มาตรการการรักษาความมั่นคงปลอดภัย ระบบสารสนเทศของ รร.การบิน พ.ศ.๒๕๖๖

สารบัญ

มาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน

๑. หลักการและเหตุผล

ในปัจจุบันมีการใช้ระบบสารสนเทศในหน่วยงานมากขึ้น ทำให้มีภัยคุกคามหลากหลายประเภทตามมา ดังนั้น หน่วยงานที่ไม่มีการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างรัดกุมจึงมีความเสี่ยงที่จะเกิดผลกระทบจากภัยคุกคามต่าง ๆ เหล่านั้น หน่วยงานจึงจำเป็นที่จะต้องยกระดับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายขององค์กร เพื่อลดความเสี่ยงดังกล่าว โดยในปัจจุบันเป็นที่ยอมรับกันว่า คอมพิวเตอร์และอุปกรณ์สารสนเทศ ได้กลายเป็นส่วนหนึ่งของชีวิต มีบทบาทในงานต่าง ๆ เกือบทุกด้านในสังคมมนุษย์ การนำคอมพิวเตอร์และอุปกรณ์สารสนเทศมาใช้ในหน่วยงานนั้นจำเป็นจะต้องไปสัมพันธ์กับเจ้าหน้าที่และผู้ปฏิบัติจำนวนมาก บุคคลเหล่านี้มีแนวคิดและทัศนคติแตกต่างกันออกไป ดังนั้น เพื่อให้การรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ รร.การบิน สามารถดำเนินการได้อย่างมีประสิทธิภาพ จึงจำเป็นต้องมีระเบียบปฏิบัติที่ชัดเจน

๒. วัตถุประสงค์

๒.๑ เพื่อให้การรักษาความมั่นคงปลอดภัยการใช้งานในระบบสารสนเทศของ รร.การบิน ดำเนินงานไปได้อย่างมีประสิทธิภาพ และเกิดประสิทธิผล

๒.๒ เพื่อเป็นมาตรฐานและแนวทางปฏิบัติรวมทั้งกำหนดความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บังคับบัญชากำลังพลของหน่วย ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับ รร.การบิน เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศของ รร.การบิน

๒.๓ เพื่อเป็นกรอบและแนวทางการปรับปรุงพัฒนาระบบสารสนเทศของ รร.การบิน ยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไปสู่สากล

๒.๔ เพื่อเป็นมาตรการในการรักษาความปลอดภัยระบบสารสนเทศของ รร.การบิน สำหรับการพิทักษ์รักษาและป้องกัน มิให้ข้อมูลและสิ่งที่เป็นความลับของทางราชการ รั่วไหล หรือตกไปอยู่ในมือของฝ่ายตรงข้ามหรือบุคคลผู้ไม่มีอำนาจหน้าที่ ป้องกันการจารกรรมทั้งจากบุคคลภายในและภายนอกส่วนราชการ พิทักษ์รักษาและป้องกันการก่อวินาศกรรมแก่เครื่องคอมพิวเตอร์ อุปกรณ์สารสนเทศเครื่องใช้สำนักงาน อาคาร สถานที่ และเอกสารที่เกี่ยวข้องกับระบบสารสนเทศ เป็นต้น

๓. ความสำคัญ

ข้าราชการ ลูกจ้าง และพนักงานราชการ รร.การบิน มีสิทธิ์ใช้เครือข่ายคอมพิวเตอร์และอุปกรณ์สารสนเทศได้ภายใต้ข้อกำหนดตามมาตรการนี้ การฝ่าฝืนข้อกำหนดดังกล่าว หรือการกระทำที่อาจก่อให้เกิดความเสียหายแก่หน่วยงาน หรือบุคคลใดบุคคลหนึ่ง หน่วยงานจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ข้าราชการ ลูกจ้าง และพนักงานราชการที่ฝ่าฝืนทันที

๔. ผู้รับผิด...

๔. ผู้รับผิดชอบหลัก

ข้าราชการ ลูกจ้าง และพนักงานราชการ รร.การบิน

๕. คำนิยามที่เกี่ยวข้อง

๕.๑ หน่วยงาน หมายถึง หน่วยขึ้นตรงของ รร.การบิน

๕.๒ ผู้ใช้งาน (User) หมายถึง ข้าราชการ พนักงานราชการ และลูกจ้างของ รร.การบิน ที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศของ รร.การบิน รวมถึงบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของ รร.การบิน

๕.๓ สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๕.๔ สินทรัพย์ หมายความว่า สิ่งที่มีคุณค่าสำหรับองค์กรหรือหน่วยงาน

๕.๕ ทรัพย์สินสารสนเทศ หมายความว่า

๕.๕.๑ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๕.๕.๒ เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

