติ และวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศการเดินอากาศ	นายพงษ์นรินทร์ อนันตศิริจินดา		

คำนำ

ปัจจุบันระบบสารสนเทศมีส่วนสำคัญอย่างยิ่งในการดำเนินชีวิตประจำวันของประชาชน และต่อเนื่องกับการใช้งานระบบสารสนเทศอย่างแพร่หลาย ก็จะมีภัยอันตรายต่าง ๆ จากภัยคุกคาม โจมตีต่อระบบสารสนเทศติดตามมา หรือเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เกิดผลเสียหายต่อผู้ใช้งานระบบสารสนเทศ ภาครัฐจึงได้มีการบัญญัติกฎหมาย พระราชบัญญัติต่าง ๆ ทั้งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่น ๆ ที่เกี่ยวข้อง เพื่อเป็นการป้องกันผลเสียหายที่จะเกิดขึ้นตามมา ทั้งใช้เป็นเครื่องมือในการส่งเสริมการใช้งานอย่างถูกต้อง ป้องกัน และปราบปรามผู้ไม่ประสงค์ดีที่อาจคุกคาม โจมตี หรือก่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

บริษัท วิทยุการบินแห่งประเทศไทย จำกัด เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ ได้มีการนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้สนับสนุนกิจการภายในหน่วยงานต่าง ๆ ของบริษัทฯ เพื่อให้เกิดความสะดวก รวดเร็ว และมีประสิทธิภาพในการให้บริการ ดังนั้น ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้กำหนดไว้ให้หน่วยงานที่มีระบบสารสนเทศที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด

คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ ได้พิจารณากำหนดขอบเขตให้บริษัทฯ มีแนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ สอดคล้องกับข้อกฎหมาย พระราชบัญญัติ และมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ให้ทุกประเภทระบบสารสนเทศของบริษัทฯ ทั้งสารสนเทศบริการการเดินกาศ สารสนเทศอำนวยการ และสารสนเทศสนับสนุนอื่น ๆ มีทิศทางเดียวกันครอบคลุมทั่วทั้งองค์กร จึงได้มีประกาศเรื่อง “แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท วิทยุการบินแห่งประเทศไทย จำกัด”

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศฯ ฉบับนี้ได้กำหนดบทบาทหน้าที่ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของผู้เกี่ยวข้องทั้งหมด กำหนดแนวทางในการนำไปปฏิบัติรักษาความมั่นคงปลอดภัย และพร้อมรับมือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศในความรับผิดชอบ โดยแนวปฏิบัติฯ สอดคล้องกับข้อกฎหมาย พระราชบัญญัติ และมาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศต่าง ๆ ตามเอกสารอ้างอิงกฎหมายและมาตรฐานที่เกี่ยวข้องที่ระบุแนบท้าย

บันทึกประวัติการแก้ไขเอกสาร

ครั้งที่แก้ไข	วันที่แก้ไข	รายละเอียดการแก้ไข	ผู้จัดทำ
–	–	จัดทำเอกสารครั้งแรก	คณะทำงานฯ

สารบัญ

คำจำกัดความ

“บริษัทฯ” หมายความว่า บริษัท วิทยุการบินแห่งประเทศไทย จำกัด

“พนักงาน” หมายความว่า ผู้ที่ได้รับเข้าทำงานเป็นบุคคลากรในสังกัดของบริษัทฯ

“ผู้บริหาร” หมายความว่า พนักงานตั้งแต่ระดับผู้อำนวยการกองหรือเทียบเท่าขึ้นไปตามโครงสร้างองค์กรของบริษัทฯ

“ผู้ใช้งาน” หมายความว่า พนักงาน ผู้รับจ้าง หรือบุคคลที่ใช้งานระบบสารสนเทศของบริษัทฯ

“ระบบสารสนเทศ” หมายความว่า ระบบสารสนเทศภายใต้โครงสร้างการบริหารความมั่นคงปลอดภัยด้านสารสนเทศทั้ง ๕ ประเภท ได้แก่ สารสนเทศบริการการเดินอากาศ สารสนเทศอำนวยการ สารสนเทศวิจัยและพัฒนา สารสนเทศสนับสนุน และสารสนเทศธุรกิจ

“ผู้บริหารระบบสารสนเทศ” หมายความว่า ผู้บริหารของหน่วยงานที่รับผิดชอบระบบสารสนเทศในแต่ละประเภท มีหน้าที่บริหารจัดการ กำกับ ดูแลระบบสารสนเทศ รวมถึงการอนุมัติ/ให้สิทธิการเข้าถึง ระบบสารสนเทศที่อยู่ในความรับผิดชอบ

“ผู้ดูแลระบบสารสนเทศ” หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บริหารระบบสารสนเทศในแต่ละประเภทให้มีหน้าที่ดูแล จัดการระบบสารสนเทศ ทั้งส่วนของอุปกรณ์สารสนเทศ และ/หรือซอฟต์แวร์ระบบปฏิบัติการและแอปพลิเคชันต่าง ๆ ของระบบสารสนเทศ ที่อยู่ในความรับผิดชอบและ/หรือดำเนินการเกี่ยวกับการสร้างบัญชีผู้ใช้งาน กำหนด/ปรับปรุง/ถอดถอนสิทธิการเข้าถึงระบบสารสนเทศตามที่ได้รับอนุมัติ

“ระบบเครือข่ายสารสนเทศ” หมายความว่า ระบบโครงข่ายสื่อสารที่สนับสนุนบริการระบบสารสนเทศด้านต่าง ๆ ในภารกิจของบริษัทฯ

“ผู้บริหารระบบเครือข่ายสารสนเทศ” หมายความว่า ผู้บริหารของหน่วยงานประเภทสารสนเทศสนับสนุน รับผิดชอบระบบโครงข่ายสื่อสาร และสาธารณูปโภคที่สนับสนุนระบบสารสนเทศด้านต่าง ๆ ของบริษัทฯ มีหน้าที่บริหารจัดการ กำกับ ดูแลระบบเครือข่ายสารสนเทศ รวมถึงการอนุมัติ/ให้สิทธิการเข้าถึงระบบสารสนเทศที่อยู่ในความรับผิดชอบ

“ผู้ดูแลระบบเครือข่ายสารสนเทศ” หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บริหารระบบเครือข่ายสารสนเทศให้มีหน้าที่ดูแล จัดการ ดำเนินระบบเครือข่ายสารสนเทศที่อยู่ในความรับผิดชอบ และ/หรือประสานงาน ดำเนินการเกี่ยวกับการสร้างบัญชีผู้ใช้งาน กำหนด/ปรับปรุง/ถอดถอนสิทธิการเข้าถึงระบบสารสนเทศในแต่ละประเภทตามที่ได้รับอนุมัติ

“ผู้บริหารการพัฒนาระบบสารสนเทศ” หมายความว่า ผู้บริหารของหน่วยงานที่รับผิดชอบในการพัฒนาระบบสารสนเทศสนับสนุนภารกิจในแต่ละประเภทระบบสารสนเทศ มีหน้าที่บริหารจัดการ กำกับ ดูแลการพัฒนาระบบสารสนเทศที่อยู่ในความรับผิดชอบ

“ผู้พัฒนาระบบสารสนเทศ” หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บริหารการพัฒนาระบบสารสนเทศ ให้มีหน้าที่ดำเนินการพัฒนาระบบสารสนเทศสนับสนุนภารกิจในแต่ละประเภทของระบบสารสนเทศ

“เจ้าของพื้นที่” หมายความว่า ผู้บริหารระบบสารสนเทศและผู้ดูแลระบบสารสนเทศในแต่ละประเภทที่รับผิดชอบ รวมถึงผู้ที่ได้รับมอบหมายให้เป็นผู้ดูแลเฝ้าระวังระบบสารสนเทศที่อยู่ในความรับผิดชอบ

“ผู้ดูแลงานจ้างบุคคล” หมายความว่า ผู้ที่มีหน้าที่รับผิดชอบในกระบวนการจ้างพนักงานหรือผู้รับจ้าง

“ผู้ดูแลงานฝึกอบรม” หมายความว่า ผู้ที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบดูแลให้ความรู้หรือฝึกอบรมด้านความมั่นคงปลอดภัยระบบสารสนเทศที่อยู่ในความรับผิดชอบให้กับพนักงาน หรือผู้รับจ้าง

“ผู้ดูแลงานนิติการ” หมายความว่า หน่วยงานที่รับผิดชอบเป็นผู้ให้ความเห็น/คำแนะนำเกี่ยวกับข้อกฎหมาย/ระเบียบ ข้อบังคับ และข้อกำหนดต่าง ๆ ที่มีผลต่อการดำเนินกิจการและภารกิจของหน่วยงานในบริษัทฯ และดำเนินการเกี่ยวกับคดีความของบริษัทฯ หรือผู้ที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบเกี่ยวกับกฎหมาย ระเบียบข้อบังคับ และข้อกำหนดต่าง ๆ ที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

“ผู้รับจ้าง” หมายความว่า หน่วยงาน บุคคลภายนอก หรือผู้ให้บริการที่ได้รับการจ้างงานดำเนินการเกี่ยวกับระบบสารสนเทศ โดยผู้ดูแลงานจ้างบุคคลตามขั้นตอนกระบวนการจัดจ้างของบริษัทฯ

“พื้นที่ควบคุมด้านสารสนเทศ” หมายความว่า พื้นที่ติดตั้งระบบสารสนเทศที่ถูกกำหนดให้มีการควบคุมการเข้าออก เพื่อรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

“ข้อมูล” หมายความว่า ข้อมูลต่าง ๆ ในรูปแบบอิเล็กทรอนิกส์ที่อยู่ภายในระบบสารสนเทศ

“อุปกรณ์สารสนเทศ” หมายความว่า เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ เครื่องคอมพิวเตอร์แบบพกพา Smartphone Tablet อุปกรณ์เครือข่าย และอุปกรณ์ต่อพ่วงอื่น ๆ

