องค์การคลังสินค้า กระทรวงพาณิชย์
563 ถนนนนทบุรี ตำบลบางกระสอ อำเภอเมืองนนทบุรี จังหวัดนนทบุรี 11000
โทร. 0-2507-5267 แฟกซ์ 0-2507-5268

ประกาศองค์การคลังสินค้า
เรื่อง นโยบายและแนวปฏิบัติในการธรรมาภิบาลข้อมูลภาครัฐ การคุ้มครองข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการใช้บริการคลาวด์

.....

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒ มาตรา ๘ (๔) การกำหนดนโยบายหรือกฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูลที่ชัดเจนและมีระบบบริหารจัดการ รวมทั้งมีมาตรการและหลักประกันในการคุ้มครองข้อมูลที่อยู่ในความครอบครองให้มีความมั่นคงปลอดภัยและมิให้ข้อมูลส่วนบุคคลถูกละเมิด ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ และตามพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ และ พ.ศ.๒๕๖๓ กำหนดให้ผู้ควบคุมข้อมูลซึ่งเป็นหน่วยงาน หรือกิจการตามบัญชีท้ายพระราชกฤษฎีกาดังกล่าวต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ มาตรา ๔๔ “ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางการปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษา ความมั่นคงปลอดภัยไซเบอร์โดยเร็ว” และตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๖๒โดยประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการใช้บริการคลาวด์ พ.ศ. ๒๕๖๒ นั้น

เพื่อให้ระบบเทคโนโลยีดิจิทัลขององค์การคลังสินค้า หรือต่อไปเรียกว่า “อคส.” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง ทันยุค ทันสมัย กับกฎหมายในปัจจุบัน รวมทั้งให้สามารถป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศ ระบบเทคโนโลยีดิจิทัล ในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ อคส. จึงเห็นสมควรปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นนโยบายและแนวปฏิบัติในการธรรมาภิบาลข้อมูลภาครัฐ การคุ้มครองข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการใช้บริการคลาวด์ ให้สอดคล้องกับกฎหมายและประกาศที่เกี่ยวข้อง อย่างเป็นมาตรฐานสากลต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ระบบเทคโนโลยีดิจิทัลขององค์กร

๒.๒ เพื่อใช้เป็นแนวทางในการจัดทำแนวปฏิบัติของผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคล ภายนอกที่ปฏิบัติงานให้กับองค์กร โดยให้เป็นไปตามกฎหมายและประกาศที่เกี่ยวข้อง อย่างเป็นมาตรฐานสากล

๒.๓ เพื่อให้ผู้ใช้งานเกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ ระบบเทคโนโลยีดิจิทัล ขององค์กร

๒.๔ เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรมีประสิทธิภาพ

๒.๕ เพื่อให้การบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน

๒.๖ เพื่อเพิ่มประสิทธิภาพและให้มีการใช้ระบบดิจิทัลอย่างคุ้มค่าและเต็มศักยภาพ

๒.๗ เพื่อการพัฒนามาตรฐาน หลักเกณฑ์ และวิธีการเกี่ยวกับระบบดิจิทัล และพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่จำเป็น ให้เป็นไปตามมาตรฐานสากล

๒.๘ เพื่อสร้างและพัฒนากระบวนการทำงานของหน่วยงานของรัฐให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้งมีความมั่นคงปลอดภัยและน่าเชื่อถือ

๒.๙ เพื่อความสะดวกในการให้บริการแก่ผู้ใช้บริการที่เข้าใช้บริการผ่านเว็บไซต์ของ อคส. เช่น ระบบติดตามการจ่ายเงิน เป็นต้น

๒.๑๐ เพื่อใช้ในการบริหารทางอิเล็กทรอนิกส์ แก่ผู้ใช้บริการตามพันธกิจของ อคส.

๒.๑๑ เพื่อใช้ตรวจสอบย้อนหลังในการวิเคราะห์ปัญหาและการปรับปรุงการให้บริการของ อคส.

๒.๑๒ เพื่อให้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้บริการคลาวด์ มีความมั่นคงปลอดภัย เชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล

๓. องค์ประกอบของนโยบาย

๓.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ขององค์การคลังสินค้า

(๓) กำหนดผู้รับผิดชอบตามแนวนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๓.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การธรรมาภิบาลข้อมูลภาครัฐ

๑.๑ มีการกำหนดสิทธิ หน้าที่ และความรับผิดชอบในการบริหารจัดการข้อมูลของหน่วยงานของรัฐ รวมถึงสิทธิและหน้าที่ของผู้ครอบครองหรือควบคุมข้อมูลดังกล่าวในทุกขั้นตอน

๑.๒ มีระบบบริหารและกระบวนการจัดการและคุ้มครองข้อมูลที่ครบถ้วนตั้งแต่การจัดทำ การจัดเก็บ การจำแนกหมวดหมู่ การประมวลผลหรือใช้ข้อมูล การปกปิดหรือเปิดเผยข้อมูล การตรวจสอบ และการทำลาย

๑.๓ มีมาตรการในการควบคุมและพัฒนาคุณภาพข้อมูล เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน พร้อมใช้งาน เป็นปัจจุบัน สามารถบูรณาการและมีคุณสมบัติแลกเปลี่ยนกันได้ รวมทั้งมีการวัดผลการบริหารจัดการข้อมูลเพื่อให้หน่วยงานของรัฐที่มีข้อมูลที่มีคุณภาพและต่อยอดนวัตกรรมจากการใช้ข้อมูลได้

๑.๔ มีการกำหนดนโยบายหรือกฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูลที่ชัดเจนและมีระบบบริหารจัดการ รวมทั้งมีมาตรการและหลักประกันในการคุ้มครองข้อมูลที่อยู่ในความครอบครองให้มีความมั่นคงปลอดภัยและมิให้ข้อมูลส่วนบุคคลถูกละเมิด

๑.๕ มีการจัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ เพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิในการเข้าถึงข้อมูล

(๒) การเก็บรวบรวมข้อมูลส่วนบุคคล

๒.๑ มีการเก็บรวบรวมข้อมูลส่วนบุคคล โดยให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

๒.๒ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

๒.๒.๑ แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

๒.๒.๒ ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

๒.๒.๓ ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

๒.๒.๔ ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

๒.๓ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

๒.๓.๑ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

๒.๓.๒ เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๒.๓.๓ เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

๒.๓.๔ เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๒.๓.๕ เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

๒.๓.๖ เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

๒.๔ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่มิใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่ ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

๒.๕ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

๒.๕.๑ เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ไม่ว่าด้วยเหตุใดก็ตาม

๒.๕.๒ เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมขององค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกองค์กรที่ไม่แสวงหากำไรนั้น

๒.๕.๓ เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

๒.๕.๔ เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

๒.๖ ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม ต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

(๓) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งาน และประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็วรวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย ดังนี้

๓.๑ การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

อคส.ไม่มีการให้บุคคลอื่นเข้าถึงหรือใช้ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมมา เว้นแต่

๓.๑.๑ ได้รับความยินยอมจากท่าน

๓.๑.๒ การให้ข้อมูลดังกล่าวเป็นไปเพื่อช่วยให้ท่านสามารถทำธุรกรรมที่ท่านประสงค์

๓.๑.๓ การเปิดเผยข้อมูลนั้นๆ เป็นไปโดยถูกต้องตามกฎหมาย หรือตามคำสั่งของหน่วยงานของรัฐที่เกี่ยวข้องร้องขอ

๓.๒ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบ สารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัย

สารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๓.๓ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบ ทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผล

๓.๔ มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๓.๕ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึง ระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๓.๖ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น และสารสนเทศ (application and information access control) โดยต้องมีการควบคุมการจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๓.๗ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๓.๘ มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๓.๙ มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

๓.๑๐ มีการบริหารจัดการการเข้าถึงผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

๓.๑๑ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

๓.๑๒ มีการจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๔) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศ และระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งานรวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง และมีแผนการรับมือภัยคุกคามทางไซเบอร์ ตามแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด นำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

(๕) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

มีนโยบายในการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๖) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

มีนโยบายในการสร้างความรู้ความเข้าใจโดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

(๗) แนวทางการใช้บริการคลาวด์

ในปัจจุบันการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ในส่วนของภาครัฐ มีการใช้บริการคลาวด์ (Cloud Computing) อย่างแพร่หลาย โดยการใช้บริการคลาวด์ (Cloud Computing) เป็นเทคโนโลยีพื้นฐานในการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ เพื่อส่งเสริมและพัฒนาการให้บริการแบบคลาวด์ที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย ความน่าเชื่อถือ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล โดยต้องตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ รวมทั้งปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสม

๔. ข้อปฏิบัตินโยบายและแนวปฏิบัติในการธรรมาภิบาลข้อมูลภาครัฐ การคุ้มครองข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการใช้บริการคลาวด์

ข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นไปตามที่กำหนดในเอกสารแนบท้ายประกาศองค์การคลังสินค้า เรื่อง "นโยบายและแนวปฏิบัติในการธรรมาภิบาลข้อมูลภาครัฐ การคุ้มครองข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการใช้บริการคลาวด์ องค์การคลังสินค้า"

๕. อำนาจหน้าที่

ต้องกำหนดความรับผิดชอบที่ชัดเจนกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัตินี้ โดยให้สำนักที่รับผิดชอบด้านเทคโนโลยีดิจิทัล องค์การคลังสินค้าเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันเมื่อนโยบายและแนวปฏิบัติมีการเปลี่ยนแปลงให้ประกาศใหม่ โดยให้เจ้าหน้าที่องค์การคลังสินค้าและหน่วยงานภายนอกทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

ประกาศฉบับนี้มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๕

(นายเกรียงศักดิ์ ประทีปวิศรุต)
ผู้อำนวยการองค์การคลังสินค้า

เอกสารแนบท้ายประกาศองค์การคลังสินค้า

เรื่อง นโยบายและแนวปฏิบัติในการธรรมาภิบาลข้อมูลภาครัฐ การคุ้มครองข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการใช้บริการคลาวด์ องค์การคลังสินค้า