๕.๕.๓ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๕.๖ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๕.๗ ระบบสารสนเทศ (Information System) หมายความว่า ระบบที่ประกอบด้วย บุคคล ระบบคอมพิวเตอร์ ซอฟต์แวร์ ฐานข้อมูล เครือข่ายสารสนเทศ และกระบวนการ ได้แก่ วิธีการสร้างข้อมูล วิธีการประมวลผลข้อมูล วิธีการเก็บข้อมูล และวิธีการแสดงผล โดยทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อเปลี่ยนข้อมูลให้เป็นสารสนเทศและส่งการแสดงผลให้ผู้ใช้งานสามารถนำไปใช้ประโยชน์ในการปฏิบัติงานหรือสนับสนุนการปฏิบัติภารกิจของหน่วยงาน ซึ่งมีองค์ประกอบดังนี้

๕.๗.๑ ระบบคอมพิวเตอร์ (Computer System) หมายถึง ระบบที่ประกอบด้วย ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และบุคลากรทางคอมพิวเตอร์ (People ware)

๕.๗.๒ เครือข่ายคอมพิวเตอร์ (Computer Network) หมายความว่า การติดต่อสื่อสารหรือการรับ - ส่งข้อมูลระหว่างระบบสารสนเทศภายใน รร.การบิน และหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับ รร.การบิน

๕.๗.๓ สารสนเทศ (Information) หมายความว่า สิ่งที่มีต้นกำเนิดจากข้อมูล เช่น ตัวอักษร ตัวเลข ข้อความ รูปภาพ เป็นต้น โดยการได้มาซึ่งสารสนเทศนั้น ต้องมีการนำข้อมูลผ่านการประมวลผลการจัดระเบียบด้วยวิธีต่าง ๆ เช่น การประมวลผลด้วยระบบคอมพิวเตอร์ การประมวลผลภายในระบบสารสนเทศเป็นต้น

เพื่อให้ข้อ...

เพื่อให้ข้อมูลเหล่านั้นอยู่ในรูปแบบที่มีความหมาย ผู้ใช้งานสามารถเข้าใจได้ และนำไปใช้ประโยชน์ในการปฏิบัติงาน การบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๕.๘ จดหมายอิเล็กทรอนิกส์ (Electronic Mail : E-mail) หมายถึง การรับ - ส่งข้อมูลผ่านอินเทอร์เน็ตหรืออินทราเน็ต โดยชื่อที่ใช้ในการรับ - ส่งจดหมายอิเล็กทรอนิกส์ จะมีรูปแบบซึ่งประกอบไปด้วย ๒ ส่วน คือ ชื่อผู้ใช้งาน และชื่อโดเมน ดังตัวอย่าง user@rtaf.mi.th เป็นต้น

๕.๙ ผู้ดูแลระบบ (System Administrator) หมายถึง นายทหารสัญญาบัตร หรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลระบบสารสนเทศของหน่วยงานนั้น ๆ

๕.๑๐ ผู้ดูแลเครือข่าย (Network Administrator) หมายถึง นายทหารสัญญาบัตร หรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลเครือข่ายสารสนเทศของหน่วยงานนั้น ๆ

๕.๑๑ ผู้ดูแลฐานข้อมูล (Database Administrator) หมายถึง นายทหารสัญญาบัตร หรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลฐานข้อมูล

๕.๑๒ ผู้บังคับบัญชา หมายถึง หัวหน้าหน่วยงานของผู้ปฏิบัติหน้าที่ในระบบสารเทศของหน่วยงานนั้น ๆ

๕.๑๓ ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า ความมั่นคงและความปลอดภัยในบริบทของ การรักษาความลับ ความเชื่อถือได้ และความพร้อมใช้งานของข้อมูล สำหรับระบบสารสนเทศของ รร.การบิน

๕.๑๔ เหตุการณ์ด้านความมั่นคงปลอดภัย (Security incidents) หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของ รร.การบิน หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อนหรืออาจสร้างความเสียหายได้ในที่สุดซึ่งอาจส่งผลให้

๕.๑๔.๑ เกิดการหยุดชะงักต่อกระบวนการ หรือขั้นตอนการปฏิบัติงานสำคัญ หรือระบบงานสารสนเทศของหน่วยเกิดการหยุดชะงัก

๕.๑๔.๒ เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของ รร.การบิน

๕.๑๔.๓ เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับหรือข้อกำหนดต่าง ๆ ที่กำหนดไว้

๕.๑๔.๔ เกิดภาพลักษณ์ที่ไม่ดีต่อ รร.การบิน หรือทำให้สูญเสียชื่อเสียง ดังตัวอย่าง การไปโพสต์ข้อความพาดพิงถึง รร.การบิน ในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของ รร.การบิน เป็นต้น

๕.๑๕ สิทธิของผู้ใช้งาน (User Access Right) หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของ ทอ. หรือ เพื่อการเข้าถึงเข้าใช้สารสนเทศและทรัพย์สินสารสนเทศของ รร.การบิน

๕.๑๖ การเข้าถึง (Access) หมายถึง ความสามารถในการเข้าไป อันอาจทำให้สามารถจะอ่าน ทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใด ๆ หรือได้อ่าน ทำ สร้าง แก้ไข ปรับปรุง

เปลี่ยนแปลง...