“แอปพลิเคชัน” หมายความว่า ชุดโปรแกรมประยุกต์หรือชุดโปรแกรมฐานข้อมูลที่ถูกพัฒนาขึ้น เพื่ออำนวยความสะดวกในด้านต่าง ๆ ตามความต้องการของผู้ใช้งาน ซึ่งถูกออกแบบมาให้สามารถใช้งานบนระบบปฏิบัติการของอุปกรณ์สารสนเทศ

“ซอฟต์แวร์” หมายความว่า ชุดโปรแกรมที่ถูกพัฒนาขึ้นจากชุดคำสั่งที่ใช้งานบนอุปกรณ์สารสนเทศ เพื่อทำหน้าที่ควบคุมการประมวลผลของอุปกรณ์สารสนเทศให้ปฏิบัติและทำตามชุดคำสั่งของโปรแกรมแอปพลิเคชันต่าง ๆ ที่ถูกพัฒนาขึ้น

“ระบบปฏิบัติการ” หมายความว่า ซอฟต์แวร์ที่ทำหน้าที่ควบคุมการทำงานทั้งหมดของอุปกรณ์สารสนเทศ และติดต่อประสานกันกับซอฟต์แวร์แอปพลิเคชันต่าง ๆ ที่ติดตั้งบนอุปกรณ์สารสนเทศ ในการประมวลผล ควบคุมการทำงานให้เป็นไปตามความต้องการที่กำหนดของโปรแกรมแอปพลิเคชันนั้น ๆ

“ฮาร์ดแวร์” หมายความว่า ชิ้นส่วนของอุปกรณ์สารสนเทศ ที่สามารถมองเห็นและสัมผัสสิ่งต่าง ๆ นั้นได้

“สินทรัพย์” หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

“ทรัพย์สินสารสนเทศ” หมายความว่า สินทรัพย์ที่เกี่ยวข้องกับระบบสารสนเทศ ทั้งฮาร์ดแวร์และซอฟต์แวร์

“บัญชีทรัพย์สินสารสนเทศ” หมายความว่า บันทึกที่แสดงรายการของทรัพย์สินสารสนเทศที่ใช้งานในบริษัทฯ

“โปรแกรมไม่พึงประสงค์” หมายความว่า ชุดคำสั่งคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือข้อมูลที่ได้รับการออกแบบขึ้นมาเพื่อก่อกวนหรือสร้างความเสียหาย ไม่ว่าโดยทางตรงหรือทางอ้อมแก่อุปกรณ์สารสนเทศ

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทฯ ตามที่ได้รับอนุมัติจากผู้บริหารระบบสารสนเทศ

“บัญชีผู้ใช้งาน” หมายความว่า ชื่อผู้ใช้งานและรหัสผ่านที่ใช้ในการยืนยันตัวตน ก่อนเข้าใช้งานระบบสารสนเทศ เช่น ชื่อผู้ใช้งานและรหัสผ่าน

“ทะเบียนบัญชีผู้ใช้งาน” หมายความว่า บันทึกรายชื่อผู้ใช้งาน ที่มีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศ รายละเอียดและสถานะต่าง ๆ ของผู้ใช้งาน

“การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ” หมายความว่า การอนุญาตการกำหนดสิทธิให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นกับบุคคลภายนอก ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

“ความมั่นคงปลอดภัยสารสนเทศ” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมถึงคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบสารสนเทศขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยด้านสารสนเทศถูกคุกคาม

“เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่อาจจะเกิดจากมาตรการป้องกันที่ล้มเหลว หรือการฝ่าฝืน/ละเมิด/ไม่ปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศ หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

“สื่อบันทึกข้อมูล” หมายความว่า อุปกรณ์ที่ใช้จัดเก็บข้อมูลต่าง ๆ ในรูปแบบอิเล็กทรอนิกส์ เช่น Thumb drive, External hard disk เป็นต้น

“ข้อมูล Log” หมายความว่า ข้อมูลจราจรทางคอมพิวเตอร์ ที่บันทึกเหตุการณ์ กิจกรรมเกี่ยวกับการติดต่อสื่อสารของระบบสารสนเทศ ซึ่งสามารถแสดงถึงผู้ใช้งาน แหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ในการติดต่อสื่อสารภายในระบบสารสนเทศนั้น

“ช่องโหว่ทางเทคนิค” หมายความว่า จุดอ่อนหรือช่องทางเข้าถึงระบบสารสนเทศ ที่ทำให้ผู้บุกรุกหรือผู้ไม่ประสงค์ดี สามารถเข้าถึงระบบสารสนเทศได้โดยไม่ได้รับอนุญาต ก่อให้เกิดภัยคุกคามหรือเกิดความเสียหาย ส่งผลกระทบต่อความมั่นคงปลอดภัยระบบสารสนเทศและกระทบกับการให้บริการระบบสารสนเทศ

บทที่ ๑ นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีนโยบายการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ประกาศใช้ภายใน*บริษัทฯ* โดยมีความสอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*

๒. เพื่อให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* ให้เป็นปัจจุบัน

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

๑. จัดให้มีการควบคุมการเข้าถึงระบบสารสนเทศ ทั้งระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์หรือแอปพลิเคชัน และข้อมูลอย่างมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่มีสิทธิหรือผู้ที่ไม่ได้รับอนุญาต

๒. จัดให้มีระบบสารสนเทศและระบบสำรองสารสนเทศที่อยู่ในสภาพพร้อมใช้งาน โดยมีแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินหรือเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ระบบสารสนเทศสามารถให้บริการได้อย่างต่อเนื่อง

๓. จัดให้มีการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

แนวปฏิบัติ

๑. คณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร จัดทำนโยบายการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่สอดคล้องกับนโยบายดังกล่าว นำเสนอคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสารพิจารณา

๒. คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสารพิจารณาอนุมัติและประกาศใช้นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๓. คณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสารทบทวนนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมาย หรือมาตรฐานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๔. คณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสารเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* ให้กับผู้เกี่ยวข้องทั้งหมดทราบผ่านช่องทางสื่อสารภายใน*บริษัทฯ* เช่น ระบบ Intranet ระบบสารบรรณอิเล็กทรอนิกส์ Line Social Ambassador เป็นต้น

บทที่ ๒ โครงสร้างการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ

วัตถุประสงค์

๑. เพื่อกำหนดโครงสร้างการบริหารความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๒. เพื่อให้มีการกำหนดบทบาท แบ่งแยกหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ให้ครอบคลุมทั้ง*บริษัทฯ*

แนวปฏิบัติ

๑. โครงสร้างการบริหารความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

โครงสร้างการบริหารความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* โดยแบ่งโครงสร้างการบริหาร*ระบบสารสนเทศ* ออกเป็น ๕ ประเภท ประกอบด้วย

๑.๑ สารสนเทศบริการการเดินอากาศ

*ระบบสารสนเทศ*ที่สนับสนุนภารกิจด้านการให้บริการสารสนเทศบริการการเดินอากาศ เช่น

๑.๑.๑ ระบบ Air Traffic Service (ATS)

๑.๑.๒ ระบบ Flight Information Services (FIS)

๑.๑.๓ ระบบ Aviation Meteorology Services (MET)

๑.๑.๔ ระบบ Alerting Services

๑.๑.๕ ระบบ Air Navigation Systems

เป็นต้น

๑.๒ สารสนเทศอำนวยการ

*ระบบสารสนเทศ*ที่สนับสนุนภารกิจด้านอำนวยการต่าง ๆ ของ*บริษัทฯ*

๑.๓ สารสนเทศวิจัยและพัฒนา

*ระบบสารสนเทศ*ที่สนับสนุนภารกิจด้านวิจัยและพัฒนาระบบสารสนเทศ เพื่อสนับสนุนภารกิจของ*บริษัทฯ* ในการให้บริการด้านการเดินอากาศ อำนวยการ และอื่น ๆ

๑.๔ สารสนเทศสนับสนุน

*ระบบสารสนเทศ*ที่สนับสนุนภารกิจด้านการให้บริการระบบโครงข่ายสื่อสาร และสาธารณูปโภค ที่สนับสนุนบริการ*ระบบสารสนเทศ*ด้านต่าง ๆ ของ*บริษัทฯ*

๑.๕ สารสนเทศธุรกิจ

*ระบบสารสนเทศ*ที่สนับสนุนภารกิจทางด้านพัฒนาธุรกิจ ในการให้บริการแก่สายการบินหน่วยงาน และธุรกิจด้านต่าง ๆ ของ*บริษัทฯ*

๒. บทบาทหน้าที่

กรรมการผู้อำนวยการใหญ่ ในฐานะผู้บริหารสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายใด ๆ ที่เกิดขึ้นแก่องค์กร หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติ ตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๒.๑ คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีกรรมการผู้อำนวยการใหญ่เป็นประธานคณะกรรมการฯ มีหน้าที่รับผิดชอบ ดังนี้

๒.๑.๑ กำหนดนโยบาย ทิศทางการดำเนินงานในภารกิจขององค์กร เกี่ยวกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้สอดคล้องกับข้อกำหนด/กฎหมาย/มาตรฐานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย *ระบบสารสนเทศ*ของ*บริษัทฯ*

๒.๑.๒ สนับสนุน ส่งเสริมและขับเคลื่อนให้หน่วยงานดำเนินงานตามนโยบายภาครัฐ

๒.๑.๓ แต่งตั้งคณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อบริหารงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ*บริษัทฯ*

๒.๒ คณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) เป็นประธานคณะอนุกรรมการฯ มีหน้าที่รับผิดชอบ ดังนี้

๒.๒.๑ บริหารงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ*บริษัทฯ*

๒.๒.๒ กำกับ ดูแล การปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๒.๒.๓ กำหนดแนวปฏิบัติการรักษาความปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* ให้สอดคล้องกับระเบียบและกฎหมายที่เกี่ยวข้อง ดังต่อไปนี้