ส่วนที่ ๑

บทที่ ๑ นโยบายและแนวปฏิบัติในการธรรมาภิบาลข้อมูลภาครัฐ การคุ้มครองข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการใช้บริการคลาวด์

๑.๑ นโยบายการธรรมาภิบาลข้อมูลภาครัฐ

๑.๑.๑ มีการกำหนดสิทธิ หน้าที่ และความรับผิดชอบในการบริหารจัดการข้อมูลของหน่วยงานของรัฐ รวมถึงสิทธิและหน้าที่ของผู้ครอบครองหรือควบคุมข้อมูลดังกล่าวในทุกขั้นตอน

๑.๑.๒ มีระบบบริหารและกระบวนการจัดการและคุ้มครองข้อมูลที่ครบถ้วนตั้งแต่การจัดทำ การจัดเก็บ การจำแนกหมวดหมู่ การประมวลผลหรือใช้ข้อมูล การปกปิดหรือเปิดเผยข้อมูล การตรวจสอบ และการทำลาย

๑.๑.๓ มีมาตรการในการควบคุมและพัฒนาคุณภาพข้อมูล เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน พร้อมใช้งานเป็นปัจจุบัน สามารถบูรณาการและมีคุณสมบัติแลกเปลี่ยนกันได้ รวมทั้งมีการวัดผลการบริหารจัดการข้อมูลเพื่อให้หน่วยงานของรัฐที่มีข้อมูลที่มีคุณภาพและต่อยอดนวัตกรรมจากการใช้ข้อมูลได้

๑.๑.๔ มีการกำหนดนโยบายหรือกฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูลที่ชัดเจนและมีระบบบริหารจัดการ รวมทั้งมีมาตรการและหลักประกันในการคุ้มครองข้อมูลที่อยู่ในความครอบครองให้มีความมั่นคงปลอดภัยและมิให้ข้อมูลส่วนบุคคลถูกละเมิด

๑.๑.๕ มีการจัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ เพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิในการเข้าถึงข้อมูล

๑.๒ นโยบายการเก็บรวบรวมข้อมูลส่วนบุคคล

๑.๒.๑ มีการเก็บรวบรวมข้อมูลส่วนบุคคล โดยให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

๑.๒.๒ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

๑.๒.๓ แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

๑.๒.๔ ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถ

กำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

๑.๒.๕ ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

๑.๒.๖ ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

๑.๒.๗ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(๔) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๕) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(๖) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

๑.๒.๘ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่มิใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่ ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

๑.๒.๙ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ไม่ว่าด้วยเหตุใดก็ตาม

(๒) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมขององค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกองค์กรที่ไม่แสวงหากำไรนั้น

(๓) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

(๔) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

๑.๒.๑๐ ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

๑.๓ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

๑.๓.๑ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการถอดถอนสิทธิ์ผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๒) การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning) การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึงทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ ต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท ทุกระบบในองค์กร

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

๑.๓.๒ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่านการใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๑.๓.๓ มีการควบคุมการเข้าถึงเครือข่าย (Network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะ เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๒) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๔) การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์ บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๕) ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสม เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๖) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๗) การแบ่งแยกเครือข่าย (Segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๘) การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๙) การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

(๑๐) ระบบเครือข่ายต้องได้รับการออกแบบหรือตั้งค่าให้ทำงานได้อย่างมีประสิทธิภาพ (Reliable) มีความยืดหยุ่น (Flexible) รวมถึงสามารถรองรับการขยายตัวและความต้องการใช้งานในอนาคต (Scalable)

๑.๓.๔ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึง ระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities) ควรจำกัดและควบคุม

การใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๑.๓.๕ มีการควบคุมการเข้าถึงระบบสารสนเทศ โปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (System and Application Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) การกำหนดขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure) โดยกำหนดให้ระบบปฏิเสธการให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกินจำนวนครั้งที่กำหนด

(๓) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and teleworking)

(๔) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และ สื่อสารเคลื่อนที่

(๕) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

(๖) การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

(๗) การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code) ต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ให้บริการ

๑.๓.๖ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access control) อย่างน้อยดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจขององค์กร

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล สำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๑.๓.๗ การใช้หรือเปิดเผยข้อมูลส่วนบุคคล
อคส.ไม่มีการให้บุคคลอื่นเข้าถึงหรือใช้ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมมา เว้นแต่ได้รับความยินยอมจากท่าน และการให้ข้อมูลดังกล่าวเป็นไปเพื่อช่วยให้ท่านสามารถทำธุรกรรมที่ท่านประสงค์ การเปิดเผยข้อมูลนั้นๆ เป็นไปโดยถูกต้องตามกฎหมาย หรือตามคำสั่งของหน่วยงานของรัฐที่เกี่ยวข้องร้องขอ

๑.๓.๘ มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๑.๓.๙ มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

๑.๓.๑๐ มีการบริหารจัดการการเข้าถึงผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

๑.๓.๑๑ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

๑.๓.๑๒ มีการจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๑.๔ นโยบายการจัดทำระบบสำรองของสารสนเทศ

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองระบบแผนเตรียมพร้อมกรณีฉุกเฉิน และทดสอบข้อมูลสำรองที่บันทึกไว้ อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

(๖) มีแผนการรับมือภัยคุกคามทางไซเบอร์ ทั้งนี้ เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

๑.๕ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๑) องค์การคลังสินค้าต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับ

ระบบสารสนเทศ (Information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในขององค์การคลังสินค้า (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) เพื่อให้องค์การคลังสินค้าได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๑.๖ นโยบายการสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

(๑) องค์การคลังสินค้าต้องจัดให้มีการสร้างความรู้และความเข้าใจ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม โดยเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแจ้งให้เจ้าหน้าที่ทราบและถือปฏิบัติ

(๒) จัดอบรมให้ความรู้ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับ แนวปฏิบัติขององค์การคลังสินค้า

๑.๗ นโยบายการใช้บริการคลาวด์

มีนโยบายและแนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยสารสนเทศ การพัฒนาทรัพยากรบุคลากรให้มีความรู้ความเข้าใจในเรื่องความมั่นคงปลอดภัยของข้อมูล นโยบายการจัดการสินทรัพย์ นโยบายการจัดการเปลี่ยนแปลง นโยบายการบริหารความเสี่ยง กระบวนการตอบสนองต่อเหตุการณ์ฉุกเฉิน การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน การติดตามดูแลการให้บริการ กระบวนการจ้างช่วงต่อสัญญา และการปฏิบัติอื่นใดตามที่กฎหมายกำหนด

ประกอบด้วย

"ผู้บริหารระดับสูงสุด" (CEO) หมายถึง ผู้อำนวยการองค์การคลังสินค้า

"ผู้บังคับบัญชา" หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ อคส.

"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง" (DCIO) หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีดิจิทัลของ อคส.

"สำนักเทคโนโลยีดิจิทัล" หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีดิจิทัล ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบงาน ระบบคอมพิวเตอร์และเครือข่ายภายใน อคส.

"การรักษาความมั่นคงปลอดภัย" หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของ อคส.

"แนวทางปฏิบัติ (Guideline)" หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

"ผู้ใช้งาน" หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role)

"ผู้บริหาร" หมายถึง ผู้มีอำนาจบริหารในระดับสูงของ อคส. เช่น ผู้อำนวยการสำนัก/ส่วนงาน เป็นต้น

"ผู้ดูแลระบบ (System Administrator)" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบงาน ระบบฐานข้อมูล ระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์(User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

"เจ้าหน้าที่" หมายถึง พนักงาน ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างโครงการต่างๆ พนักงานจ้างเหมา ของ อคส.

"หน่วยงานภายนอก" หมายถึง องค์กรหรือหน่วยงานภายนอกที่ อคส. อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของ อคส. โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูลของ อคส.

"ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้ โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือ วิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"สารสนเทศ (Information)" หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบ ให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้ สามารถเข้าใจได้ง่าย และ สามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย(Network System)" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่างๆ ขององค์กรได้

"แลน (LAN) และอินทราเน็ต (Intranet)" หมายถึง ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

"อินเทอร์เน็ต (Internet)" หมายถึง ระบบเครือข่ายที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงาน เข้ากับเครือข่ายคอมพิวเตอร์ทั่วโลก

"ระบบสารสนเทศ (Information System)" หมายถึง ระบบงานของหน่วยงานที่นำเอาระบบคอมพิวเตอร์ และ

ระบบการสื่อสารมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการดำเนินการต่างๆ ของ หน่วยงาน

"เจ้าของข้อมูล" หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบสารสนเทศโดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

"สิทธิของผู้ใช้งาน" หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ ของหน่วยงาน ตามที่กำหนดในภารกิจของผู้ใช้งาน (User Role)

"สินทรัพย์" หมายถึง ข้อมูล และทรัพย์สินด้านเทคโนโลยีดิจิทัลของหน่วยงาน

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน หรือบุคคลภายนอก เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง ครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)" หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของการบริการหรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่านโยบายด้านความ มั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคง ปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)" หมายถึง สถานการณ์ ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูก คุกคาม

"จดหมายอิเล็กทรอนิกส์ (Email)" หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่ง ข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP

"ระบบจดหมายอิเล็กทรอนิกส์ของ อคส." หมายถึง ระบบจดหมายอิเล็กทรอนิกส์ของ สำนักงานปลัด กระทรวงพาณิชย์หรือ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ซึ่งอนุญาตให้ผู้ใช้งานใช้เพื่อการดำเนินงานของ อคส.