เปลี่ยนแปลง ล่วงรู้ด้วยประการใด ๆ สำหรับข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ สารสนเทศระบบคอมพิวเตอร์ ระบบสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์และวิธีการทางกายภาพ

๕.๑๗ การควบคุมการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๕.๑๘ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง เหตุบกพร่องหรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบของ รร.การบิน สูญเสียการปฏิบัติงาน รวมถึงการให้บริการต่าง ๆ แต่เพียงบางส่วนหรือทั้งหมด จากการถูกบุกรุกหรือโจมตีทางช่องโหว่และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามรูปแบบต่าง ๆ

๕.๑๙ ภัยคุกคาม (Threats) หมายถึง เหตุการณ์ต่างๆ ที่เป็นไปได้หรือเหตุการณ์ที่ไม่พึงประสงค์ซึ่งอาจส่งผลกระทบหรือสร้างความเสียหายต่อระบบสารสนเทศของ รร.การบิน

๕.๒๐ ช่องโหว่ (Vulnerabilities) หมายถึง จุดอ่อนของทรัพย์สินหรือมาตรการ ที่เป็นช่องทางเกิดปัจจัยเสี่ยงจากภัยคุกคามที่มีผลกระทบต่อทรัพย์สินหรือต่อระบบสารสนเทศของ รร.การบิน

๕.๒๑ ให้ นทสส.รร.การบิน เป็นผู้รักษาการให้เป็นไปตามมาตรการนี้ และให้กำหนดการทบทวนมาตรการให้มีความทันสมัย อย่างต่อเนื่อง โดยมีวงรอบตามเห็นสมควร

๖. แนวทางการปฏิบัติทั่วไป

๖.๑ ให้ผู้ใช้งานที่ถือครองเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นในกรณีที่เครื่องคอมพิวเตอร์นั้นเกิดความเสียหาย หรือสูญหายไป

๖.๒ ให้ผู้ใช้งานตรวจสอบว่า โปรแกรมป้องกันไวรัสยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ ต้องทำการตรวจสอบอย่างน้อยวันละ ๑ ครั้ง หากพบว่าทำงานผิดปกติให้แจ้ง นทสส.รร.การบิน เพื่อดำเนินการแก้ไขโดยทันที

๖.๓ ให้ผู้ใช้งานปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ (Server) ให้บริการที่ต้องใช้งานตลอด ๒๔ ชั่วโมง

๖.๔ ให้ผู้ใช้งานทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๐ นาที

๖.๕ ให้ผู้ใช้งานกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์แบบพกพา

๖.๖ ให้ผู้ใช้งานลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตนเพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

๖.๗ ให้ผู้ใช้...

๖.๗ ให้ผู้ใช้งานระมัดระวังการใช้งาน และสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคล และระบบเครือข่ายเหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและระบบเครือข่ายแล้วแต่กรณี

๖.๘ ห้ามผู้ใช้งานติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมที่นอกเหนือจากที่หน่วยงานได้ติดตั้งไว้ให้ใช้งานโดยไม่ได้รับอนุญาตจาก นทสส.รร.การบิน

๖.๙ ห้ามผู้ใช้งานติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้น หรือระบบเครือข่ายของหน่วยงานได้

๖.๑๐ กรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกสำนักงานจะต้องได้รับอนุมัติจากผู้มีอำนาจในการนำทรัพย์สินออกก่อนทุกครั้ง

๖.๑๑ ให้ทำการติดตั้งเครื่องสำรองไฟฟ้า (UPS) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีการใช้งานข้อมูลเป็นปริมาณมากและมีความถี่ในการใช้งานสูง

๖.๑๒ ห้ามทำการปรับแต่งค่าระบบที่ได้รับจากการติดตั้งแต่เริ่มแรกอย่างเด็ดขาด เพราะอาจทำให้เกิดความเสียหายต่อระบบการทำงานของเครื่องคอมพิวเตอร์

๖.๑๓ ห้ามทำการถอดหรือเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ได้รับการติดตั้งไว้ โดยไม่ได้แจ้งให้กับผู้ดูแลระบบคอมพิวเตอร์ที่รับผิดชอบทราบล่วงหน้า

๖.๑๔ ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ ตู้กระจายสัญญาณ (Rack, Switch) ก่อนได้รับอนุญาต

๖.๑๕ ผู้ใช้งานคอมพิวเตอร์ต้องรับทราบ รวมถึงทำความเข้าใจและปฏิบัติตามระเบียบ ทอ. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ อย่างเคร่งครัด

๗. แนวทางการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์คอมพิวเตอร์

๗.๑ เครื่องคอมพิวเตอร์ที่หน่วยอนุญาตให้ผู้ใช้งาน ใช้งานเป็นสิ่งอุปกรณ์หรือทรัพย์สินของ รร.การบิน ดังนั้น ผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพต่อการปฏิบัติงานของ รร.การบิน เท่านั้น

๗.๒ ระบบปฏิบัติการที่ติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ รร.การบิน ที่เป็นระบบที่ถูกลิขสิทธิ์ในรูปแบบ Digital License ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๗.๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงานโดยไม่ได้รับอนุญาตจาก นทสส.รร.การบิน

๗.๔ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์สารสนเทศใด ๆ เข้าไปในระบบและเครือข่ายสารสนเทศของ รร.การบิน โดยไม่ได้รับอนุญาตจาก นทสส.รร.การบิน

๗.๕ การเคลื่อน...