๒.๒.๓.๑ กฎหมายด้านธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายด้านการเดินอากาศ รวมถึงกฎหมายอื่นใดที่เกี่ยวข้อง

๒.๒.๓.๒ ประกาศคณะกรรมการการบินพลเรือน เรื่อง แผนรักษาความปลอดภัยในการบินพลเรือนแห่งชาติ (NCASP)

๒.๒.๓.๓ ระเบียบว่าด้วยการกำกับดูแลมาตรฐานและความปลอดภัยบริการการเดินอากาศ พ.ศ. ๒๕๖๒

๒.๒.๔ อนุมัติวิธีปฏิบัติ/มาตรการภายใต้แนวปฏิบัติการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๒.๒.๕ รายงานผลการดำเนินการด้านการรักษาความมั่นคงปลอดภัย *ระบบสารสนเทศ* ของ *บริษัทฯ* ต่อคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานภายนอกที่เกี่ยวข้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๒.๖ แต่งตั้งคณะบริหารความมั่นคงปลอดภัย*ระบบสารสนเทศ*ในแต่ละประเภท ตามโครงสร้างการบริหารจัดการความมั่นคงปลอดภัย *ระบบสารสนเทศ*ของ*บริษัทฯ*

๒.๒.๗ แต่งตั้งคณะบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

๒.๓ คณะบริหารความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของบริษัทฯ ในแต่ละประเภท มีหน้าที่รับผิดชอบ ดังนี้

๒.๓.๑ กำกับดูแลระบบสารสนเทศให้เป็นไปตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๒.๓.๒ จัดทำหรือทบทวนแนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้อง กับการรักษาความมั่นคงปลอดภัย *ระบบสารสนเทศ*ของ *บริษัทฯ* ให้สอดคล้องกับข้อกำหนด/กฎหมาย/มาตรฐานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย *ระบบสารสนเทศ*

๒.๓.๓ สื่อสารนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๒.๓.๔ จัดให้มีการตรวจประเมินภายใน (Internal Audit) เพื่อตรวจสอบการดำเนินการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ *บริษัทฯ*

๒.๓.๕ จัดให้มีการประเมินความเสี่ยงเกี่ยวกับการรักษาความมั่นคงปลอดภัย *ระบบสารสนเทศ* ของบริษัทฯ อย่างน้อยปีละ ๑ ครั้ง

๒.๓.๖ ติดตามและตรวจสอบการดำเนินการแก้ไขหรือป้องกันข้อบกพร่องที่ตรวจพบจากผลการตรวจประเมิน

๒.๓.๗ รายงานผลการปฏิบัติงานให้คณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสารทราบตามกรอบระยะเวลาที่คณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสารกำหนด

๒.๔ คณะบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่รับผิดชอบ ดังนี้

๒.๔.๑ สนับสนุน *ผู้ดูแลระบบสารสนเทศ*แต่ละประเภทในการตรวจสอบ และแก้ไข *เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ*

๒.๔.๒ วิเคราะห์ ประเมินผลกระทบจาก*เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ*

๒.๔.๓ สืบสวน สอบสวน รวบรวม และจัดเก็บหลักฐานของ*เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ*

๒.๔.๔ รายงานผลการดำเนินงาน และนำเสนอแนวทางการบริหารจัดการ*เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ* ต่อคณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๕ *ผู้บริหารระบบสารสนเทศ* มีหน้าที่บริหารงาน*ระบบสารสนเทศ*ในความรับผิดชอบให้เป็นไปตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* และเป็นผู้อนุมัติหรือให้สิทธิการเข้าถึง*ระบบสารสนเทศ*ที่อยู่ในความรับผิดชอบของตน

๒.๖ *ผู้ดูแลระบบสารสนเทศ* มีหน้าที่ดูแลบริหารจัดการ*ระบบสารสนเทศ*ที่อยู่ในความรับผิดชอบให้เป็นไปตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๒.๗ *ผู้บริหาร* มีหน้าที่รับผิดชอบในการกำกับดูแล*ผู้ใช้งานระบบสารสนเทศ*ที่อยู่ใต้บังคับบัญชาในสังกัดให้ปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๒.๘ *ผู้ใช้งาน* มีหน้าที่ต้องใช้งาน*ระบบสารสนเทศ*อย่างถูกต้องเหมาะสมและปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* โดยเคร่งครัด

บทที่ ๓ ความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ

๒. สารสนเทศอำนวยการ

๓. สารสนเทศวิจัยและพัฒนา

๔. สารสนเทศสนับสนุน

๕. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อให้*ผู้ดูแลงานจ้างบุคคล*จัดทำบันทึกข้อตกลงกับ*ผู้ใช้งาน*ในการปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* ตั้งแต่การจ้างงานจนสิ้นสุดการจ้างงาน

๒. เพื่อให้*ผู้ดูแลงานจ้างบุคคล* และ*ผู้ใช้งาน*เข้าใจบทบาทหน้าที่ และตระหนักรู้ด้านความมั่นคงปลอดภัย*ระบบสารสนเทศ*

แนวปฏิบัติ

๑. ก่อนเริ่มปฏิบัติงาน/จ้างงาน

๑.๑ *ผู้ดูแลงานจ้างบุคคล*ต้องจัดทำสัญญาจ้างหรือบันทึกข้อตกลงด้านความมั่นคงปลอดภัย*ระบบสารสนเทศ*กับ*ผู้ใช้งาน* เพื่อให้รับทราบ/รับรองข้อมูล/ยินยอมปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* ก่อนเริ่มปฏิบัติงาน

๑.๒ *ผู้ใช้งาน*ลงทะเบียนขอใช้งาน*ระบบสารสนเทศ*ตามบทบาทหน้าที่ที่ได้รับมอบหมาย และส่งข้อมูลการลงทะเบียนขอใช้งานให้*ผู้บริหารระบบสารสนเทศ*ที่เกี่ยวข้องพิจารณาอนุมัติการเข้าถึง*ระบบสารสนเทศ*

๑.๓ *ผู้ดูแลงานฝึกอบรม*ต้องจัดให้มีการสร้างความตระหนักรู้ หรืออบรมให้ความรู้เกี่ยวกับนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* ให้กับ*ผู้ใช้งาน*

๒. ระหว่างการปฏิบัติงาน/จ้างงาน

๒.๑ *ผู้ดูแลงานจ้างบุคคล*หรือ*ผู้ใช้งาน*ต้องแจ้งให้*ผู้ดูแลระบบสารสนเทศ*ทราบ เมื่อ*ผู้ใช้งาน*มีการโอนย้ายสังกัด/หน่วยงาน/เปลี่ยนแปลงหน้าที่รับผิดชอบ

๒.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องสร้าง/ปรับปรุงสิทธิการเข้าถึงเข้าถึง *ระบบสารสนเทศ*ตามที่*ผู้บริหารระบบสารสนเทศ*อนุมัติ

๒.๓ *ผู้ดูแลงานฝึกอบรม*ต้องจัดให้มีการทบทวนความรู้ในนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* ให้กับ*ผู้ใช้งาน* อย่างน้อยปีละ ๑ ครั้ง

๓. สิ้นสุดการปฏิบัติงาน/จ้างงาน

๓.๑ *ผู้ดูแลงานจ้างบุคคล*จัดทำบันทึกข้อตกลง/เงื่อนไขด้านความมั่นคงปลอดภัย*ระบบสารสนเทศ*กับ*ผู้ใช้งาน* เพื่อให้*ผู้ใช้งาน*ยึดถือปฏิบัติตามบันทึกข้อตกลงภายหลังสิ้นสุดการปฏิบัติงาน/จ้างงาน

๓.๒ *ผู้ดูแลงานจ้างบุคคล*ต้องแจ้งให้*ผู้ดูแลระบบสารสนเทศ*ทราบ เมื่อ*ผู้ใช้งาน*สิ้นสุดการปฏิบัติงาน/จ้างงาน

๓.๓ *ผู้ดูแลระบบสารสนเทศ*ถอดถอนสิทธิและปรับปรุง*บัญชีผู้ใช้งาน*ตามที่*ผู้ดูแลงานจ้างบุคคล*แจ้งให้ทราบ

บทที่ ๔ การบริหารจัดการทรัพย์สินสารสนเทศ

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ
๒. สารสนเทศอำนวยการ
๓. สารสนเทศวิจัยและพัฒนา
๔. สารสนเทศสนับสนุน
๕. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อกำหนดให้มี *บัญชีทรัพย์สินสารสนเทศ* ที่สามารถระบุรายการ ผู้รับผิดชอบ *ผู้ใช้งานทรัพย์สินสารสนเทศของบริษัทฯ* ได้
๒. เพื่อกำหนดให้มีการปรับปรุง *บัญชีทรัพย์สินสารสนเทศ*ให้เป็นปัจจุบันอยู่เสมอ
๓. เพื่อกำหนดให้มีวิธีการใช้งาน*ทรัพย์สินสารสนเทศ*อย่างปลอดภัย
๔. เพื่อกำหนดให้มีการป้องกันการรั่วไหลของ *ข้อมูล* ในการส่งซ่อมหรือส่งคืน*ทรัพย์สินสารสนเทศ* เมื่อสิ้นสุดการใช้งาน/จ้างงาน

แนวปฏิบัติ

๑. *ทรัพย์สินสารสนเทศ*ที่จัดหาใหม่

๑.๑ *ผู้ดูแลระบบสารสนเทศ* จัดทำ/เพิ่ม *บัญชีทรัพย์สินสารสนเทศ* ในความรับผิดชอบตามรายการบัญชีทรัพย์สินของ *บริษัทฯ* โดยต้องระบุรายการ*ทรัพย์สินสารสนเทศ* หมายเลขทะเบียน ผู้รับผิดชอบ และ*ผู้ใช้งานทรัพย์สินสารสนเทศ* เป็นอย่างน้อย