"รหัสผ่าน (Password)" หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงและรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

"ซอฟต์แวร์ประสงค์ร้าย (Malware)" หมายถึง ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อทำลาย หรือสร้างความเสียหายให้กับระบบสารสนเทศ การโจรกรรมข้อมูล หรือการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

"ผู้บุกรุก" หมายถึง บุคคลที่เข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)" หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

"ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)" หมายถึง สำนักที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่สำนักรับผิดชอบตามภารกิจ ทั้งนี้ สำนักซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

"เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protecting officer)" หมายถึง บุคคลซึ่งได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในการให้คำแนะนำและตรวจสอบการดำเนินงานตามที่ได้รับมอบหมายให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยอาจเป็นพนักงานหรือผู้รับจ้างให้บริการตามสัญญากับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

"บริการคลาวด์ (Cloud Computing)" หมายถึง บริการประมวลผลด้วยการใช้ทรัพยากรคอมพิวเตอร์ร่วมกันผ่านเครือข่ายตามความต้องการได้อย่างสะดวก โดยมีรูปแบบ ดังนี้

๑. การให้บริการโครงสร้างพื้นฐานหลัก (Infrastructure as a Service: Iaas) ประกอบด้วยระบบประมวลผลข้อมูล ระบบการจัดเก็บข้อมูล ระบบเครือข่าย และทรัพยากรพื้นฐานอื่นๆ ที่เกี่ยวข้องกับระบบประมวลผล ผู้ใช้บริการสามารถใช้งานซอฟต์แวร์บนโครงสร้างพื้นฐานและทรัพยากรที่ผู้ให้บริการจัดหาให้ได้อย่างมีประสิทธิภาพ โดยไม่ต้องบริหารจัดการโครงสร้างพื้นฐานที่จำเป็นด้วยตนเอง หรือ

๒. การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) ประกอบด้วย ระบบโปรแกรมงานคอมพิวเตอร์ ระบบฐานข้อมูล และระบบจัดการหรืองานบริการจากคอมพิวเตอร์ ผู้ใช้บริการสามารถพัฒนา ติดตั้ง และปรับแต่งซอฟต์แวร์ได้ โดยไม่ต้องบริหารจัดการส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐานเครือข่าย ระบบปฏิบัติการ และระบบจัดการฐานข้อมูล หรือ

๓. การให้บริการซอฟต์แวร์ (Software as a Service: SaaS) ผู้ให้บริการจัดเตรียมซอฟต์แวร์สำเร็จรูปแล้วโดยผู้ใช้บริการสามารถกำหนดค่าความต้องการ พารามิเตอร์ ปริมาณหน่วยประมวลผลข้อมูล หน่วยเก็บข้อมูล และบริหารจัดการเพื่อให้ได้บริการตามวัตถุประสงค์ หรือ

๔. การให้บริการใดที่เป็นการรวมกันของสองบริการขึ้นไป จากข้อ ๑ ถึง ๓ หรือ

๕. การให้บริการอื่นที่ประกาศกำหนด

"ผู้ให้บริการ" หมายถึง ผู้ให้บริการคลาวด์

"ผู้ใช้บริการ" หมายถึง องค์การคลังสินค้า

ส่วนที่ ๒

แนวปฏิบัติการเก็บรวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคล การเข้าถึงหรือควบคุม การใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการบุกรุกผ่านระบบ เครือข่าย จากผู้บุกรุก หรือจากซอฟต์แวร์ประสงค์ร้าย รวมทั้งกำหนดประเภทของข้อมูล ลำดับชั้น ความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ผู้รับผิดชอบ

สำนักที่ดูแลรับผิดชอบด้านเทคโนโลยีดิจิทัล และสำนักที่มีหน้าที่ดูแลและรับผิดชอบการเก็บรวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคล การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒. ๕)

แนวปฏิบัติ

๒.๑ การเก็บรวบรวมข้อมูลส่วนบุคคล

๒.๑.๑ มีการเก็บรวบรวมข้อมูลส่วนบุคคล โดยให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

๒.๑.๒ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

๒.๑.๒.๑ แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญารวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

๒.๑.๒.๒ ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

๒.๑.๒.๓ ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

๒.๑.๒.๔ ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ ในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูลสถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

๒.๑.๓ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล **เว้นแต่**

๒.๑.๓.๑ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

๒.๑.๓.๒ เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๒.๑.๓.๓ เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคล เป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

๒.๑.๓.๔ เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

๒.๑.๓.๕ เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุม ข้อมูลส่วนบุคคล หรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

๒.๑.๓.๖ เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

๒.๑.๔ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่มิใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่ ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคล ทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

๒.๑.๕ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล ในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

๒.๑.๕.๑ เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

๒.๑.๕.๒ เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมขององค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับ การเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิกผู้ซึ่งเคยเป็นสมาชิก หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกองค์กร ที่ไม่แสวงหากำไรนั้น

๒.๑.๖ เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

๒.๑.๗ เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

๒.๑.๘ ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม ต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

๒.๒ การใช้ การเปิดเผยข้อมูลส่วนบุคคล

อคส. ไม่อนุญาตให้บุคคลอื่นเข้าถึงหรือใช้ข้อมูลที่ อคส.มีการจัดเก็บรวบรวมข้อมูลเกี่ยวกับผู้ใช้บริการ เว้นแต่ กรณีที่มีการบังคับให้เปิดเผยข้อมูลส่วนบุคคลตามกฎหมายกำหนด เพื่อประโยชน์แก่การสอบสวนของพนักงานสอบสวน หรือการพิจารณาพิพากษาคดีของศาล ตามหมายศาล

หรือคำสั่งศาล ซึ่ง อคส. มีหน้าที่ที่จะต้องปฏิบัติตาม อคส. มีการจัดเก็บรวบรวมและการใช้ข้อมูลเกี่ยวกับผู้ใช้บริการเท่าที่จำเป็นแก่การให้บริการ ตามวัตถุประสงค์ในการดำเนินงานของ อคส. เท่านั้น และจะไม่นำข้อมูลไปใช้เพื่อวัตถุประสงค์อื่น รวมทั้งไม่อนุญาตให้มีการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

๒.๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๓.๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติในการลงทะเบียนเจ้าหน้าที่ใหม่ การให้สิทธิต่างๆ ในการใช้งานตามความจำเป็น และการยกเลิกสิทธิการใช้งาน เช่น การลาออก การโยกย้ายหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึง และใช้งานระบบสารสนเทศที่สำคัญ เช่น ซอฟต์แวร์ประยุกต์ จดหมายอิเล็กทรอนิกส์ เครือข่ายไร้สาย และอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจาก ผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๓.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงและใช้งานระบบสารสนเทศของบุคลากรดังต่อไปนี้

๒.๓.๓.๑ การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration) ให้ผู้ดูแลระบบงานหรือผู้ที่ ได้รับมอบหมายจัดทำแบบฟอร์มสำหรับลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(๓) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัว แรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะ ไ ม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและอนุญาตให้ใช้เท่าที่จำเป็น

(๕) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ/หรือ ความต้องการทางธุรกิจ

(๖) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนามรับทราบด้วย

(๗) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๘) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจาก ผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๙) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออก จากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอนย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๑๐) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๓.๓.๒ การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning) การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึงทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ ต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท เช่น ผู้ใช้งาน ผู้ดูแลระบบ รวมถึงทุกระบบในองค์กร

๒.๓.๓.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียด ที่เกี่ยวกับการ ควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึง สิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) ผู้ใช้งานต้องลงทะเบียนผู้ใช้งานเพื่อนำข้อมูลไปตรวจสอบสิทธิก่อนการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒) ต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน

(๓) การมอบหมายสิทธิต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๔) ต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๒.๓.๓.๔ บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

(๑) มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการสุ่ม และต้องมีความแตกต่างกัน

(๓) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมาย อิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับ ทันที หลังจากได้รับรหัสผ่าน โดยจัดส่งบัญชีและรหัสผ่านใส่ซองปิดผนึก และประทับตรา "ลับ" และแนบเอกสารอื่นๆ ที่เกี่ยวข้องกับการ ปฏิบัติงานของผู้ใช้งาน ส่งมอบให้ผู้ใช้งาน และให้ผู้ใช้งานลงนามรับ เอกสารนั้น รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามเอกสารแนบดังกล่าวโดย เคร่งครัด

(๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๕) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๖) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๗) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๘) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งาน นั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการสำนัก เทคโนโลยีสารสนเทศ โดยมีการกำหนดระยะเวลาการใช้งานและระงับ การใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการ กำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง

(๙) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านเมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๑๐) หลีกเลี่ยงการส่งรหัสผ่านให้ผู้ใช้งาน โดยใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการรักษาความปลอดภัย

(๑๑) ต้องกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๓.๓.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

(๑) ต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งาน (Review of User Access Rights) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๒.๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

๒.๔.๑ กำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password use) สำหรับผู้ใช้งาน เพื่อให้สามารถ กำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

๒.๔.๑.๑ เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

๒.๔.๑.๒ ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา

๒.๔.๑.๓ ผู้ใช้งานต้องกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๒.๔.๑.๔ ต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๒.๔.๑.๕ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๒.๔.๑.๖ เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

๒.๔.๑.๗ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในระบบคอมพิวเตอร์

๒.๔.๑.๘ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๒.๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

๒.๔.๒.๑ ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๒.๔.๒.๒ ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๔๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๒.๔.๒.๓ มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๔.๒.๔ มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