๗.๕ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของ ผสอ.รร.การบิน, นทสส.รร.การบิน, จนท.สารสนเทศของหน่วยที่มีการแต่งตั้ง และผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์ที่ได้ทำสัญญากับ รร.การบิน เท่านั้น หากไม่มีหมายเลขพัสดุให้ผู้รับผิดชอบดำเนินการปกป้องข้อมูลที่เกี่ยวข้องกับราชการด้วยตนเองหรือแจ้ง นทสส.รร.การบิน หรือ จนท.สารสนเทศของหน่วยที่มีการแต่งตั้ง ก่อนนำเครื่องออกไปตรวจซ่อมกับผู้รับจ้างภายนอก

๗.๖ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๗.๗ ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่อง

๗.๘ ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสารที่หน่วยรับผิดชอบระบบงานสารสนเทศเป็นผู้กำหนดขึ้น

๗.๙ ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ Data Storage อื่น ๆ เป็นต้น ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของ รร.การบิน

๗.๑๐ ผู้ใช้งานต้องตรวจสอบแฟ้ม (File) ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (E-mail) หรือแฟ้ม (File) ที่ได้รับ (Download) มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๗.๑๑ ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นๆ เกิดความเสียหาย ถูกทำลาย แก้ไขเปลี่ยนแปลงหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๗.๑๒ ผู้ใช้งานคอมพิวเตอร์ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD และ External Hard Disk เป็นต้น

๗.๑๓ ผู้ใช้งานคอมพิวเตอร์มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๗.๑๔ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ส่วนบุคคล

๘. แนวทางการใช้งานเครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์สารสนเทศแบบพกพาอื่น ๆ

๘.๑ เครื่องคอมพิวเตอร์แบบพกพาที่ รร.การบิน เป็นอุปกรณ์หรือทรัพย์สินของ รร.การบิน ดังนั้นผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์ในการปฏิบัติงานของ รร.การบิน เท่านั้น

๘.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของ รร.การบิน เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๘.๓ ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๘.๔ ไม่ดัดแปลง...

๘.๔ ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และอุปกรณ์สารสนเทศรวมทั้งรักษาสภาพของคอมพิวเตอร์และอุปกรณ์สารสนเทศให้มีสภาพเดิม

๘.๕ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือ หลุดมือ เป็นต้น

๘.๖ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา ปลายดินสอ เป็นต้น กดสัมผัสหน้าจอแสดงผลให้เป็นรอยขีดข่วนหรือทำให้จอแสดงผลของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๘.๗ ไม่วางของที่มีน้ำหนักมากทับบนหน้าจอแสดงผลและแป้นพิมพ์

๘.๘ การเช็ดทำความสะอาดหน้าจอแสดงผลต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอแสดงผลมีรอยขีดข่วนได้

๘.๙ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ต้องเก็บเครื่องไว้ในสถานที่ที่มีอุปกรณ์ป้องกันขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เป็นต้น

๘.๑๐ ผู้ใช้งานต้องไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาและอุปกรณ์สารสนเทศแบบพกพาในสถานที่ที่มีความร้อน ความชื้น ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๘.๑๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

๘.๑๒ ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบงานสารสนเทศเป็นผู้กำหนดขึ้น

๘.๑๓ ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาหน้าจอแสดงผล (Screen Saver) โดยตั้งเวลาในกรณีไม่ได้ใช้งานในห้วงระยะเวลาขณะหนึ่ง เช่น ตั้งไว้ ๑๐ นาที เป็นต้น ให้ทำการปิดกั้นการใช้งาน (Lock) สำหรับหน้าจอแสดงผล หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

๘.๑๔ ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอแสดงผลเป็นเวลานาน

๘.๑๕ ห้ามบันทึกชื่อผู้ใช้งานและรหัสผ่านไว้บนสถานที่ที่พบเห็นได้ง่าย เช่น บันทึกไว้บนอุปกรณ์คอมพิวเตอร์ บันทึกไว้บนโต๊ะทำงาน เป็นต้น

๘.๑๖ ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบงานสารสนเทศเป็นผู้กำหนดขึ้น

๘.๑๗ ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

๘.๑๘ ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๘.๑๙ แผ่นสื่อ...