๑.๒ *ผู้ดูแลระบบสารสนเทศ* แจ้งให้ผู้รับผิดชอบ และ*ผู้ใช้งานทรัพย์สินสารสนเทศ* ได้รับทราบรายการ*บัญชีทรัพย์สินสารสนเทศ*ที่ต้องรับผิดชอบ

๒. การใช้งาน*ทรัพย์สินสารสนเทศ*

๒.๑ *ผู้ใช้งาน*ต้องใช้งาน*ทรัพย์สินสารสนเทศ*อย่างปลอดภัย ตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย *ระบบสารสนเทศของบริษัทฯ* โดยคำนึงถึงความปลอดภัยของ *ทรัพย์สินสารสนเทศ* และเพิ่มความระมัดระวังมากขึ้นเมื่อมีการนำ*ทรัพย์สินสารสนเทศ*ไปใช้งานภายนอกบริษัทฯ

๒.๒ *ผู้ใช้งาน*ต้องไม่เคลื่อนย้าย*ทรัพย์สินสารสนเทศ*ประเภทติดตั้งใช้งานประจำที่ โดยไม่ได้รับอนุญาตจาก*ผู้ดูแลระบบสารสนเทศ*

๒.๓ *ผู้ใช้งาน*ต้องแจ้ง*ผู้ดูแลระบบสารสนเทศ* เมื่อ*ทรัพย์สินสารสนเทศ*มีการเปลี่ยนแปลง*ผู้ใช้งาน*

๒.๔ *ผู้ดูแลระบบสารสนเทศ*ต้องปรับปรุง*บัญชีทรัพย์สินสารสนเทศ*ให้เป็นปัจจุบัน เมื่อ*ทรัพย์สินสารสนเทศ*มีการเปลี่ยนแปลง ดังนี้

๒.๔.๑ *ทรัพย์สินสารสนเทศ*มีการเปลี่ยนแปลง*ผู้ใช้งาน*

๒.๔.๒ *ทรัพย์สินสารสนเทศ*ประเภทติดตั้งใช้งานประจำที่มีการเคลื่อนย้ายสถานที่ติดตั้ง

๓. การใช้งาน*ทรัพย์สินสารสนเทศ*ส่วนตัว

๓.๑ *ผู้ใช้งาน*ที่มีความจำเป็นต้องใช้งาน*ทรัพย์สินสารสนเทศ*ส่วนตัวเชื่อมต่อกับ*ระบบเครือข่ายสารสนเทศ*ของ*บริษัทฯ* ต้องได้รับอนุญาตจาก*ผู้ดูแลระบบสารสนเทศ*ก่อนการใช้งาน

๓.๒ *ผู้ใช้งาน*ต้องใช้งาน*ทรัพย์สินสารสนเทศ*ส่วนตัวอย่างปลอดภัย ตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๓.๓ *ผู้ใช้งาน*ต้องรับผิดชอบผลเสียหายต่อ*บริษัทฯ* อันเกิดจากการใช้งาน*ทรัพย์สินสารสนเทศ*ส่วนตัว เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเป็นเหตุสุดวิสัย และไม่ได้เกิดจากความประมาทเลินเล่อ หรือไม่ได้ปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*

๔. *ทรัพย์สินสารสนเทศ*เมื่อสิ้นสุดการใช้งาน หรือชำรุด หรือตัดจำหน่าย

๔.๑ *ผู้ใช้งาน*ต้องส่งคืน*ทรัพย์สินสารสนเทศ*ให้กับหน่วยงานเจ้าของ*ทรัพย์สินสารสนเทศ*เมื่อมีการเรียกคืน*ทรัพย์สินสารสนเทศ*ที่สิ้นสุดหรือหมดอายุการใช้งาน หรือ*ผู้ใช้งาน*พ้นจากการปฏิบัติหน้าที่หรือสิ้นสุดการจ้างงาน โดยต้องโอนถ่าย*ข้อมูล*ส่วนตัวหรือลบ*ข้อมูล*ชั้นความลับ (ถ้ามี) ออกจาก*ทรัพย์สินสารสนเทศ*ก่อนส่งคืน

๔.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องลบ*ข้อมูล*หรือทำลาย*สื่อบันทึกข้อมูล*บน*ทรัพย์สินสารสนเทศ*ก่อนดำเนินการตัดจำหน่ายหรือส่งซ่อม

๔.๓ *ผู้ดูแลระบบสารสนเทศ*ต้องปรับปรุง*บัญชีทรัพย์สินสารสนเทศ*ให้เป็นปัจจุบัน เมื่อ*ทรัพย์สินสารสนเทศ*สิ้นสุดการใช้งาน

บทที่ ๕ การควบคุมการเข้าถึง

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ
๒. สารสนเทศอำนวยการ
๓. สารสนเทศวิจัยและพัฒนา
๔. สารสนเทศสนับสนุน
๕. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อให้มีการจำกัดการเข้าถึง*ระบบสารสนเทศ*ของ*บริษัทฯ* เฉพาะบุคคลที่มีสิทธิเข้าใช้งาน
๒. เพื่อให้มีการกำหนด ปรับปรุง และถอดถอนสิทธิการใช้งาน*ระบบสารสนเทศ*ของ*บริษัทฯ* ให้เหมาะสมตามบทบาทหน้าที่ของ*ผู้ใช้งาน*

แนวปฏิบัติ

๑. กำหนดสิทธิการเข้าถึง*ระบบสารสนเทศ*ก่อนเริ่มปฏิบัติงาน

๑.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดสร้าง*บัญชีผู้ใช้งาน* และกำหนดระดับสิทธิการเข้าถึง*ระบบสารสนเทศ*ให้กับผู้เกี่ยวข้อง ตามบทบาทหน้าที่ที่รับผิดชอบ หรือตามที่ได้รับอนุมัติ

๑.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องสร้าง*บัญชีผู้ใช้งาน*แยกเฉพาะเป็นรายบุคคล ไม่ให้ซ้ำซ้อนกัน โดยสามารถตรวจสอบหรือระบุตัวตนของ*ผู้ใช้งาน*ได้ และต้องแยกระดับสิทธิการเข้าถึงทั้งระดับสิทธิการเข้าถึง*ระบบเครือข่ายสารสนเทศ ระบบปฏิบัติการ* และ*แอปพลิเคชัน*

๑.๓ *ผู้ดูแลระบบสารสนเทศ*เป็นผู้พิจารณากำหนดแนวทาง/วิธีการที่สามารถตรวจสอบ/ระบุตัวตนของ*ผู้ใช้งาน*ในแต่ละเหตุการณ์ได้ เมื่อ*ระบบสารสนเทศ*มีข้อจำกัดในการแยก*บัญชีผู้ใช้งาน*เป็นรายบุคคลและจำเป็นต้องใช้*บัญชีผู้ใช้งาน*ร่วมกัน

๑.๔ *ผู้ดูแลระบบสารสนเทศ*จัดทำ*ทะเบียนบัญชีผู้ใช้งาน*และเก็บรักษาไว้เป็นหลักฐาน

๒. การรับสิทธิการเข้าถึง*ระบบสารสนเทศ*

๒.๑ *ผู้ใช้งาน*เมื่อลงทะเบียน*บัญชีผู้ใช้งาน*เพื่อขอรับสิทธิการเข้าถึง*ระบบสารสนเทศ*ตามบทบาทหน้าที่ที่ได้รับมอบหมาย ส่งให้*ผู้บริหารระบบสารสนเทศ*ที่เกี่ยวข้องพิจารณาอนุมัติการเข้าถึง*ระบบสารสนเทศ*และ*ผู้ดูแลระบบสารสนเทศ*ได้จัดสร้าง*บัญชีผู้ใช้งาน*ตามสิทธิที่ได้รับอนุมัติในทะเบียนการขอใช้งาน

๒.๒ *ผู้ใช้งาน*ต้องดูแลรักษาสิทธิการเข้าถึง*ระบบสารสนเทศ*ของตนไว้ และปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศของบริษัทฯ* โดยเคร่งครัด เมื่อได้รับสิทธิการเข้าถึง*ระบบสารสนเทศ*ที่เกี่ยวข้องแล้ว

๒.๓ *ผู้ใช้งาน*ต้องใช้สิทธิ*บัญชีผู้ใช้งาน*ในการเข้าใช้งานและออกจากการใช้งาน*ระบบสารสนเทศ* ตามภารกิจที่ได้รับมอบหมาย หรือตามกรอบระยะเวลาที่กำหนดหรือเสร็จสิ้นภารกิจ

๒.๔ *ผู้ใช้งาน*เจ้าของสิทธิ*บัญชีผู้ใช้งาน* ต้องรับผิดชอบผลเสียหายอันเกิดจาก*บัญชีผู้ใช้งาน*นั้น เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของบุคคลอื่น และไม่ได้เกิดจากความประมาทเลินเล่อของเจ้าของสิทธิ*บัญชีผู้ใช้งาน*

๓. การปรับปรุงสิทธิการเข้าถึง*ระบบสารสนเทศ*

๓.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องทบทวนหรือปรับปรุงสิทธิการเข้าถึง*ระบบสารสนเทศ*ให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสิทธิการเข้าถึงตามที่*ผู้บริหารระบบสารสนเทศ*อนุมัติ

๓.๒ *ผู้ใช้งาน*ต้องแจ้ง*ผู้ดูแลระบบสารสนเทศ*เพื่อขอปรับปรุงสิทธิการเข้าถึง*ระบบสารสนเทศ* เมื่อมีการเปลี่ยนแปลงหน้าที่รับผิดชอบการใช้งาน*ระบบสารสนเทศ*

๔. การถอดถอนสิทธิ*บัญชีผู้ใช้งาน*

๔.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องถอดถอนสิทธิ/ลบบัญชีผู้ใช้งานภายใน ๓ วัน หลังจากได้รับแจ้งจากผู้ดูแลงานจ้างบุคคล/ผู้ใช้งาน หรือเมื่อครบกำหนดระยะเวลาขอใช้งาน