๒.๔.๒.๕ สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

๒.๔.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึก ข้อมูล

คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

๒.๔.๓.๑ กำหนดวิธีป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่างๆ

- ใกล้สิ้นปีงบประมาณต้องสำรวจทะเบียนครุภัณฑ์เครื่องคอมพิวเตอร์และอุปกรณ์ว่ายังสามารถใช้งานได้หรือไม่ จำนวนครบหรือไม่ ถ้าเกิดกรณีชำรุด/เสียหาย จะทำ เรื่องส่งซ่อม/ส่งคืนพัสดุ
- จัดห้องสำหรับรวบรวมเครื่องคอมพิวเตอร์และอุปกรณ์ที่จะส่งซ่อม/ส่งคืน และปิดล็อคห้องทุกครั้งหลังเข้า-ออก เพื่อป้องกันมิให้เครื่องคอมพิวเตอร์และอุปกรณ์สูญหาย
- การควบคุมการเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ โดยการใช้การ์ดหรือสแกนนิ้วมือ ก่อนและหลังเข้า-ออกทุกครั้ง
- การจัดทำทะเบียนยืม-คืน อุปกรณ์คอมพิวเตอร์ โดยแบบฟอร์มขอใช้อุปกรณ์คอมพิวเตอร์ เพื่อใช้งานภายในและภายนอกองค์กร สำหรับควบคุมและป้องกันการสูญหาย
- การจัดทำทะเบียนยืม-คืน โน้ตบุ๊ค โดยใช้แบบฟอร์มยืมโน้ตบุ๊ค เพื่อใช้งานภายใน และภายนอกองค์กร สำหรับควบคุมและป้องกันการสูญหาย
- การวางอุปกรณ์ มีการจัดที่เฉพาะและเหมาะสมสำหรับวางเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ (Data Center)
- การจัดทำระบบเอกสารคุณภาพ (ISO ๙๐๐๑ : ๒๐๐๘) ใช้ในองค์กร

๒.๔.๓.๒ การนำเครื่องคอมพิวเตอร์ โน้ตบุ๊ค และอุปกรณ์ เข้า-ออก องค์การคลังสินค้าต้องได้รับการตรวจเช็คจากเจ้าหน้าที่ฝ่ายอาคาร อย่างเคร่งครัด

๒.๔.๓.๓ ต้องป้องกันการเข้าใช้งานเครื่องคอมพิวเตอร์ โดยใช้รหัสผู้ใช้งาน (Username) รหัสผ่าน (Password) เป็นการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน และมีการตั้งค่าพักหน้าจออัตโนมัติ เมื่อไม่ได้ใช้งาน

๒.๔.๓.๔ การป้องกันการใช้ทรัพย์สินอย่างมีประสิทธิภาพและปลอดภัย ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- Log out ออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๒.๔.๓.๕ การทำลายข้อมูลอิเล็กทรอนิกส์และสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ ดังนี้

(๑) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร

แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลาย CD/DVD
เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบน ฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD ๕๒๒๐.๓๓-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

(๒) ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้

(๑) จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับและป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึงและควรแสดงชั้นความลับบนไฟล์ข้อมูลลับ เช่น การแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

(๒) การสำเนาข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล

(๓) ระมัดระวังการกระจาย หรือแจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับขององค์การคลังสินค้าไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

(๔) ผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ต้องตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน

(๕) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย

(๖) ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายขององค์การคลังสินค้า เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

(๗) ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

(๘) ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

(๙) ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

(๑๐) ต้องทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

(๑๑) ต้องมีการพิจารณาเพื่อทำลายข้อมูลส่วนบุคคล ซึ่งรอบความถี่ในการทำลายข้อมูลส่วนบุคคลอย่างน้อยปีละ ๑ โดยเจ้าหน้าที่ที่รับผิดชอบข้อมูลจะต้องมีการตรวจสอบและพิจารณาการทำลายข้อมูลส่วนบุคคล

๒.๔.๔ ผู้ใช้งานได้ใช้งานระบบงานสารบรรณอิเล็กทรอนิกส์ที่นำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

๒.๒.๔.๑ องค์การคลังสินค้ามีระบบงานสารบรรณอิเล็กทรอนิกส์สำหรับควบคุมการจัดเก็บและนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ดังนี้

(๑) ลงทะเบียนผู้ใช้งานระบบสารบรรณอิเล็กทรอนิกส์ มีการกำหนดสิทธิ์การเข้าตาม

หน่วยงาน หรือตามผู้ใช้งาน

(๒) เข้าสู่ระบบงานสารบรรณอิเล็กทรอนิกส์ โดยระบบจะทำการตรวจสอบสิทธิ์ของผู้ใช้งานก่อนเข้าสู่ระบบ

(๓) กรณีผู้ใช้งานได้รับเอกสารลับ /ลับมาก /ลับที่สุด ให้นายทะเบียนลับ ลงรับเอกสาร โดยบันทึกข้อมูลและกำหนดชั้นความลับของเอกสารตามที่ปรากฏบนหน้าซอง พร้อมทั้งนำเลขทะเบียนรับที่ระบบออกให้ เขียนบนหน้าซอง ก่อนนำเสนอผู้มีอำนาจพิจารณาดำเนินการต่อไป

(๔) เมื่อผู้ใช้งาน เช่น เลขานุการผู้บริหาร เจ้าหน้าที่สารบรรณ เป็นต้น กำหนดชั้นความลับของเอกสารแล้ว จะไม่สามารถดำเนินการใดๆ กับเรื่องดังกล่าวในระบบได้อีก ยกเว้นเป็นผู้ที่ได้รับสิทธิ์ ให้เข้าถึงเอกสารประเภท ลับ ลับมาก ลับที่สุด ได้เท่านั้น

(๕) ต้องนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับของหน่วยงาน

๒.๔.๕ ผู้ดูแลระบบต้องมีวิธีการรับส่ง ประมวลผล และจัดเก็บข้อมูลส่วนบุคคลที่เป็นความลับตามระดับความสำคัญ

๒.๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๒.๕.๑ ตรวจสอบการใช้งานเครือข่าย ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพหากตรวจ พบสิ่งผิดปกติเกี่ยวกับการใช้งานเครือข่ายให้รีบดำเนินการแก้ไขรวมทั้งป้องกันและ บรรเทาความเสียหาย ที่อาจจะเกิดขึ้นในทันทีในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการ ใช้งานของผู้ใช้งาน และให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันทีและใน กรณีที่จำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบเครือข่ายพิจารณาระงับใช้งานเครือข่ายคอมพิวเตอร์ของผู้ใช้งานดังกล่าวได้ทันที

๒.๕.๒ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขต ของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้ เป็นปัจจุบันอยู่เสมอ

๒.๕.๓ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๕.๔ ห้ามผู้ใดกระทำการเคลื่อนย้ายติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๒.๕.๕ ระบบยืนยันตัวบุคคลต้องสามารถกำหนดสิทธิการใช้งานระบบสารสนเทศต่างๆ ผ่านเครือข่ายตามบทบาทหน้าที่ของผู้ใช้ (User role) แต่ละคนได้

๒.๕.๖ การยืนยันตัวบุคคล สำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User authentication for external connections) ให้มีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง โดยการใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

๒.๕.๗ การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks) เพื่อใช้สำหรับการยืนยันการเข้าถึง ดังนี้

๒.๕.๗.๑ กรณีอุปกรณ์บนเครือข่ายทุกตัวที่มีหมายเลข IP แบบคงที่ (Static IP address) ให้จัดทำฐานข้อมูลเพื่อจัดเก็บหมายเลข MAC ของอุปกรณ์ดังกล่าว

๒.๕.๗.๒ กรณีอุปกรณ์บนเครือข่ายทุกตัวที่มีหมายเลข IP แบบไดนามิค (Dynamic IP

address) ให้จัดเก็บ Log ใน DHCP server โดยมีข้อมูลซึ่งอ้างอิงกับหมายเลข IP อย่างน้อยดังนี้

- หมายเลข MAC ของอุปกรณ์
- ชื่ออุปกรณ์ (Hostname)
- วัน เวลาในการเข้าใช้งาน

๒.๕.๘ ให้ทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ดังนี้

๒.๕.๘.๑ กรณีพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบซึ่งไม่จำเป็นต้องใช้งาน ให้ปิดพอร์ตดังกล่าว

๒.๕.๘.๒ กรณีพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบซึ่งมีการใช้งานบางช่วงเวลา ให้กำหนดระยะเวลาการเปิดใช้งานเท่าที่จำเป็นและต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร โดยต้องมีการยืนยันตัวตนก่อนการเข้าใช้งานและต้องเชื่อมต่อผ่านโปรโตคอลที่มีการเข้ารหัสข้อมูล

๒.๕.๘.๓ กรณีพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบซึ่งจำเป็นต้องใช้งานเป็นประจำ ต้องมีการยืนยันตัวตนก่อนการเข้าใช้งานและต้องเชื่อมต่อผ่านโปรโตคอลที่มีการเข้ารหัสข้อมูล

๒.๕.๘.๔ สำหรับการป้องกันการเข้าถึงทางกายภาพ ให้ใช้แนวปฏิบัติในการควบคุมการเข้าออก ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

๒.๕.๙ การแบ่งแยกเครือข่าย (Segregation in networks) ให้จัดทำ VLAN โดยพิจารณาตามลักษณะการใช้งาน การรักษาความปลอดภัย และนโยบายของหน่วยงาน

๒.๕.๙.๑ องค์การคลังสินค้าได้มีการจัดแบ่งแยกเครือข่ายตามหน่วยงานระดับสำนักและตามหน้าที่เฉพาะ

๒.๕.๙.๒ กำหนดรหัสวงเครือข่าย (VLAN) ชื่อวงเครือข่าย IP Address และค่าอื่นๆ ที่ใช้ในการกำหนดในอุปกรณ์สวิทช์และอุปกรณ์ต่างๆที่เกี่ยวข้อง

๒.๕.๙.๓ มีการติดตั้งค่าอุปกรณ์ต่างๆ แล้วทำการทดสอบการใช้งานเครือข่ายแต่ละวง

๒.๕.๙.๔ จัดทำทะเบียนวงเครือข่ายและอุปกรณ์ต่างๆ ที่เกี่ยวข้อง

๒.๕.๙.๕ ผู้ดูแลระบบทำการบำรุงรักษา ตรวจเช็คการใช้งานเครือข่าย (Monitoring)