๘.๑๙ แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

๘.๒๐ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๙. แนวทางการใช้งานรหัสผ่าน

๙.๑ ผู้ใช้งานต้องใช้งานรหัสผ่านของตนเองหรือตามที่ได้รับอนุมัติเท่านั้น

๙.๒ ผู้ใช้งานต้องเก็บรักษารหัสผ่านที่ได้รับให้เป็นความลับ

๙.๓ ผู้ใช้งานต้องกำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยต้องมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษเข้าด้วยกัน

๙.๔ ผู้ใช้งานต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากวันเดือนปีเกิด, จากชื่อ - นามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๙.๕ ผู้ใช้งานต้องไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๙.๖ ผู้ใช้งานต้องไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Auto Save Password)

๙.๗ ผู้ใช้งานต้องไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๙.๘ กรณีที่ผู้ใช้งานมีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นไม่ว่ากรณีใดก็ตามเพื่อการปฏิบัติงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๙.๙ ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย ๕ รหัสผ่าน

๙.๑๐ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ ๑๘๐ วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๙.๑๑ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

๙.๑๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของ รร.การบิน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อคก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบโดยทันที

๙.๑๒.๑ คอมพิวเตอร์โน้ตบุ๊ค (Notebook) ต้องทำการพิสูจน์ตัวตนในระดับไบออส (BIOS) ก่อนการใช้งาน

๙.๑๒.๒ คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

๙.๑๒.๓ การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

๙.๑๒.๔ การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๙.๑๒.๕ เมื่อผู้ใช้...

๙.๑๒.๕ เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์หรืออุปกรณ์สารสนเทศแบบพกพา เช่น Tablet ต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

๙.๑๒.๖ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๑๐ นาที และมีการใช้รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

๑๐. แนวทางการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

ผู้ดูแลระบบ (System Administrator) ต้องเป็นผู้รับผิดชอบในการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานทั้งหมดอย่างสม่ำเสมอเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางดังนี้

๑๐.๑ วงรอบการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานให้ทบทวนทุก ๆ ๑ ปี หรือเมื่อเกิดการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งาน ได้แก่ การลาออก การย้ายหน่วย เป็นต้น อีกทั้งการทบทวนสิทธิ์ต้องพิจารณาถึงพฤติกรรมการทำงานของผู้ใช้งาน รวมทั้งถ้ามีการเปลี่ยนแปลงระบบงานใหม่ จะต้องมีการทบทวนสิทธิ์การใช้งานทุกครั้งอีกด้วย

๑๐.๒ ให้พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบงานสารสนเทศแยกตามหน่วยงานภายในของ รร.การบิน และจัดส่งรายชื่อนั้นให้กับผู้ที่รับผิดชอบระบบสารสนเทศของหน่วยเพื่อดำเนินการทบทวนว่ามีรายชื่อที่มีสิทธิเข้าถึงระบบสารสนเทศถูกต้องหรือไม่ หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

๑๐.๓ ให้ผู้บังคับบัญชาของหน่วย ตรวจสอบและอนุมัติรายชื่อของผู้มีสิทธิในระบบงานสารสนเทศที่ได้รับการทบทวนและแก้ไขจากผู้รับผิดชอบระบบสารสนเทศของหน่วยให้ถูกต้องแล้วแจ้งให้ผู้ดูแลระบบทราบ

๑๐.๔ ผู้ดูแลระบบงานสารสนเทศของหน่วยดำเนินการแก้ไขข้อมูลผู้มีสิทธิ์ให้ถูกต้องตามที่ได้รับแจ้งหรือได้รับการอนุมัติ

๑๐.๕ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน ให้ผู้ดูแลระบบแจ้งรายงานการทบทวนสิทธิ์เป็นลายลักษณ์อักษรให้ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายใน ทอ. อนุมัติให้ดำเนินการต่อไป

๑๑. แนวทางการใช้งานอินเทอร์เน็ต

๑๑.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตเพื่อใช้งานโปรแกรมเข้าชมเว็บไซต์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการปิดช่องโหว่ของระบบปฏิบัติการที่โปรแกรมเข้าชมเว็บไซต์ติดตั้งอยู่ก่อนการใช้งาน

๑๑.๒ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ รร.การบิน เพื่อหาประโยชน์ในเชิงธุรกิจ ส่วนตัว และการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๑๑.๓ ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ รร.การบิน โดยผ่านความเห็นชอบจากผู้บังคับบัญชา

๑๑.๔ ห้ามผู้ใช้...