๔.๒ ถอดถอนสิทธิการเข้าถึง*ระบบสารสนเทศ* ของ*ผู้ใช้งาน*เมื่อสิ้นสุดหรือพ้นจากการปฏิบัติหน้าที่ หรือครบกำหนดระยะเวลาขอใช้งาน

๔.๓ *ผู้ใช้งาน*ต้องแจ้ง*ผู้ดูแลระบบสารสนเทศ*เพื่อถอดถอนสิทธิการเข้าถึง*ระบบสารสนเทศ* เมื่อสิ้นสุดหรือพ้นจากการปฏิบัติหน้าที่เกี่ยวกับ*ระบบสารสนเทศ*นั้น

๕. การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

๕.๑ ผู้ดูแลระบบสารสนเทศต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานฟังก์ชันต่าง ๆ ของระบบสารสนเทศของผู้ใช้งานตามบทบาทหน้าที่รับผิดชอบของผู้ใช้งาน หรือตามที่ผู้บริหารระบบสารสนเทศกำหนด

๕.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มีวิธีการป้องกันการเข้าถึง*ระบบสารสนเทศ*โดยไม่ได้รับอนุญาต

๕.๓ *ผู้ดูแลระบบสารสนเทศ*ต้องกำหนดรูปแบบของรหัสผ่านของ*ระบบสารสนเทศ*ที่รับผิดชอบให้*ผู้ใช้งาน*ได้รับทราบ/ปฏิบัติตามข้อกำหนด

๕.๔ *ผู้ดูแลระบบสารสนเทศ*ต้องกำหนดรอบระยะเวลาในการเปลี่ยนรหัสผ่าน และตรวจสอบการเปลี่ยนรหัสผ่านของ*ผู้ใช้งาน*ตามรอบระยะเวลาที่กำหนด

๕.๕ *ผู้ดูแลระบบสารสนเทศ*ต้องไม่นำ*บัญชีผู้ใช้งาน*ที่มีสิทธิระดับสูงสุดมาใช้ในการปฏิบัติงานทั่วไป เช่น บัญชี Administrator หรือ Root หรือเทียบเท่า เป็นต้น ยกเว้นในกรณีที่มีความจำเป็นต้องขออนุญาตจากผู้บริหารระบบสารสนเทศ

๕.๖ ผู้ดูแลระบบสารสนเทศต้องจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงตอบโต้ หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยมีการทำงานได้ ดังนี้

๕.๖.๑ แจ้งเตือนเมื่อผู้ใช้งานกรอกรหัสผ่านผิด และจะระงับการเข้าถึงระบบทันทีเมื่อกรอกรหัสผ่านผิดเกิน ๕ ครั้ง โดยผู้ใช้งานต้องแจ้งผู้ดูแลระบบเพื่อทำการยกเลิกการระงับ

๕.๖.๒ แสดงหน้าจอการเข้าสู่ระบบภายหลังจากการเข้าสู่ระบบได้สำเร็จ

๕.๖.๓ ไม่แสดงฟังก์ชันให้ความช่วยเหลือระหว่างกระบวนการเข้าสู่ระบบ

๕.๗ *ผู้บริหารระบบสารสนเทศ*ต้องเปลี่ยนรหัสผ่านทันทีภายหลังการใช้งานบัญชีผู้ใช้งานที่มีสิทธิระดับสูงสุดแล้วเสร็จ

๕.๘ *ผู้ดูแลระบบสารสนเทศ*ต้องแยกระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อบริษัทฯ ออกจากระบบงานอื่น ๆ ของบริษัทฯ เช่น ระบบสารสนเทศบริการการเดินอากาศ เป็นต้น

๕.๙ *ผู้ดูแลระบบสารสนเทศ*ต้องกำกับ ควบคุม ดูแล *ผู้ใช้งาน*ที่ได้รับสิทธิการเข้าถึง*ระบบสารสนเทศ* ให้ปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศของบริษัทฯ* โดยเคร่งครัด

๕.๑๐ *ผู้บริหารระบบสารสนเทศ*ต้องกำหนดผู้ดูแลระบบสารสนเทศ ผู้พัฒนาระบบสารสนเทศและผู้ดูแลฐานข้อมูล ให้มีผู้รับผิดชอบแยกออกจากกัน

๕.๑๑ *ผู้บริหารระบบสารสนเทศ*กำหนดช่องทางการเข้าถึงข้อมูลให้มีความปลอดภัยกับระดับชั้นความลับของข้อมูล เช่น ระบบ Intranet ระบบ Internet และระบบ VPN เป็นต้น

๕.๑๒ *ผู้บริหารระบบสารสนเทศ*กำหนดช่วงเวลาการเข้าถึงข้อมูลให้มีความปลอดภัยกับระดับชั้นความลับของข้อมูล เช่น เข้าถึงได้ตามเวลาปฏิบัติงาน เข้าถึงได้ ๒๔ ชั่วโมง เป็นต้น

๕.๑๓ *ผู้ดูแลระบบสารสนเทศ*ต้องกำหนดให้มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกสำนักงานด้วยชื่อผู้ใช้งานและรหัสผ่านทุกครั้ง ก่อนเข้าใช้งานระบบสารสนเทศของ*บริษัทฯ*

บทที่ ๖ การเข้ารหัสลับข้อมูล

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ
๒. สารสนเทศอำนวยการ
๓. สารสนเทศวิจัยและพัฒนา
๔. สารสนเทศสนับสนุน
๕. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อป้องกันการแก้ไข ปลอมแปลง และรักษาความถูกต้องครบถ้วนของ*ข้อมูล*
๒. เพื่อให้มีการกำหนดแนวทางการบริหารกุญแจรหัส

แนวปฏิบัติ

๑. *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มีมาตรการเข้ารหัสลับ*ข้อมูล* ให้สอดคล้องกับแนวทางการกำหนดชั้นความลับของ*ข้อมูล*ตามประกาศของ*บริษัทฯ* หรือมาตรฐานที่กำหนดของระบบที่ให้บริการ
๒. *ผู้ดูแลระบบสารสนเทศ*ต้องกำหนดให้มีแนวทางการบริหารจัดการกุญแจรหัส และปฏิบัติตามตลอดวงจรชีวิตของกุญแจรหัส

บทที่ ๗ การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ

๒. สารสนเทศอำนวยการ

๓. สารสนเทศวิจัยและพัฒนา

๔. สารสนเทศสนับสนุน

๕. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อให้มีการกำหนดขอบเขต และควบคุมการเข้าถึงพื้นที่ใช้งาน*ระบบสารสนเทศ*โดยไม่ได้รับอนุญาต

๒. เพื่อควบคุม*อุปกรณ์สารสนเทศ*ให้อยู่ในสภาพแวดล้อมทางกายภาพที่มั่นคงปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับ*ระบบสารสนเทศ*

แนวปฏิบัติ

๑. การป้องกันพื้นที่ใช้งาน*ระบบสารสนเทศ*

๑.๑ *เจ้าของพื้นที่*ต้องกำหนดเขต*พื้นที่ควบคุมด้านสารสนเทศ*ให้ชัดเจน และต้องกำหนดให้เฉพาะผู้ที่มีสิทธิหรือได้รับอนุญาตในการผ่านเข้า–ออก*พื้นที่ควบคุมด้านสารสนเทศ*เท่านั้น

๑.๒ *เจ้าของพื้นที่*ต้องกำหนด*พื้นที่ควบคุมด้านสารสนเทศ*ซึ่งเป็นพื้นที่ปฏิบัติงานของระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงกับ*บริษัทฯ* โดยแยกออกเป็นสัดส่วนจากระบบงานอื่นของ*บริษัทฯ*

๑.๓ *เจ้าของพื้นที่*ต้องกำหนดมาตรการควบคุมการเข้า–ออก*พื้นที่ควบคุมด้านสารสนเทศ* และต้องบันทึกการเข้า–ออกพื้นที่ทุกครั้ง โดยต้องสามารถตรวจสอบได้

๑.๔ *เจ้าของพื้นที่*ต้องตรวจสอบระบบการรักษาความมั่นคงปลอดภัยในการผ่านเข้า–ออก*พื้นที่ควบคุมด้านสารสนเทศ*อย่างต่อเนื่อง

๑.๕ บุคคลที่ได้รับอนุญาตในการผ่านเข้า–ออก*พื้นที่ควบคุมด้านสารสนเทศ*ต้องปฏิบัติตามมาตรการ/ข้อกำหนดการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* โดยเคร่งครัด

๒. การควบคุมอุปกรณ์*ระบบสารสนเทศ*

๒.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องติดตั้งอุปกรณ์*ระบบสารสนเทศ*ไว้ในสภาพแวดล้อมทางกายภาพที่มั่นคงปลอดภัย เช่น มีการควบคุมอุณหภูมิ ควบคุมความชื้น และป้องกันอัคคีภัย เป็นต้น

๒.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องติดตั้งอุปกรณ์*ระบบสารสนเทศ*ไว้ในสภาพแวดล้อมทางกายภาพที่มั่นคงปลอดภัยจากภัยธรรมชาติ ภัยคุกคามจากภายนอก จากการโจมตี การบุกรุก

๒.๓ *ผู้ดูแลระบบสารสนเทศ*ต้องกำหนดมาตรการในการควบคุมการเคลื่อนย้ายหรือนำ*ทรัพย์สินสารสนเทศ*ออกนอก*พื้นที่ควบคุมด้านสารสนเทศ*

๒.๔ *เจ้าของพื้นที่*ต้องควบคุมการนำอุปกรณ์หรือสิ่งอื่นใดที่อาจส่งผลกระทบกับความมั่นคงปลอดภัย*ระบบสารสนเทศ*เข้า*พื้นที่ควบคุมด้านสารสนเทศ* เช่น วัตถุไวไฟ อาหาร เครื่องดื่ม เป็นต้น