๒.๕.๙.๖ เมื่อมีการเปลี่ยนหน่วยงานจะมีการทบทวนและจัดการแบ่งแยกเครือข่ายตามโครงสร้างหน่วยงานใหม่

๒.๕.๑๐ การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ให้ควบคุม การเข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ดังนี้

๒.๕.๑๐.๑ ต้องตรวจสอบการเชื่อมต่อเครือข่ายของอุปกรณ์ต่างๆ ในศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center) อย่างน้อยเดือนละ ๑ ครั้ง

๒.๕.๑๐.๒ ต้องติดตั้งอุปกรณ์ ไฟร์วอลล์ เพื่อควบคุมการใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

๒.๕.๑๐.๓ ต้องตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๒.๕.๑๑ การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ให้ทำการควบคุมการจัดเส้นทางบนเครือข่าย ดังนี้

๒.๕.๑๑.๑ ต้องกำหนดค่าโปรโตคอลสำหรับการหาเส้นทาง (Routing protocol) ที่สอดคล้องกับเครือข่ายหลักที่หน่วยงานเชื่อมต่อ

๒.๕.๑๑.๒ ต้องบันทึกข้อมูลแผนผังการจัดเส้นทางบนเครือข่ายและข้อมูลการตั้งค่าอุปกรณ์หาเส้นทาง

๒.๕.๑๑.๓ เมื่อมีความจำเป็นต้องเปลี่ยนการหาเส้นทางบนเครือข่าย ให้ผู้ดูแลทำการปรับปรุงข้อมูลที่บันทึกไว้และแจ้งผู้บังคับบัญชาทราบ

๒.๕.๑๑.๔ กำหนดให้มีการแปลงหมายเลขเครือข่าย (NAT) เพื่อแยกเครือข่ายย่อย

๒.๕.๑๒ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่ เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๒.๕.๑๒.๑ กำหนดระบบสารสนเทศที่ต้องควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้ใช้งานได้

๒.๕.๑๒.๒ กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๒.๕.๑๒.๓ กำหนดการใช้งานระบบสารสนเทศที่สำคัญ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง ซึ่งองค์การคลังสินค้ามีแบบฟอร์มการขอใช้บริการดังกล่าว โดยมีขั้นตอนการปฏิบัติดังนี้

- ผู้ใช้งานกรอกแบบฟอร์มขอใช้บริการ/แจ้งปัญหา และได้รับอนุมัติตามสาย งานผู้แจ้ง และส่งแบบฟอร์มมายังหน่วยงานผู้ดูแลระบบแล้ว
- ผู้ดูแลระบบดำเนินการวิเคราะห์และกำหนดสิทธิการใช้งาน พร้อมทั้งทำการทดสอบการใช้งานตามสิทธิ์ เมื่อสามารถใช้งานได้แล้ว จึงแจ้งรหัสผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ปิดซองอย่างมิดชิด ส่งให้ผู้ขอใช้บริการ และให้ลงลายมือชื่อการใช้บริการ
- ผู้ดูแลระบบจัดทำรายงานสรุปการขอใช้บริการ/รับแจ้งปัญหารายไตรมาส
- สิ้นปีจะทำการทบทวนสิทธิ์การใช้งานตามรายชื่อผู้ใช้งานเทียบกับรายชื่อพนักงานที่ปฏิบัติงานอยู่ และรายชื่อบุคคลภายนอกหรือ Out Source ที่ขอ ใช้บริการ

๒.๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๒.๖.๑ ให้มีการกำหนดชื่อผู้ใช้ และรหัสผ่าน เพื่อยืนยันตัวตนในการเข้าใช้งานระบบปฏิบัติการ

๒.๖.๒ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่านของตนในการเข้าใช้งาน ระบบปฏิบัติการร่วมกัน

๒.๖.๓ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ แบบที่มีการสอบถามรหัสผ่านในการกลับเข้าใช้งานระบบปฏิบัติการ

๒.๖.๔ ผู้ใช้งานต้องทำการ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒..๕ ติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดซอฟต์แวร์ประสงค์ร้ายรวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๒.๖.๖ องค์การคลังสินค้าใช้การบริหารจัดการรหัสผ่านที่ทำงานแบบ Interactive ซึ่งรองรับโปรโตคอลมาตรฐาน LDAP หรือ Active directory

๒.๖.๗ การใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบ (Use of system utilities) ให้มีการจำกัดและควบคุมการใช้งานดังนี้

๒.๖.๗.๑ จำกัดสิทธิการติดตั้งโปรแกรมอรรถประโยชน์สำหรับระบบตามสิทธิของผู้ใช้งาน

๒.๖.๗.๒ หากผู้ใช้งานมีความจำเป็นต้องติดตั้งโปรแกรมอรรถประโยชน์สำหรับระบบให้ขออนุญาตจากผู้ดูแลระบบเป็นลายลักษณ์อักษร

๒.๖.๗.๓ กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์สำหรับระบบที่ไม่จำเป็นออกจากระบบปฏิบัติการ

๒.๖.๗.๔ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

๒.๖.๘ กำหนดมาตรการกรณีมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งดังนี้

๒.๖.๘.๑ กรณีระบบสารสนเทศทั่วไป ให้ยุติการใช้งานระบบสารสนเทศ (Session time out) หลังจากไม่มีการใช้งานเป็นเวลา ๑๕ นาที

๒.๖.๘.๒ กรณีระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญทั่วไป ให้ยุติการใช้งานระบบสารสนเทศ (Session time out) หลังจากไม่มีการใช้งานเป็นเวลา ๕ นาที

๒.๖.๙ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ให้ดำเนินการดังนี้

๒.๖.๙.๑ ให้กำหนดระยะเวลาการเชื่อมต่อสำหรับการใช้งานระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง แต่ละครั้งได้ไม่เกิน ๓ ช.ม.เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

๒.๖.๙.๒ กรณีระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง ซึ่งจำเป็นต้องเชื่อมต่อเกินระยะเวลาหรือช่วงเวลาที่กำหนด ให้ผู้ใช้งานแจ้งผู้ดูแลระบบเป็นลายลักษณ์อักษร

๒.๖.๑๐ ระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ ขั้นตอนทางเทคนิคในการยืนยันตัวตน ที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งาน ที่ระบุถึง โดยมีแนวปฏิบัติดังนี้

๒.๖.๑๐.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบ สารสนเทศของหน่วยงาน

๒.๖.๑๐.๒ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค

๒.๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๒.๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ให้จำกัดสิทธิการใช้ งานโปรแกรมประยุกต์และสารสนเทศตามสิทธิของผู้ใช้งานหรือผู้รับจ้าง (Out Source) ที่ได้รับอนุญาตเท่านั้น

๒.๗.๒ ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน โดยกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของ ข้อมูล

๒.๗.๓ ตรวจสอบการใช้งานโปรแกรมประยุกต์ ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับโปรแกรมที่ใช้ หรือการทำงานของโปรแกรมผิดพลาดให้ รีบดำเนินการแก้ไขในทันที

๒.๗.๔ สำรองโปรแกรมระบบงานประยุกต์ (File Program Backup) อย่างน้อยปีละ ๑- ๒ ครั้ง

๒.๗.๕ ทำการแยกระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน เช่นระบบที่มีข้อมูลส่วนบุคคล จะต้องดำเนินการดังนี้

๒.๗.๕.๑ แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ ให้ระบบสารสนเทศที่ใช้เฉพาะภายในหน่วยงานให้ติดตั้งในเครือข่ายภายใน ส่วนระบบสารสนเทศที่สามารถใช้งานผ่านเครือข่ายอินเทอร์เน็ตต้องติดตั้งอยู่หลังไฟร์วอลล์

๒.๗.๕.๒ ติดตั้งระบบสารสนเทศแต่ละระบบ บนสภาพแวดล้อมการประมวลผล (Computing environment) ที่แยกจากกัน เพื่อควบคุมสภาพแวดล้อมของระบบ

๒.๗.๖ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ให้ดำเนินการดังนี้

๒.๗.๖.๑ ผู้ใช้งานที่ต้องการนำอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ส่วนตัว มาใช้ในหน่วยงาน ต้องลงทะเบียนอุปกรณ์ดังกล่าวจึงจะสามารถใช้งานระบบเครือข่ายของหน่วยงานได้

๒.๗.๖.๒ บุคคลภายนอกหรือผู้รับจ้าง (Out Source) ที่ต้องการนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ส่วนตัว มาใช้ในหน่วยงาน ให้สามารถใช้งานได้เฉพาะอินเทอร์เน็ต โดยให้ติดต่อผู้ดูแลระบบเพื่อขอชื่อผู้ใช้และรหัสผ่าน

๒.๗.๗ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) มีข้อกำหนดในการปฏิบัติงานดังนี้

๒.๗.๗.๑ ไม่ใช้เครื่องคอมพิวเตอร์สาธารณะในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน

๒.๗.๗.๒ ไม่ใช้งานระบบสารสนเทศของหน่วยงานผ่านเครือข่ายที่ไม่น่าเชื่อถือ เครือข่ายในร้านอินเทอร์เน็ต เครือข่ายไร้สายที่ไม่ได้ให้บริการโดยผู้ให้บริการอินเทอร์เน็ต หรือหน่วยงานภาครัฐ เป็นต้น

๒.๗.๗.๓ การนำเครื่องคอมพิวเตอร์ของหน่วยงานออกไปใช้ภายนอกหน่วยงานต้องมีการเข้ารหัสข้อมูลที่สำคัญในสื่อบันทึกข้อมูลต่างๆ

๒.๘ การควบคุมการเข้าออกศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

๒.๘.๑ มีการควบคุมดูแลการเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ของ อคส. ๒ ชั้น