๑๑.๔ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับทางราชการและที่เกี่ยวข้องกับ รร.การบิน โดยไม่ได้รับอนุญาตอย่างเป็นทางการผ่านเครือข่ายอินเทอร์เน็ต เช่น เอกสารที่กำหนดชั้นความลับร่างหนังสือประกาศหรือคำสั่งต่าง ๆ เอกสารการบรรยายสรุปที่เกี่ยวข้องกับความมั่นคง เอกสารที่เป็นสื่ออิเล็กทรอนิกส์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคง เป็นต้น

๑๑.๕ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๑๑.๖ การใช้งานสื่อสังคมออนไลน์ของหน่วย และสื่อสาธารณะผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลส่วนบุคคล และเป็นความลับของทางราชการ โดยไม่ได้รับอนุญาตรวมทั้งต้องไม่บันทึกข้อมูลที่เป็นการใส่ร้าย ให้ร้ายบุคคลอื่น และการบันทึกข้อมูลที่ผิดกฎหมายต่าง ๆ

๑๑.๗ หลังจากใช้งานอินเทอร์เน็ตเสร็จเรียบร้อยแล้ว ให้ทำการออกจากระบบ (Logout) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๑.๘ ผู้ใช้งานต้องปฏิบัติตาม ระเบียบ ทอ.ว่าด้วย การรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ อย่างเคร่งครัด

๑๑.๙ การขอเปิดใช้บริการเชื่อมต่ออินเตอร์เน็ตความเร็วสูง ผ่านโทรศัพท์เลขหมายเอกชนหน่วยผู้ขอใช้จะต้องเสนอขออนุมัติ ทอ.ผ่านกรมการทหารสื่อสารเพื่อพิจารณาความเหมาะสมและความจำเป็นในการใช้งานต่อไป

๑๑.๑๐ การเชื่อมต่ออินเตอร์เน็ตความเร็วสูงจะต้องไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์ของทางราชการที่เชื่อมต่อกับเครือข่ายภายใน (Intranet) รร.การบิน หรือเครื่องคอมพิวเตอร์ส่วนตัวที่มีข้อมูลข่าวสารของ รร.การบิน ที่เป็นชั้นความลับ และ/หรือ ข้อมูลที่อาจส่งผลกระทบด้านความมั่นคงของประเทศโดยเด็ดขาด และต้องมีหนังสือเป็นลายลักษณ์อักษรขออนุญาตติดตั้งอุปกรณ์หรือเชื่อมต่ออินเตอร์เน็ตความเร็วสูงผ่าน นทสส.รร.การบิน และอนุมัติโดย เสธ.รร.การบิน ก่อนการติดตั้ง

๑๒. แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์

๑๒.๑ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ของ ทอ. หรือ จดหมายอิเล็กทรอนิกส์ (E-mail) ของภาครัฐเพื่อใช้ในการติดต่องานราชการ

๑๒.๒ ผู้ใช้งานต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๑๒.๓ ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยต้องเปลี่ยนรหัสผ่านทุก ๑๘๐ วัน

๑๒.๔ ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อ สำนักงาน รร.การบิน หรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของ รร.การบิน

๑๒.๕ หลังจาก...

๑๒.๕ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องทำการ ออกจากระบบ (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๑๒.๖ ผู้ใช้งานต้องทำการตรวจสอบเอกสารที่แนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบแฟ้มข้อมูลโดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดแฟ้มข้อมูลที่เป็น Executable File เช่น .exe และ .com เป็นต้น

๑๒.๗ ผู้ใช้งานไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๒.๘ ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและต้องจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๑๒.๙ ผู้ใช้งานต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๑๓. แนวทางการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑๓.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายใน รร.การบิน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน

๑๓.๒ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๑๓.๓ ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

๑๓.๔ การระบุอุปกรณ์ที่จะเข้าใช้งานในเครือข่ายไร้สายของ รร.การบิน นอกจากการลงทะเบียนการใช้งานแล้ว จะต้องแจ้งค่า MAC Address ของเครื่อง หรืออุปกรณ์ที่จะเข้ามาใช้งาน เพื่อให้ผู้รับผิดชอบเครือข่ายไร้สายของ ทอ. บันทึกเป็นหลักฐานการเข้าใช้งานต่อไป

๑๔. แนวทางการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ผู้รับผิดชอบระบบสารสนเทศของ รร.การบิน ต้องจัดการควบคุมการเข้า - ออก (Physical Entry Controls) ดังนี้

๑๔.๑ ให้มีการบันทึกวันและเวลาการเข้า - ออกพื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

๑๔.๒ ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๑๔.๓ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๑๔.๔ สร้างความ...

๑๔.๔ สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๔.๕ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๑๔.๖ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๑๔.๗ มีการพิสูจน์ตัวตน เช่น การแสดงบัตรผ่าน การใช้บัตรแถบแม่เหล็ก การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า - ออกในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๔.๘ บุคคลภายนอก เช่น เจ้าหน้าที่บริษัท, นักศึกษาฝึกงานหรือผู้ได้รับการว่าจ้างอื่น ๆ ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๑๔.๙ ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๑๔.๑๐ ต้องจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๔.๑๑ จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๑๕. แนวทางการเข้าถึงหรือการใช้งานระบบสารสนเทศ

ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายใน รร.การบิน ต้องจัดการควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงาน โดยกำหนดเป็นมาตรการทั้ง ๔ ด้าน ดังนี้

๑๕.๑ ด้านการเข้าถึงระบบสารสนเทศทั่วไป

๑๕.๑.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้รับผิดชอบข้อมูล และ/หรือ ผู้รับผิดชอบระบบงาน ตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

๑๕.๑.๒ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ได้แก่ ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นบันทึกและกรอกแบบเอกสารที่ รร.การบิน กำหนดเพื่อขอสิทธิ์ในการเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน

๑๕.๑.๓ ผู้รับผิดชอบข้อมูลและผู้รับผิดชอบระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๑๕.๒ ด้านการเข้าถึงระบบเครือข่ายสารสนเทศ

๑๕.๒.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้รับผิดชอบระบบเครือข่ายของ รร.การบิน ตามสิทธิและความจำเป็นในการเข้าถึงเครือข่ายก่อนที่จะเข้าใช้งาน

๑๕.๒.๒ ผู้ดูแล...