๒.๕ *เจ้าของพื้นที่*ต้องตรวจสอบความพร้อมใช้งานของ*ระบบสารสนเทศ* ในความรับผิดชอบอย่างต่อเนื่อง ทั้งระบบป้องกันตามสภาพแวดล้อมทางกายภาพ และระบบสนับสนุนการทำงานของ*ระบบสารสนเทศ* เช่น ระบบไฟฟ้า ระบบปรับอากาศ เป็นต้น

บทที่ ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ
๒. สารสนเทศอำนวยการ
๓. สารสนเทศวิจัยและพัฒนา
๔. สารสนเทศสนับสนุน
๕. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อจัดให้มีเอกสารคู่มือหรือขั้นตอนการปฏิบัติงานที่ครบถ้วน และเหมาะสมกับการปฏิบัติงาน
๒. เพื่อให้มีการควบคุมการเปลี่ยนแปลงที่เกิดขึ้นกับ *ระบบสารสนเทศ*อย่างมั่นคงปลอดภัย และไม่ส่งผลกระทบกับการใช้งาน
๓. เพื่อให้ทรัพยากรของ*ระบบสารสนเทศ*มีการใช้งานอย่างเหมาะสม เพียงพอ และมีประสิทธิภาพ
๔. เพื่อจัดให้มีการบันทึกเหตุการณ์ที่สามารถตรวจสอบได้ภายหลัง และควบคุมไม่ให้มีการเปลี่ยนแปลง*ข้อมูล*บันทึกเหตุการณ์
๕. เพื่อให้*ระบบสารสนเทศ*มีการตั้งค่าเวลาของระบบให้ถูกต้องตรงกัน มีมาตรฐานเดียวกัน และสอดคล้องตามที่กฎหมายกำหนด
๖. เพื่อจัดให้มีการตรวจสอบและป้องกันการถูกโจมตีจากผู้ไม่ประสงค์ดีผ่าน*ช่องโหว่ทางเทคนิค*
๗. เพื่อให้มีการสำรอง และทดสอบการกู้คืน*ข้อมูล*
๘. เพื่อบำรุงรักษา*อุปกรณ์สารสนเทศ*ให้มีความพร้อมใช้งาน

แนวปฏิบัติ

๑. การจัดทำเอกสารคู่มือหรือขั้นตอนการปฏิบัติงาน

๑.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มีเอกสารคู่มือหรือขั้นตอนการปฏิบัติงานสำหรับ*ระบบสารสนเทศ*ที่อยู่ในความรับผิดชอบที่ครบถ้วนเหมาะสม

๑.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มีการเข้าถึงเอกสารคู่มือหรือขั้นตอนการปฏิบัติงานเฉพาะ*ผู้ใช้งาน*ที่มีสิทธิหรือจำเป็นต้องใช้งานเท่านั้น

๒. การบริหารการเปลี่ยนแปลง

๒.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องมีการบริหารจัดการในการเปลี่ยนแปลงเกี่ยวกับ *ระบบสารสนเทศ* เพื่อไม่ให้เกิดผลกระทบกับการให้บริการโดยรวม หรือไม่เกิดผลกระทบกับความมั่นคงปลอดภัย*ระบบสารสนเทศ* อย่างน้อยดังนี้

๒.๑.๑ เมื่อมีการติดตั้งหรือปรับปรุงฮาร์ดแวร์และซอฟต์แวร์ใหม่

๒.๑.๒ เมื่อมีการเปลี่ยนแปลงฟังก์ชันการใช้งาน

๒.๑.๓ เมื่อมีการเปลี่ยนแปลงของกฎหมาย นโยบายภาครัฐ หน่วยงานกำกับดูแล และนโยบายของ*บริษัทฯ* ที่ส่งผลกระทบต่อ*ระบบสารสนเทศ*

๒.๑.๔ เมื่อ*ระบบสารสนเทศ*หยุดให้บริการ

๒.๑.๕ เมื่อมีการปรับปรุงช่องโหว่ทางเทคนิค

๒.๒ *ผู้ดูแลระบบสารสนเทศ*ประสานผู้เกี่ยวข้อง เพื่อวิเคราะห์ ประเมินถึงผลกระทบที่จะเกิดขึ้นก่อนและหลังการเปลี่ยนแปลงนั้น ๆ โดยนำเสนอข้อมูลต่อ*ผู้บริหารระบบสารสนเทศ*พิจารณาอนุมัติ ก่อนเริ่มดำเนินการเปลี่ยนแปลง โดยมีข้อมูลอย่างน้อยดังนี้

๒.๒.๑ ข้อมูลการวิเคราะห์ผลกระทบจากการเปลี่ยนแปลง

๒.๒.๒ ขั้นตอนแผนดำเนินการ

๒.๒.๓ แผนกู้คืนเพื่อรองรับกรณีที่การเปลี่ยนแปลงไม่เป็นไปตามขั้นตอนของแผนดำเนินการ

๒.๓ *ผู้ดูแลระบบสารสนเทศ*ต้องแจ้ง*ผู้ใช้งาน*ที่เกี่ยวข้องได้รับทราบถึงผลกระทบต่าง ๆ ในการให้บริการ ก่อนเริ่มดำเนินการเปลี่ยนแปลง

๒.๔ *ผู้ดูแลระบบสารสนเทศ*ต้องบันทึกประวัติการเปลี่ยนแปลงให้เป็นปัจจุบัน เช่น เวอร์ชันของระบบ การตั้งค่าระบบ (Configuration/Parameter) เป็นต้น

๒.๕ *ผู้ดูแลระบบสารสนเทศ*ต้องรายงานผลตรวจติดตาม ประเมินผล การดำเนินการเปลี่ยนแปลง

๓. การบริหารจัดการขีดความสามารถของ*ระบบสารสนเทศ*

๓.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องมีการวิเคราะห์และวางแผนงานการใช้งานทรัพยากรของ*ระบบสารสนเทศ* อย่างเหมาะสม เพียงพอ และมีประสิทธิภาพ

๓.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องติดตาม ปรับปรุงการใช้งานทรัพยากรของ*ระบบสารสนเทศ*ได้อย่างเหมาะสม เพียงพอ และมีประสิทธิภาพ

๔. การบันทึกและจัดเก็บ*ข้อมูล Log*

๔.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มีการบันทึกจัดเก็บ*ข้อมูล Log* การทำงานของ*ระบบสารสนเทศ*ตามที่กฎหมายกำหนดเป็นอย่างน้อย และต้องป้องกันการแก้ไขเปลี่ยนแปลงหรือทำลาย*ข้อมูล Log* ที่บันทึกจัดเก็บ โดยไม่ได้รับอนุญาต

๔.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องวิเคราะห์*ข้อมูล Log* อย่างสม่ำเสมอ เพื่อพัฒนาปรับปรุงประสิทธิภาพ และเฝ้าระวังภัยคุกคามที่อาจเกิดขึ้นกับ*ระบบสารสนเทศ*

๕. การตั้งค่าเวลานาฬิกาของ*ระบบสารสนเทศ*

๕.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มีการตั้งค่าเวลานาฬิกาของ *ระบบสารสนเทศ* ในความรับผิดชอบให้ถูกต้องตรงกัน (Clock Synchronization) และเป็นมาตรฐานเดียวกัน

๕.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องใช้ค่าอ้างอิงเวลานาฬิกาของ*ระบบสารสนเทศ* จากเวลามาตรฐานสากล (Stratum 0) หรือ GPS Clock และมีความผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

๖. การจัดการช่องโหว่ทางเทคนิคของ*ระบบสารสนเทศ*

๖.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มีการตรวจสอบช่องโหว่ทางเทคนิคของ *ระบบสารสนเทศ* อย่างสม่ำเสมอ

๖.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มีการปิด/ลดช่องโหว่ทางเทคนิคที่เกิดขึ้นกับ *ระบบสารสนเทศ* เพื่อจัดการความเสี่ยงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย*ระบบสารสนเทศ*

๗. การสำรอง*ข้อมูล*

๗.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องกำหนด*ข้อมูล*ทั้ง*ซอฟต์แวร์ ระบบปฏิบัติการ แอปพลิเคชัน* และการตั้งค่าระบบ (Configuration/Parameter) ที่จำเป็นต่าง ๆ ของ*ระบบสารสนเทศ* เพื่อการสำรองข้อมูลไว้ใช้งานในกรณีฉุกเฉิน

๗.๒ *ผู้ดูแลระบบสารสนเทศ*กำหนดแผนงาน ความถี่ และรูปแบบการสำรอง*ข้อมูล*

๗.๓ *ผู้ดูแลระบบสารสนเทศ*ดำเนินการสำรอง*ข้อมูล* และทดสอบการกู้คืน*ข้อมูล*ตามแผนงาน

๗.๔ *ผู้ดูแลระบบสารสนเทศ*วิเคราะห์และรายงานนำเสนอแนวทางแก้ไขข้อผิดพลาดที่เกิดจากการสำรอง*ข้อมูล* และการทดสอบการกู้คืน*ข้อมูล*

๘. การบำรุงรักษา*ระบบสารสนเทศ*

๘.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดทำแผนบำรุงรักษา*ระบบสารสนเทศ*

๘.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องบำรุงรักษา*ระบบสารสนเทศ*ตามแผนที่กำหนด

๘.๓ *ผู้ดูแลระบบสารสนเทศ*ต้องวิเคราะห์และรายงานผลการบำรุงรักษา นำเสนอแนวทางการป้องกันความเสี่ยงที่อาจส่งผลกระทบต่อการให้บริการ

บทที่ ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ
๒. สารสนเทศอำนวยการ
๓. สารสนเทศวิจัยและพัฒนา
๔. สารสนเทศสนับสนุน
๕. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อจัดให้มีการกำหนดและควบคุมสิทธิการเข้าถึงระบบเครือข่ายสารสนเทศ ให้มีความมั่นคงปลอดภัย
๒. เพื่อกำหนดให้มีการแบ่งแยกกลุ่มการให้บริการเครือข่ายอย่างเป็นสัดส่วน
๓. เพื่อให้มีการเฝ้าระวังและตรวจสอบอุปกรณ์เครือข่ายที่ให้บริการได้อย่างมั่นคงปลอดภัย