๒.๘๖.๑.๑. ประตูชั้นนอก ใช้คีย์การ์ด หรือการแสกนลายนิ้วมือที่ให้เฉพาะเจ้าหน้าที่ที่ดูแลระบบของแต่ละหน่วยงานในกระทรวงพาณิชย์เท่านั้น

๒.๘.๑.๒ ประตูชั้นใน เป็นประตูเหล็กที่มีระบบแสกนนิ้วมือให้เจ้าหน้าที่แต่ละหน่วยงานเพื่อเข้า-ออกในห้องควบคุมของหน่วยงานตนเอง

๒.๘.๑.๓ มีกล้องวงจรปิดบันทึกผู้เข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ เพื่อเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้ง ป้องกันความเสียหายอื่นๆที่อาจเกิดขึ้นได้

๒.๘.๒ มีการกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อคส. เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายประกอบด้วย

๒.๘.๒.๑ เจ้าหน้าที่ส่วนงานบริหารฐานข้อมูลที่ดูแลห้องควบคุมระบบคอมพิวเตอร์ อคส.ต้องได้รับการแสกนลายนิ้วมือจากสำนักงานปลัด กระทรวงพาณิชย์ เพื่อเข้า-ออกห้องควบคุมเท่านั้น

๒.๘.๒.๒ มีการจัดทำ "ตารางเวรของเจ้าหน้าที่ดูแลห้องควบคุมฯ " เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับเท่านั้น

๒.๘.๒.๓ เจ้าหน้าที่องค์การคลังสินค้า หรือบุคคลภายนอก (Out Source) ที่เข้ามาติดต่อขอเข้า

ห้องควบคุมระบบคอมพิวเตอร์ต้องได้รับอนุญาต และต้องลงชื่อในสมุดบันทึกการเข้า-ออกในแบบฟอร์มและจะต้องมีเจ้าหน้าที่ที่ดูแลห้องควบคุมอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๒.๙ การควบคุมการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

๒.๙.๑ ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูง หรือ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดย เคร่งครัด

๒.๙.๒ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูง หรือ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้งาน

๒.๑๐ การควบคุมการเข้าถึงเครือข่ายไร้สาย (Wireless Network Access Control)

๒.๑๐.๑ การติดตั้ง Access Point, Wireless Router หรืออุปกรณ์อื่นๆ ที่มีการทำงานในลักษณะเดียวกัน ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และ ต้องกำหนดรหัสการเข้าใช้งาน เพื่อเป็นการรักษาความมั่นคงปลอดภัยในการใช้งาน อุปกรณ์ดังกล่าวกรณีได้รับอนุญาต ให้ผู้ดูแลระบบดำเนินการ ดังนี้

๒.๑๐.๑.๑ ต้องวางอุปกรณ์ในตำแหน่งที่เหมาะสม และ ต้องเพิ่มการรับรองการเข้ารหัสด้วย (Authentication)

๒.๑๐.๑.๒ ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้อุปกรณ์ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น หรือตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น

๒.๑๐.๑.๓ ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำอุปกรณ์มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัวอุปกรณ์ด้วย

๒.๑๐.๑.๔ ต้องเขียนคู่มือการติดตั้งอุปกรณ์อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

๒.๑๐.๑.๕ ต้องกำหนดรูปแบบการรักษาความปลอดภัย แบบ WPA๒ (Wi-Fi Protected Access) หรือรูปแบบที่ดีกว่า

๒.๑๐.๒ ห้ามผู้ใช้งาน ใช้งานเครือข่ายแบบ Ad-Hoc หรือ Peer-To-Peer

๒.๑๐.๓ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๒.๑๐.๔ ผู้ดูแลระบบใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของเครือข่ายไร้ สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์น่าสงสัยที่เกิดขึ้นในเครือข่ายไร้สาย และ จัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งาน เครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการสำนักเทคโนโลยี สารสนเทศทราบทันที

๒.๑๑ การใช้จดหมายอิเล็กทรอนิกส์ (Email)

๒.๑๑.๑ ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (Email) ต้องทำการกรอกข้อมูล คำขอ

เข้าใช้บริการจดหมายอิเล็กทรอนิกส์ ของหน่วยงานลงในแบบฟอร์ม โดยยื่น แบบฟอร์มกับเจ้าหน้าที่ ผู้ดูแลระบบ สำนักเทคโนโลยีสารสนเทศ อคส.

๒.๑๑.๒ เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ต้องเปลี่ยนรหัสผ่านโดยทันที

๒.๑๑.๓ ห้ามบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

๒.๑๑.๔ ทำการเปลี่ยนรหัสผ่านทุก ๖ เดือน

๒.๑๑.๕ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์ และให้ ถือว่าเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานที่อยู่จดหมาย อิเล็กทรอนิกส์ดังกล่าว

๒.๑๑.๖ การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของ อคส. ผู้ใช้งาน จะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมาย อิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. ขัดข้องและ ได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

๒.๑๑.๗ การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๒.๑๑.๘ การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุก ปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็น ส่วนบุคคล โดยอ้างว่าเป็นความเห็นของ อคส. หรือก่อให้เกิดความเสียหายต่อ อคส.

๒.๑๑.๙ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เพื่อเผยแพร่ ข้อมูลข้อความ รูปภาพ หรือ สิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อ การดำเนินงานของ อคส. ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของ อคส.

๒.๑๑.๑๐ ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นในอีเมล์ หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด

๒.๑๑.๑๑ ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ E-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม

๒.๑๑.๑๒ ผู้ใช้งานต้องหลีกเลี่ยงการใช้คำสั่ง "Reply with History" ซึ่งเป็นการตอบกลับอีเมล์พร้อมไฟล์แนบไปยังผู้รับ ยกเว้นในกรณีที่จำเป็นต้องใช้งานเท่านั้น อย่างไรก็ตาม เมื่อมีการใช้งานคำสั่ง "Reply with History" ผู้ใช้งานควรทำการลบไฟล์แนบทิ้งเสียก่อนที่จะทำการส่งอีเมล์

๒.๑๑.๑๓ ผู้ใช้งานต้องทำการส่งอีเมล์ให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้นและห้ามใช้คำสั่ง "Reply All" ถ้าหากอีเมล์ฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน

๒.๑๑.๑๔ ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้าต่างๆ (Spam Mail) เป็นต้น

๒.๑๑.๑๕ ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใดๆ กับการส่ง อีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด

๒.๑๑.๑๖ ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

๒.๑๑.๑๗ การส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เสร็จสิ้นต้องออกจาก

ระบบ (Log out) ทุกครั้ง

๒.๑๒ การใช้เครือข่ายอินเทอร์เน็ต (Internet)

๒.๑๒.๑ ผู้ใช้งานที่ต้องการใช้เครือข่ายอินเทอร์เน็ต ต้องลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ต โดยยื่นคำขอกับเจ้าหน้าที่ผู้ดูแลระบบ สำนักเทคโนโลยีสารสนเทศ อคส. สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

๒.๑๒.๒ ไม่ใช้เครือข่ายคอมพิวเตอร์ของหน่วยงานที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความ มั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๒.๑๒.๓ ผู้ใช้งานอินเทอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และ ต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่อง แม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๒.๑๒.๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ตของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ เครือข่ายอินเทอร์เน็ตนั้นต้องเป็นผู้รับผิดชอบ

๒.๑๒.๕ ห้ามเปิดเผยข้อมูลของหน่วยงานที่เป็นความลับ หรือข้อมูลสำคัญที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านเครือข่ายอินเทอร์เน็ต

๒.๑๒.๖ การดาวน์โหลดข้อมูลและโปรแกรมต่างๆ จากเครือข่ายอินเทอร์เน็ต ต้องกระทำด้วย ความระมัดระวัง และหากมีความจำเป็นต้องดาวน์โหลดไฟล์ขนาดใหญ่ ให้ดำเนินการ นอกเวลาปฏิบัติงาน

๒.๑๒.๗ ห้ามดาวน์โหลดข้อมูลและโปรแกรมต่างๆ ที่ละเมิดลิขสิทธิ์ จากเครือข่ายอินเทอร์เน็ต

๒.๑๒.๘ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้ เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรขอ หน่วยงานอื่นๆ

๒.๑๒.๙ ผู้ใช้งาน ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้สำนักงานฯ และบุคคลผู้ที่เกี่ยวข้องกับสำนักงานฯ เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

๒.๑๒.๑๐ ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใดๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

๒.๑๒.๑๑ หลังจากใช้งานเครือข่ายอินเทอร์เน็ตเสร็จแล้ว ให้ Log out จากระบบการพิสูจน์ตัวจริง เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๒.๑๓ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access control)

๒.๑๓.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒.๑๓.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

๒.๑๓.๒.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

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

๒.๑๓.๒.๒ กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

๒.๑๓.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๑๓.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

๒.๑๓.๓.๑ จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการพาณิชย์ที่ให้บริการ ข้อมูลรับจำนำโครงการต่างๆ ข้อมูลซื้อ-ขายสินค้า ข้อมูลคลังสินค้า เป็นต้น

๒.๑๓.๓.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๒.๑๓.๓.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๒.๑๓.๓.๔ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๒.๑๓.๓.๕ การกำหนดเวลาที่ได้เข้าถึง

- ข้อมูลสารสนเทศด้านการบริหาร (Back Office) สำหรับผู้ใช้งานภายในสามารถเข้าถึงระบบสารสนเทศได้ตลอด ๒๔ ชั่วโมง (ต้องเข้ามาที่สำนักงานเท่านั้น)
- ข้อมูลสารสนเทศด้านการพาณิชย์ที่ให้บริการ (Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง

๒.๑๓.๓.๖ การกำหนดช่องทางที่สามารถเข้าถึง

- ผ่านระบบสารสนเทศที่ให้บริการ
- ผ่านทางจดหมายอิเล็กทรอนิกส์
- ผ่านทาง Teleworking
- ผ่านเครื่องมือ (Tools) การเข้าถึง