๑๕.๒.๒ ผู้ดูแลเครือข่ายสารสนเทศของ รร.การบิน มีหน้าที่ตรวจสอบการอนุมัติและกำหนดการอนุญาตในการผ่านเข้าสู่เครือข่ายสารสนเทศของ รร.การบิน ตามสิทธิ์และความจำเป็นในการปฏิบัติงานเท่านั้น

๑๕.๒.๓ ผู้ดูแลเครือข่ายสารสนเทศของ รร.การบิน จะต้องจัดให้มีการบันทึกการใช้งานของผู้ใช้งาน ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิ์การใช้งาน ล่วงละเมิดสิทธิ์ของผู้ใช้งานอื่น ๆ อีกด้วย

๑๕.๓ ด้านการควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องปฏิบัติดังนี้

๑๕.๓.๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยสำหรับการเข้าถึงระบบปฏิบัติการซึ่งจะต้องควบคุมด้วยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยใช้วิธีการยืนยันตัวตนด้วยการใส่ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

๑๕.๓.๒ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานโดยกำหนดให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นการระบุตัวตน และต้องเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึงซึ่งในการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) นั้น ชื่อที่ใช้ในการยืนยันตัวตน จะมีรูปแบบซึ่งประกอบไปด้วย ๒ ส่วน คือ ชื่อผู้ใช้งาน และชื่อโดเมน ดังตัวอย่าง user@rtaf.mi.th หรือ rtaf\user

๑๕.๓.๓ ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่าน (Password Management System) ของระบบปฏิบัติการ โดยต้องปรับแต่งค่าการรักษาความปลอดภัยของระบบปฏิบัติการให้สามารถจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ และต้องสอดคล้องกับแนวทางการใช้งานรหัสผ่าน

๑๕.๓.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานหรืออุปกรณ์สารสนเทศร่วมกัน

๑๕.๓.๕ ผู้ใช้งานต้องได้รับอนุญาตจากผู้รับผิดชอบระบบปฏิบัติการ ซึ่งเป็นทรัพย์สินของ รร.การบิน จึงจะสามารถเข้าถึงการใช้งานได้ และผู้ใช้งานต้องใช้งานเฉพาะระบบปฏิบัติการที่ รร.การบินจัดหามาเท่านั้นหากต้องการใช้ระบบปฏิบัติการอื่นใดต้องได้รับอนุญาตจาก นทสส.รร.การบิน ก่อนการติดตั้ง

๑๕.๓.๖ ผู้รับผิดชอบระบบปฏิบัติการ มีหน้าที่ตรวจสอบสิทธิ์อนุญาตให้เข้าใช้งานระบบปฏิบัติการของผู้ใช้งาน และควบคุมการใช้งานให้เป็นไปตามสิทธิ์และตามความจำเป็นในการใช้งานรวมถึงการบันทึกการใช้งานของผู้ใช้งาน ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิ์การใช้งาน รวมถึงล่วงละเมิดสิทธิ์ของผู้ใช้งานอื่น ๆ อีกด้วย

๑๕.๓.๗ ผู้ใช้งาน...

๑๕.๓.๗ ผู้ใช้งานต้องตั้งค่าการใช้โปรแกรมรักษาหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องใช้งานผู้ใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

๑๕.๓.๘ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๑๕.๔ ด้านการเข้าถึงโปรแกรมประยุกต์ (Application)

๑๕.๔.๑ ผู้ใช้งานต้องได้รับอนุญาตจากผู้รับผิดชอบโปรแกรมประยุกต์ ซึ่งเป็นทรัพย์สินของ รร.การบิน จึงจะสามารถเข้าถึงการใช้งานได้ และผู้ใช้งานต้องใช้งานเฉพาะโปรแกรมประยุกต์ที่ รร.การบิน จัดหามาเท่านั้นหากต้องการใช้งานโปรแกรมประยุกต์พิเศษเพิ่มเติม ให้ติดต่อขออนุญาตใช้งานจาก นทสส.รร.การบิน ก่อนการติดตั้ง