แนวปฏิบัติ

๑. ผู้ดูแลระบบเครือข่ายสารสนเทศต้องกำหนดและควบคุมสิทธิการเข้าถึงระบบเครือข่ายสารสนเทศทั้งก่อนและขณะใช้งาน ตามสิทธิที่ได้รับอนุญาตจาก *ผู้บริหารระบบเครือข่ายสารสนเทศ*เท่านั้น
๒. *ผู้ดูแลระบบเครือข่ายสารสนเทศ*ต้องควบคุมการเข้าถึงเครือข่ายจากระยะไกล และต้องกำหนดช่องทางการให้บริการของ *ระบบสารสนเทศ*ที่จำเป็นต่อการให้บริการอย่างปลอดภัย สามารถตรวจสอบและป้องกันการปรับตั้งค่าระบบเครือข่ายสารสนเทศที่ไม่ได้รับอนุญาตได้
๓. ผู้ดูแลระบบเครือข่ายสารสนเทศต้องตั้งค่าการเชื่อมต่อเครือข่ายไร้สายให้มีการยืนยันตัวตนด้วยบัญชีผู้ใช้งานและรหัสผ่านก่อนเข้าใช้งานเป็นอย่างน้อย
๔. ผู้ดูแลระบบเครือข่ายสารสนเทศต้องจำกัดการเข้าถึงอุปกรณ์สารสนเทศที่เชื่อมต่อกับระบบเครือข่ายสารสนเทศที่ไม่ได้รับอนุญาต
๕. *ผู้ดูแลระบบเครือข่ายสารสนเทศ*ต้องจัดกลุ่มการให้บริการเครือข่ายตามประเภทของ *ระบบสารสนเทศ*อย่างเป็นสัดส่วน และป้องกันการเข้าถึง*ข้อมูล*บนระบบสารสนเทศที่ไม่ได้รับอนุญาต โดยจัดกลุ่มการให้บริการเป็นเครือข่ายภายใน และภายนอก เช่น Internal Zone External Zone Demilitarized Zone (DMZ) เป็นต้น
๖. ผู้ดูแลระบบเครือข่ายสารสนเทศต้องควบคุมการจัดเส้นทางบนระบบเครือข่ายและการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ
๗. *ผู้ดูแลระบบเครือข่ายสารสนเทศ*ต้องจัดให้มีการเฝ้าระวังเหตุผิดปกติ หรือภัยคุกคามด้านความมั่นคงปลอดภัย*ระบบสารสนเทศ* ผ่านทางระบบเครือข่ายสารสนเทศ

๘. *ผู้ดูแลระบบเครือข่ายสารสนเทศ*ต้องจัดทำแผนผังเครือข่าย (Network Diagram) และ*ข้อมูล*การตั้งค่าของอุปกรณ์เครือข่าย โดยต้องปรับปรุงให้เป็นปัจจุบัน และต้องควบคุมการเข้าถึงได้เฉพาะผู้ที่มีสิทธิเข้าถึงเท่านั้น

๙. ผู้ดูแลระบบเครือข่ายสารสนเทศต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์เครือข่ายได้ เช่น หมายเลข IP Address หรือหมายเลข Mac Address เป็นต้น

๑๐. ผู้ดูแลระบบเครือข่ายสารสนเทศต้องตั้งค่าอุปกรณ์รักษาความมั่นคงปลอดภัยทางเครือข่าย (เช่น Firewall) เพื่อป้องกันการเข้าถึงหมายเลข IP Address ของอุปกรณ์สารสนเทศภายในบริษัทฯ จากภายนอกโดยตรง

๑๑. ผู้ดูแลระบบเครือข่ายสารสนเทศต้องกำหนดค่าเริ่มต้นพื้นฐานของระบบเครือข่ายต้องเป็นแบบอนุญาตบางส่วนและปฏิเสธทั้งหมด (Permit any & Deny all)

๑๒. ผู้ดูแลระบบเครือข่ายสารสนเทศต้องเปิดเฉพาะพอร์ตที่จำเป็นต่อการให้บริการเท่านั้น และปิดพอร์ตที่ไม่จำเป็นต่อการให้บริการ ทั้งการเข้าถึงพอร์ตทางกายภาพและทางเครือข่าย

๑๓. *ผู้ดูแลระบบเครือข่ายสารสนเทศ*ต้องจัดให้มีการป้องกันระบบสายสัญญาณที่ใช้ในการสื่อสารไม่ให้สามารถดักจับสัญญาณ หรือทำให้เกิดความเสียหายขึ้นได้

บทที่ ๑๐ การจัดหา จัดจ้าง และพัฒนาระบบสารสนเทศ

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ

๒. สารสนเทศอำนวยการ

๓. สารสนเทศวิจัยและพัฒนา

๔. สารสนเทศสนับสนุน

๕. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อจัดให้มีข้อกำหนดด้านความมั่นคงปลอดภัยการพัฒนา*ระบบสารสนเทศ*

๒. เพื่อควบคุมการพัฒนา*ระบบสารสนเทศ*ให้เป็นไปตามข้อกำหนดการพัฒนา*ระบบสารสนเทศ* และมีความมั่นคงปลอดภัย

แนวปฏิบัติ

๑. การพัฒนา*ระบบสารสนเทศ*

๑.๑ *ผู้พัฒนาระบบสารสนเทศ*ต้องควบคุมการพัฒนา*ระบบสารสนเทศ* เพื่อให้มีความมั่นคงปลอดภัย โดยมีข้อกำหนดอย่างน้อยดังนี้

๑.๑.๑ มีการประเมินความเสี่ยงจากการถูกโจมตีจากภัยคุกคามต่าง ๆ วิเคราะห์ออกแบบ ให้มีการป้องกันและรักษาความปลอดภัยที่จะเกิดขึ้นจากทั้งภายในและภายนอกของ*ระบบสารสนเทศ*ที่จะพัฒนา

๑.๑.๒ มีการควบคุมและตรวจสอบ*ข้อมูล*นำเข้า – นำออกจากระบบ (Input – Output validation) และ/หรือมีการเข้ารหัสลับ (Encryption) ที่เป็นไปตามความเหมาะสม หรือเป็นไปตามมาตรฐานที่กำหนดของ*ระบบสารสนเทศ*

๑.๑.๓ มีการควบคุมการเชื่อมโยงกับระบบอื่น ๆ (Interface with other system)

๑.๑.๔ มีการบันทึก*ข้อมูล Log* เพื่อแสดงการทำงาน เหตุการณ์ต่าง ๆ ที่เกิดขึ้นกับ*ระบบสารสนเทศ*

๑.๑.๕ มีการควบคุมการเปลี่ยนแปลง*ระบบสารสนเทศ*ที่พัฒนา

๑.๑.๖ มีการควบคุมการเข้าถึง*ข้อมูล*ตามสิทธิ

๑.๑.๗ มีการวิเคราะห์ผลกระทบต่อธุรกิจ

๑.๑.๘ มีการป้องกัน*ข้อมูล*เมื่อมีการส่ง*ข้อมูล*ผ่านเครือข่ายสาธารณะ ไม่ให้มีการรั่วไหล หรือรับส่ง*ข้อมูล*ที่ไม่สมบูรณ์ หรือถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

๑.๒ *ผู้บริหารการพัฒนาระบบสารสนเทศ*ต้องกำหนดหน้าที่รับผิดชอบของ*ผู้พัฒนาระบบสารสนเทศ* โดยแยกหน้าที่การพัฒนา และการทดสอบออกจากกัน

๑.๓ *ผู้บริหารการพัฒนาระบบสารสนเทศ*ต้องจัดให้มีการตรวจรับ ทดสอบด้านความมั่นคงปลอดภัย (Security test) ของ*ระบบสารสนเทศ*ที่พัฒนาแล้วเสร็จ ก่อนนำไปใช้ในการปฏิบัติงานจริง

๑.๔ *ผู้พัฒนาระบบสารสนเทศ*ต้องจัดเก็บ Source code และ*ข้อมูล*การตั้งค่าซอฟต์แวร์ที่ใช้ในการพัฒนา*ระบบสารสนเทศ*ไว้ในที่ปลอดภัย และต้องป้องกันการแก้ไขหรือดัดแปลง Source code โดยไม่ได้รับอนุญาต

๑.๕ *ผู้พัฒนาระบบสารสนเทศ*ต้องใช้ข้อมูลจำลองในการทดสอบระบบ และป้องกัน*ข้อมูล*ดังกล่าวไม่ให้มีการเปิดเผย แก้ไข หรือลบ*ข้อมูล*ดังกล่าว โดยไม่ได้รับอนุญาต

๑.๖ *ผู้พัฒนาระบบสารสนเทศ*ต้องไม่ใช้ข้อมูลส่วนบุคคล ข้อมูลที่ต้องระมัดระวังในการเปิดเผยต่อบุคคลอื่น (Sensitive data) และ*ข้อมูล*ที่มีชั้นความลับสำหรับการทดสอบระบบโดยไม่ได้รับอนุญาต หากจำเป็นต้องใช้*ข้อมูล*ดังกล่าว ต้องเป็นการสำเนา*ข้อมูล*ดังกล่าวเพื่อการทดสอบ โดยต้องป้องกันไม่ให้มีการเปิดเผยโดยไม่ได้รับอนุญาต และต้องทำลาย*ข้อมูล*ดังกล่าวเมื่อการทดสอบแล้วเสร็จ

๑.๗ *ผู้ดูแลระบบสารสนเทศ*จัดให้มีระบบที่ใช้ในการพัฒนาแยกออกจาก*ระบบสารสนเทศ*ที่ใช้งานจริง

๒. การจ้างพัฒนาระบบสารสนเทศ

๒.๑ *ผู้พัฒนาระบบสารสนเทศ*ต้องกำหนดให้สัญญาจ้างพัฒนา*ระบบสารสนเทศ* มีข้อกำหนดด้านความมั่นคงปลอดภัยตามแนวปฏิบัติการพัฒนา*ระบบสารสนเทศ*ข้อ ๑.๑ เป็นอย่างน้อย