๒.๑๔ การป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

๒.๑๔.๑ เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส รุ่นล่าสุดที่ได้รับการอนุมัติ และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง

๒.๑๔.๒ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุด (Update Latest Pattern) อยู่เสมอ เครื่องให้บริการ เครื่องตั้งโต๊ะ และโน้ตบุ๊คทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส

๒.๑๔.๓ เอกสารการติดตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุก ๖ เดือน และต้องจัดทำเอกสาร Checklist ประกอบการตรวจสอบด้วย

๒.๑๔.๔ ห้ามเจ้าหน้าที่ทำการดาวน์โหลด แชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต โดยปราศจากการอนุมัติ หลังจากการอนุมัติแล้ว เจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัส ก่อนการใช้งาน

๒.๑๔.๕ ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมล์ สำเนาจากแผ่นดิสก์ หรือไฟล์แชร์ต่าง ๆ ต้องได้รับการสแกนหาไวรัส

๒.๑๔.๖ ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใดๆ ตัวอย่าง เช่น ไวรัส หนอนอินเทอร์เน็ต โปรแกรมแฝง (ม้าโทรจัน) อีเมล์บอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ขององค์การ

๒.๑๔.๗ ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

๒.๑๔.๘ ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้น ที่ได้รับอนุญาตให้สามารถรับ-ส่งผ่านระบบเครือข่ายขององค์การ ได้ ทั้งนี้ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จัก และจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสขององค์การ ก่อนเปิดใช้งานเสมอ

๒.๑๔.๙ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชั่นการทำงานเชื่อมต่อกับอินเทอร์เน็ตยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

๒.๑๕ การบริหารจัดการทรัพย์สินด้านเทคโนโลยีดิจิทัลขององค์การคลังสินค้า (Asset Management)

๒.๑๕.๑ หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์การคลังสินค้า มีวัตถุประสงค์เพื่อป้องกันทรัพย์สินขององค์การคลังสินค้าจากความเสียหายที่อาจเกิดขึ้นได้

- จัดทำบัญชีทรัพย์สิน
- ระบุผู้เป็นเจ้าของทรัพย์สิน
- การใช้งานทรัพย์สินที่เหมาะสม

๒.๑๕.๒ การจัดหมวดหมู่สารสนเทศ มีจุดประสงค์เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์การคลังสินค้าอย่างเหมาะสม

- จัดหมวดหมู่ทรัพย์สินสารสนเทศ โดยจะต้องจัดให้มีกระบวนการนการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นของความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อองค์การคลังสินค้า ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม
- จัดทำป้ายชื่อ และจัดการทรัพย์สินสารสนเทศ จะต้องจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว

ส่วนที่ ๓

แนวปฏิบัติการจัดทำระบบสำรองของสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลัก และไฟล์โปรแกรมระบบงานที่สำคัญ ที่ทำหน้าที่ให้บริการข้อมูลที่ถูกต้องและทันสมัย และเตรียมความ พร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้ กลับคืนได้ภายในระยะเวลาที่เหมาะสม

ผู้รับผิดชอบ

สำนักที่ดูแลรับผิดชอบด้านเทคโนโลยีดิจิทัล

อ้างอิงมาตรฐาน

ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ (Information Security Management System : ISMS)

แนวปฏิบัติ

๓.๑ การสำรองสารสนเทศ

ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพ พร้อมใช้งาน โดยต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพ และพร้อมใช้งานตามแนวทางต่อไปนี้

๓.๑.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อย ปีละ ๑ ครั้ง

๓.๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental backup)
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อ ข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ การจัดการข้อมูลในฐานข้อมูล เป็นต้น
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้ สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการ สำรองข้อมูลไว้อย่างชัดเจน
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
- ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

- ทดสอบข้อมูลสำรองที่บันทึกไว้อย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- ต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูล และการเรียกคืนข้อมูลในแต่ละครั้ง
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๓.๒ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉิน

๓.๒.๑ ต้องจัดทำระบบสำรองของระบบสารสนเทศหลักที่สำคัญของหน่วยงานไว้อย่างเพียงพอและต้องมีการทดสอบการทำงานของระบบสำรองอย่างสม่ำเสมอ

๓.๒.๒ ต้องจัดทำแผนการกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยมีรายละเอียดดังนี้

- การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินงานของหน่วยงาน และการให้บริการด้านเทคโนโลยีสารสนเทศ
- การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
- การดำเนินการเพื่อให้สามารถดำเนินงานของหน่วยงาน เป็นไปได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
- การกลับคืนสู่การทำงานปกติ เพื่อให้การดำเนินงานหน่วยงาน กลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

๓.๒.๓ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.๒.๔ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการ ด้วยวิธีการทางอิเล็กทรอนิกส์

๓.๒.๕ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๖ ต้องทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่ เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

ส่วนที่ ๔

แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

กำหนดมาตรการในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของหน่วยงาน เพื่อให้ระบบสารสนเทศของ อคส. มีความปลอดภัยและเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิด ขึ้นกับระบบสารสนเทศของ อคส. ได้

ผู้รับผิดชอบ

สำนักที่ดูแลรับผิดชอบด้านเทคโนโลยีดิจิทัล

อ้างอิงมาตรฐาน

COBIT ๕

แนวปฏิบัติ

๔.๑ การตรวจสอบและประเมินความเสี่ยง

๔.๑.๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit And Assessment) โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) และให้จัดทำ รายงานพร้อมข้อเสนอแนะอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๔.๑.๒. มีการจัดทำและทบทวนกระบวนการบริหารจัดการความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง โดยมีการวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงด้านสารสนเทศอย่างเหมาะสม รวมถึงการควบคุมและลดความเสี่ยงเหล่านั้น

๔.๑.๓. มีการทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๔.๑.๔. ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

๔.๑.๕. ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๔.๑.๖ กรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้ โดยมีการป้องกันเป็นอย่างดี

๔.๑.๗. ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบและ ประเมินความเสี่ยงด้านสารสนเทศ โดยแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบสารสนเทศที่ให้บริการจริงหรือที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกัน เครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๕

แนวปฏิบัติการสร้างความรู้ความเข้าใจเกี่ยวกับ ความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า

วัตถุประสงค์

เพื่อสร้างความรู้ ความเข้าใจและความตระหนักเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร โดยการเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และจัดฝึกอบรมให้ความรู้ ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับแนวปฏิบัติขององค์กร

ผู้รับผิดชอบ

สำนักที่ดูแลรับผิดชอบด้านเทคโนโลยีดิจิทัล

อ้างอิงมาตรฐาน

ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ (Information Security Management System : ISMS)

แนวปฏิบัติ

๕.๑ การสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัย

๕.๑.๑. จัดฝึกอบรมนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับ ภาระงาน บทบาทหน้าที่ในการปฏิบัติงานของของบุคลากร อย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน เพื่อเป็นการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

๕.๑.๒. เผยแพร่ หรือประชาสัมพันธ์ให้ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่เข้าใจง่าย โดยมีการปรับปรุงความรู้อย่างสม่ำเสมอ

๕.๑.๓. บุคลากรใหม่ต้องได้รับการอบรมเกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องอย่างน้อยภายใน ๙๐ วันนับจากเข้าปฏิบัติหน้าที่

ส่วนที่ ๖

แนวปฏิบัติการใช้บริการคลาวด์

ขององค์การคลังสินค้า

วัตถุประสงค์

เพื่อใช้อ้างอิงประกอบการพิจารณาบริการของผู้ให้บริการคลาวด์ โดยคำนึงถึงหลักเกณฑ์ขั้นพื้นฐาน ซึ่งเป็นมาตรการขั้นต่ำในการลดความเสี่ยงจากภัยคุกคาม โดยจะต้องตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ รวมทั้งปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสม

ผู้รับผิดชอบ

สำนักที่ดูแลรับผิดชอบด้านเทคโนโลยีดิจิทัล

อ้างอิงมาตรฐาน

- ISO

ISO/ IEC ๒๐๐๐๐- ๑ (Information Technology Service Management System: ITSMS)

ISO/IEC ๒๗๐๐๑ (Information Security Management System)

ISO/ IEC ๒๗๐๑๗ (Information technology – Security techniques –Code of practice for information security controls based on

ISO/IEC ๒๗๐๐๒ for Cloud Service)

ISO/ IEC ๒๗๐๑๘ (Information technology – Security techniques –Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)

- CSA STAR

CSA STAR Self-Assessment

CSA STAR Certification

CSA STAR Attestation

- NIST

SP ๘๐๐-๑๗๑ Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

แนวปฏิบัติ

๖.๑ กระบวนการทำงาน

นโยบายและแนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยสารสนเทศ นโยบายการพัฒนาทรัพยากรบุคลากรให้มีความรู้ความเข้าใจในเรื่องความมั่นคงปลอดภัยของข้อมูล นโยบายการจัดการสินทรัพย์ นโยบายการจัดการเปลี่ยนแปลง นโยบายการบริหารความเสี่ยง กระบวนการตอบสนองต่อเหตุการณ์ฉุกเฉิน การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน การติดตามดูแลการให้บริการ กระบวนการจ้างช่วงต่อสัญญาและการปฏิบัติอื่นใดตามที่กฎหมายกำหนด

๖.๒ มาตรการป้องกันทางกายภาพ

มาตรการป้องกันเพื่อรักษาความมั่นคงปลอดภัยแก่สินทรัพย์ทางกายภาพ เช่น การกำหนดควบคุมพื้นที่ ความปลอดภัยในพื้นที่หวงห้าม การควบคุมการเข้าออกพื้นที่