๑๕.๔.๒ ผู้รับผิดชอบโปรแกรมประยุกต์ มีหน้าที่ตรวจสอบสิทธิ์อนุญาตให้เข้าใช้งานโปรแกรมประยุกต์ของผู้ใช้งาน และควบคุมการใช้งานให้เป็นไปตามสิทธิ์และตามความจำเป็นในการใช้งาน รวมถึงการบันทึกการใช้งานของผู้ใช้งาน ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิ์การใช้งาน รวมถึงล่วงละเมิดสิทธิ์ของผู้ใช้งานอื่น ๆ อีกด้วย

๑๖. แนวทางการป้องกันชุดคำสั่งไม่พึงประสงค์

๑๖.๑ ห้ามการติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้แฟ้มข้อมูล (File) อื่นที่ รร.การบิน ไม่อนุญาตให้ใช้งาน

๑๖.๒ ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอเพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๑๖.๓ ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันชุดคำสั่งไม่พึงประสงค์ให้กับระบบเทคโนโลยีสารสนเทศของ รร.การบิน

๑๖.๔ ให้ผู้ดูแลระบบดำเนินการตรวจสอบชุดคำสั่งไม่พึงประสงค์ในเครื่องคอมพิวเตอร์ที่ให้บริการและอุปกรณ์เทคโนโลยีสารสนเทศอื่น ๆ ในบริเวณจุดทางเข้า - ออก เครือข่ายอย่างสม่ำเสมอเพื่อดักจับชุดคำสั่งไม่พึงประสงค์ที่จะเข้าสู่ระบบ

๑๖.๕ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับชุดคำสั่งไม่พึงประสงค์ ได้แก่ การรายงานการเกิดขึ้นของชุดคำสั่งไม่พึงประสงค์ การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่ตรวจพบ เป็นต้น

๑๖.๖ มีการติดตามข้อมูลข่าวสารเกี่ยวกับชุดคำสั่งไม่พึงประสงค์อย่างสม่ำเสมอ

๑๖.๗ ให้มีการสร้างความตระหนักเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุชุดคำสั่งไม่พึงประสงค์ว่าต้องดำเนินการอย่างไร รวมทั้งให้หน่วยมีการจัดการฝึกอบรมสร้างความตระหนักอย่างน้อยปีละ ๑ ครั้ง

๑๗. หน้าที่...

๑๗. หน้าที่และความรับผิดชอบ

๑๗.๑ ความรับผิดชอบของผู้บังคับบัญชา กรณีที่มีการละเมิดการปฏิบัติตามมาตรการนี้ โดยเฉพาะในกรณีระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตาม ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ ให้ผู้บังคับบัญชาสูงสุดในพื้นที่และรับผิดชอบระบบสารสนเทศของหน่วย เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น โดยมีแนวทางปฏิบัติ ดังนี้

๑๗.๑.๑ ให้แจ้งรายงานการละเมิดตามสายการบังคับบัญชาให้หน่วยเหนือและหน่วยที่เกี่ยวข้องทราบ

๑๗.๑.๒ สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

๑๗.๑.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

๑๗.๑.๔ ให้พิจารณาสั่งการลงโทษทางวินัยตามแบบธรรมเนียมทหารหรือดำเนินคดีตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิด และผู้รับผิดชอบเมื่อมีการละเมิดหรือไม่ปฏิบัติตามแนวปฏิบัตินี้ จะโดยเจตนาหรือไม่เจตนาและการละเมิดนั้นจะเกิดความเสียหายหรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

๑๗.๒ ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบงานสารสนเทศ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของระบบสารสนเทศดำเนินการ ดังนี้

๑๗.๒.๑ พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่างๆ ประมวลลับ หรือรหัสผ่านที่จำเป็นในการใช้ เครือข่ายสื่อสารข้อมูลสารสนเทศมีผลกระทบกระเทือนหรือเกิดเสียหายอย่างใดหรือไม่

๑๗.๒.๒ ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันทีในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่างๆ ที่เกี่ยวข้องตามที่เห็นควร

๑๗.๓ ความรับผิดชอบของผู้ใช้งานต่อแนวปฏิบัติฉบับนี้ มีดังนี้

๑๗.๓.๑ ปฏิบัติตามมาตรการนี้ อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

๑๗.๓.๒ ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบคอมพิวเตอร์และเครือข่ายของ รร.การบิน

๑๗.๓.๓ ไม่รบกวนหรือแทรกแซงการสื่อสารข้อมูลในเครือข่ายคอมพิวเตอร์ของ รร.การบิน

๑๗.๓.๔ รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังผู้บังคับบัญชาและผู้รับผิดชอบระบบงานสารสนเทศโดยเร็วที่สุด

๑๗.๔ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบกระเทือนเสียหายอย่างร้ายแรงให้อยู่ในดุลพินิจของของผู้บังคับบัญชาสามารถแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติหากจำเป็นให้รายงานหน่วยเหนือได้ตามความเหมาะสม

นาวาอากาศเอก

(ขวัญชาติ ชวนสนิท)

เสนาธิการ รร.การบิน/ผู้บริหารเทคโนโลยีสารสนเทศ (CIO)

ประธานคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน

ธ.ค.๖๖