๒.๒ *ผู้พัฒนาระบบสารสนเทศ*ต้องควบคุม*ผู้รับจ้างพัฒนาระบบสารสนเทศ* ไม่ให้เข้าถึง*ระบบสารสนเทศ*โดยไม่ได้รับอนุญาต

บทที่ ๑๑ การกำกับดูแลผู้รับจ้าง

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ
๒. สารสนเทศอำนวยการ
๓. สารสนเทศวิจัยและพัฒนา
๔. สารสนเทศสนับสนุน
๕. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อกำกับดูแลการดำเนินงานของ*ผู้รับจ้าง*ให้ปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ*
๒. เพื่อควบคุมการใช้งาน*ทรัพย์สินสารสนเทศ*ของ*ผู้รับจ้าง* เมื่อเชื่อมต่อกับ*ระบบสารสนเทศ*ของ*บริษัทฯ*

แนวปฏิบัติ

๑. *ผู้ดูแลระบบสารสนเทศ*กำกับดูแลการดำเนินงานของ*ผู้รับจ้าง*ให้ปฏิบัติตามนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* โดยเคร่งครัด อย่างสม่ำเสมอ
๒. *ผู้ดูแลระบบสารสนเทศ*ต้องควบคุมไม่ให้*ผู้รับจ้าง*ดำเนินการใด ๆ ที่เกี่ยวกับ*ระบบสารสนเทศ*ของ*บริษัทฯ* ก่อนได้รับอนุญาตจาก*ผู้บริหารระบบสารสนเทศ*
๓. *ผู้ดูแลระบบสารสนเทศ*ต้องควบคุมไม่ให้*ผู้รับจ้าง*เชื่อมต่อ*อุปกรณ์สารสนเทศ*กับ*ระบบสารสนเทศ*ของ*บริษัทฯ* ก่อนได้รับอนุญาตจาก*ผู้บริหารระบบสารสนเทศ*
๔. *ผู้ดูแลระบบสารสนเทศ*ต้องควบคุมไม่ให้*ผู้รับจ้าง*นำ*ซอฟต์แวร์*ที่ละเมิดลิขสิทธิ์มาใช้ในการปฏิบัติงานของ*บริษัทฯ*

บทที่ ๑๒ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ
๒. สารสนเทศอำนวยการ
๓. สารสนเทศวิจัยและพัฒนา
๔. สารสนเทศสนับสนุน
๕. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อให้มีการบริหารจัดการ*เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ*ให้สอดคล้องตามกฎหมาย
๒. เพื่อกำหนดแนวทางการเผชิญเหตุและรายงาน*เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ*

แนวปฏิบัติ

๑. *ผู้ใช้งาน*ต้องแจ้งเหตุผิดปกติใด ๆ ที่เกิดขึ้นกับ *ระบบสารสนเทศ* หรือเมื่อพบจุดอ่อนที่อาจส่งผลกระทบต่อ*ระบบสารสนเทศ*กับ*ผู้ดูแลระบบสารสนเทศ*ทันที
๒. *ผู้ดูแลระบบสารสนเทศ* รับแจ้งเหตุ เฝ้าระวัง สังเกต วิเคราะห์ผลกระทบ แจ้งรายงานเหตุเบื้องต้น และเข้าเผชิญเหตุ แก้ไข*เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ*
๓. *ผู้ดูแลระบบสารสนเทศ* รายงานผลการดำเนินงาน และนำเสนอแนวทางป้องกัน เพื่อลดผลกระทบจาก*เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ*ต่อคณะบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ และเพื่อเป็นหลักฐาน หรือประยุกต์ใช้เป็นบทเรียนในการลดโอกาสและผลกระทบของเหตุที่อาจจะเกิดขึ้นได้อีกในอนาคต
๔. *ผู้ดูแลระบบสารสนเทศ* รวบรวมข้อมูล ขั้นตอนการดำเนินการในการแก้ไขปัญหา ประเมินความเสี่ยง จัดทำและทบทวนแผนเผชิญ*เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ* และจัดให้มีการทดสอบขั้นตอนการปฏิบัติตามแผนอย่างน้อยปีละ ๑ ครั้ง
๕. คณะบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ วิเคราะห์ ประเมินผลกระทบ สืบสวน สอบสวน รวบรวมและจัดเก็บหลักฐาน เมื่อเกิด*เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ* และรายงานผลการดำเนินงาน พร้อมทั้งแนวทางการบริหารจัดการ*เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ* ต่อคณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร
๖. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงต้องรายงานให้กรรมการผู้อำนวยการใหญ่ทราบ เพื่อขอการสนับสนุนจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (ThaiCERT) หรือหน่วยงานที่เกี่ยวข้อง ในกรณีไม่สามารถแก้ไขและควบคุมผลกระทบที่เกิดขึ้นได้

๓. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงรายงาน *เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ*ที่มีผลกระทบอย่างมีนัยสำคัญ ต่อคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ (กกม.) ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

บทที่ ๑๓ การบริหารความต่อเนื่องทางธุรกิจด้านความมั่นคงปลอดภัย ระบบสารสนเทศ

ขอบเขต

๑. สารสนเทศบริการการเดินอากาศ

๒. สารสนเทศอำนวยการ

๓. สารสนเทศสนับสนุน

๔. สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อจัดให้มีแผนความต่อเนื่องทางธุรกิจด้านความมั่นคงปลอดภัย *ระบบสารสนเทศของ บริษัทฯ*

๒. เพื่อจัดให้มีการทบทวนและซ้อมแผนความต่อเนื่องทางธุรกิจด้านความมั่นคงปลอดภัย *ระบบสารสนเทศของบริษัทฯ* อย่างสม่ำเสมอ

๓. เพื่อจัดให้มีระบบสำรองให้มีความพร้อมใช้ และใช้งานทดแทนระบบหลักได้

แนวปฏิบัติ

๑. การบริหารความต่อเนื่องทางธุรกิจ *ระบบสารสนเทศ*

๑.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มี *ระบบสารสนเทศ*สำรอง เพื่อให้มี *ระบบสารสนเทศ* พร้อมใช้งานทดแทนระบบหลักได้อย่างต่อเนื่อง

๑.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้ *ระบบสารสนเทศ*หลักและ *ระบบสารสนเทศ*สำรอง มี*ซอฟต์แวร์*และ*ข้อมูล*ที่ใช้ในการทำงานที่เหมือนกัน โดยมีการสำรอง *ข้อมูล*อย่างต่อเนื่อง และสามารถทำงานทดแทนกันได้

๑.๓ *ผู้ดูแลระบบสารสนเทศ*ต้องทดสอบระบบสำรองอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าระบบสำรองสามารถทำงานทดแทนระบบหลักได้

๒. แผนความต่อเนื่องทางธุรกิจด้านความมั่นคงปลอดภัย *ระบบสารสนเทศ*

๒.๑ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มีแผนความต่อเนื่องทางธุรกิจที่ครอบคลุมด้านความมั่นคงปลอดภัย*ระบบสารสนเทศ* และต้องมีการทบทวนแผนอย่างน้อยปีละ ๑ ครั้ง

๒.๒ *ผู้ดูแลระบบสารสนเทศ*ต้องจัดให้มีขั้นตอนปฏิบัติในการเผชิญเหตุต่อความเสียหายของ *ระบบสารสนเทศ* และมีการซักซ้อมขั้นตอนการปฏิบัติงานตามแผนความต่อเนื่องทางธุรกิจที่กำหนด

บทที่ ๑๔ การปฏิบัติตามข้อกำหนด

ขอบเขต

๑ สารสนเทศบริการการเดินอากาศ

๒ สารสนเทศอำนวยการ

๓ สารสนเทศวิจัยและพัฒนา

๔ สารสนเทศสนับสนุน

๕ สารสนเทศธุรกิจ

วัตถุประสงค์

๑. เพื่อให้มีการควบคุมการใช้งาน*ระบบสารสนเทศ*ให้เป็นไปตามกฎหมาย ระเบียบข้อบังคับ หรือข้อตกลงตามสัญญาที่เกี่ยวข้อง

๒. เพื่อให้มีการทบทวนนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* ให้สอดคล้องกับกฎหมาย

แนวปฏิบัติ

๑. *ผู้ดูแลงานนิติการ*ต้องติดตาม/กำกับ/ดูแล/ตรวจสอบ ข้อกฎหมาย ระเบียบ หรือข้อตกลงที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* ให้เป็นปัจจุบันอย่างสม่ำเสมอ

๒. *ผู้ดูแลระบบสารสนเทศ*ต้องควบคุมการนำ*ซอฟต์แวร์*ละเมิดลิขสิทธิ์มาใช้งานใน*บริษัทฯ*

๓. *ผู้ดูแลระบบสารสนเทศ*ต้องเสนอแนวทางหรือข้อเสนอแนะ ในการทบทวนนโยบาย/แนวปฏิบัติ/วิธีปฏิบัติ/มาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย*ระบบสารสนเทศ*ของ*บริษัทฯ* ให้สอดคล้องกับกฎหมาย ระเบียบ หรือข้อตกลงที่เกี่ยวข้อง

๔. *ผู้ดูแลระบบสารสนเทศ*ต้องป้องกัน*ข้อมูล*บน*ระบบสารสนเทศ* ไม่ให้เกิดความเสียหาย สูญหาย ถูกปลอมแปลง หรือถูกเผยแพร่โดยไม่ได้รับอนุญาต ตามกฎหมายหรือข้อตกลงตามสัญญาที่เกี่ยวข้อง

กฎหมายและมาตรฐานที่เกี่ยวข้อง

๑. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔
๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
๓. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๔. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๕. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙
๖. พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
๗. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕
๘. ประกาศคณะกรรมการการบินพลเรือน เรื่อง แผนรักษาความปลอดภัยในการบินพลเรือนแห่งชาติ พ.ศ. ๒๕๖๓
๙. มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013