๖.๓ มาตรการป้องกันทางเทคนิค

มาตรการป้องกันสาหรับความมั่นคงปลอดภัยและความน่าเชื่อถือทางเทคนิค เช่น โครงสร้างระบบเสมือน (Virtual Infrastructure) และสภาพแวดล้อมของระบบ การควบคุมการเข้าถึง การยืนยันตัวตน การตรวจสอบสิทธิของผู้ใช้งาน ระบบความมั่นคงปลอดภัยเครือข่าย การคุ้มครองข้อมูลการเข้ารหัส การวิเคราะห์ออกแบบและพัฒนาระบบตามวัฏจักรการพัฒนาระบบงาน (System Development Life Cycle : SDLC) แนวทางการรักษาความปลอดภัยในการพัฒนาซอฟต์แวร์และ Application Programming Interface (API) และแนวทางในการรักษาความปลอดภัยในการจ้างบุคคลภายนอก (Outsourcing)

๖.๔ ประสิทธิภาพการให้บริการ

ผู้ใช้บริการควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับสภาพพร้อมใช้งาน ระยะเวลาการตอบสนอง ความสามารถรองรับปริมาณงาน บริการสนับสนุน และกระบวนการยุติสัญญา ซึ่งมีสาระสำคัญดังต่อไปนี้

๖.๔.๑ สภาพพร้อมใช้งาน (Availability) ความพร้อมใช้งานของบริการครอบคลุมร้อยละของเวลาที่พร้อมให้บริการต่อปี (Uptime) เช่น ไม่ต่ำกว่าร้อยละ ๙๙.๙ เป็นต้น

๖.๔.๒ ระยะเวลาการตอบสนอง (Response Time) ระยะเวลาการตอบสนองต่อเหตุการณ์ ซึ่งเป็นระยะเวลานับแต่ผู้ใช้บริการแจ้งความประสงค์ และผู้ให้บริการได้ดาเนินการต่อความประสงค์นั้น โดยระยะเวลาการตอบสนองเป็นหลักการพิจารณาที่สำคัญ ของผู้ใช้บริการ การตอบสนองล่าช้ากว่ากำหนดอาจส่งผลให้เกิดความเสียหาย

๖.๔.๓ ความสามารถรองรับปริมาณงาน (Capacity) จำนวนปริมาณการเชื่อมต่อสูงสุดพร้อมกัน (Maximum Simultaneous Connections) ปริมาณการใช้งานของผู้ใช้บริการพร้อมกัน (Maximum Simultaneous Users) ปริมาณความจุของระบบที่รองรับการใช้งาน (Resource Capacity) และปริมาณงาน (Throughput)

๖.๔.๔ การบริการสนับสนุน ช่องทางและช่วงเวลาที่ผู้ใช้บริการสามารถแจ้งปัญหา หรือติดต่อสอบถามจากผู้ให้บริการ เช่น การกำหนดให้ผู้ใช้บริการสามารถติดต่อผู้ให้บริการได้ตลอด ๒๔ ชั่วโมง และระยะเวลาในการแก้ไขปัญหาการใช้งานตั้งแต่เริ่มต้นจนปัญหานั้นสิ้นสุด

๖.๔.๕ กระบวนการยุติสัญญา แนวทางกระบวนการยุติสัญญาล่วงหน้า กรณีผู้ใช้บริการ หรือผู้ให้บริการต้องการยุติสัญญา โดยควรกำหนดแนวทางการดาเนินการ เช่น ระยะเวลาสาหรับการเข้าถึงข้อมูลของผู้ใช้บริการ และระยะเวลาการเก็บรักษาข้อมูลของผู้ให้บริการ และการกำหนดแผนการเลิกใช้บริการ (Exit Plan)

๖.๕ การรักษาความมั่นคงปลอดภัย

ควรพิจารณามาตรการ การรักษาความมั่นคงปลอดภัยในระบบสารสนเทศในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับความน่าเชื่อถือของบริการ การพิสูจน์ตัวตนและการอนุญาต การเข้ารหัส การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ การตรวจสอบขั้นตอนกระบวนการทางานและความปลอดภัย

๖.๕.๑ การพิสูจน์ตัวตนและการอนุญาต กระบวนการพิสูจน์ตัวตนเพื่อเป็นการตรวจสอบความมีตัวตนของผู้มีสิทธิ์ในการเข้าใช้งาน ระยะเวลาเวลาในการดาเนินการเพิ่มหรือถอนสิทธิ์ผู้ใช้บริการที่เหมาะสม การป้องกันการเข้าใช้งานจากผู้ที่ไม่มีสิทธิ์ การกำหนดระดับการยืนยันตัวตน (Authentication Level) และการควบคุมการเข้าถึงการใช้งานจากบุคคลภายนอกที่สนับสนุนการให้บริการ (Outsourcing)

๖.๕.๒ การเข้ารหัส การเข้ารหัสในการแปลงข้อมูลเพื่อปกปิดข้อมูลป้องกันการเข้าถึง การแก้ไข และการใช้งาน โดยไม่ได้รับอนุญาต การกาหนดการเข้ารหัสให้สอดคล้องกับประเภทข้อมูล (Data Classification) และจัดให้มีนโยบายการควบคุมกุญแจสำหรับการเข้ารหัส (Key Access Control Policy) ตามความเหมาะสม

๖.๕.๓ การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย การจัดการเหตุการณ์และ

การรักษาความมั่นคงปลอดภัยของข้อมูล เริ่มตั้งแต่กระบวนการตรวจพบเหตุการณ์ การรายงานเหตุการณ์ การประเมิน การตอบสนอง การแก้ปัญหา และการเรียนรู้จากเหตุการณ์ความปลอดภัยที่เกิดขึ้น

๖.๕.๔ การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ การบันทึกข้อมูลที่เกี่ยวข้องกับการดำเนินการและการใช้บริการเพื่อให้สามารถตรวจสอบข้อมูลย้อนหลังได้

๖.๕.๕ การตรวจสอบขั้นตอนกระบวนการทางานและความปลอดภัย การตรวจสอบกระบวนการทางานและความปลอดภัยอย่างเป็นระบบอ้างอิงมาตรฐานสากล มีความเป็นอิสระ มีขั้นตอนการทางานที่มีเอกสารหลักฐาน และกำหนดสิทธิของผู้ตรวจสอบภายในผู้ตรวจสอบภายนอก เป็นประจำอย่างสม่ำเสมอ รวมถึงการกำหนดให้หน่วยงานของรัฐที่มีอำนาจตามกฎหมายสามารถเข้าตรวจสอบได้

๖.๕.๖ การจัดการช่องโหว่ การตรวจสอบ ประเมิน และบริหารจัดการช่องโหว่ หรือจุดเสี่ยงในระบบกระบวนการรักษาความปลอดภัยของระบบ มาตรการรักษาความมั่งคงปลอดภัยไซเบอร์ การควบคุมภายในหรือการใช้งานที่อาจถูกนาไปใช้หรือถูกเรียกใช้โดยภัยคุกคาม กรณีบริการที่มีความสำคัญและมีความจาเป็นอาจมีการทดสอบระบบความปลอดภัย Vulnerability Assessments และ Penetration Testing โดยจะต้องดำเนินการตามมาตรการ และวิธีการที่เหมาะสมเพื่อลดความเสี่ยงในการเกิดความเสียหาย

๖.๕.๗ ธรรมาภิบาล การแจ้งให้ผู้ใช้บริการทราบล่วงหน้าในระยะเวลาที่เหมาะสม กรณีการเปลี่ยนแปลงการให้บริการอันเนื่องมาจากการปรับปรุง อัพเดตซอฟต์แวร์ ที่อาจส่งผลกระทบต่อกระบวนการทางาน ช่องทางการให้บริการหรือรายละเอียดในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA)

๖.๖ การจัดการข้อมูล

ควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับการจัดประเภทข้อมูล การสารองข้อมูลและการเรียกคืนข้อมูล วงจรชีวิตของข้อมูล และการโอนย้ายข้อมูล ซึ่งมีสาระสำคัญดังต่อไปนี้

๖.๖.๑ การจัดประเภทข้อมูล ประเภทความเป็นเจ้าของข้อมูล ได้แก่ ข้อมูลของผู้ใช้บริการ ข้อมูลของผู้ให้บริการ และ ข้อมูลที่เกิดจากการประมวลผลข้อมูลของผู้ใช้บริการ (Derived Data) ผู้ให้บริการควรจัดให้มีนโยบายที่เกี่ยวข้องกับการใช้ข้อมูลของผู้ใช้บริการ การกาหนดขอบเขตและแนวปฏิบัติ รวมถึงกาหนดสิทธิ์ในการตรวจสอบข้อมูลที่เกิดจากการประมวลผลข้อมูลของผู้ใช้บริการ

๖.๖.๒ การสารองข้อมูล และการเรียกคืนข้อมูล การสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งาน โดยกำหนดระยะเวลา ความถี่ในการดาเนินการวิธีการ และการเก็บรักษาที่เหมาะสม ในกรณีที่ข้อมูลปัจจุบันถูกทำลายหรือได้รับความเสียหายส่งผลทำให้ไม่สามารถใช้งานได้ ผู้ให้บริการควรดาเนินการเรียกคืนข้อมูลเพื่อให้เกิดความพร้อมในการใช้งานตามที่ระบุไว้ในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA)

๖.๖.๓ วงจรชีวิตของข้อมูล นโยบายและแนวปฏิบัติที่เหมาะสมในการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพครอบคลุม กระบวนการสร้าง การเก็บรักษา การใช้ การเปิดเผย และการทำลายข้อมูล

๖.๖.๔ การโอนย้ายข้อมูล นโยบายและแนวปฏิบัติในการส่งออกข้อมูล โดยกำหนดรูปแบบ หรือกระบวนการส่งออก ตามความเหมาะสมในกรณียุติข้อตกลงการให้บริการ

๖.๗ การคุ้มครองข้อมูลส่วนบุคคล

ควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA)ที่เกี่ยวข้องกับแนวปฏิบัติตามมาตรฐานสากลในการคุ้มครองข้อมูลส่วนบุคคล การระบุวัตถุประสงค์การเก็บข้อมูล การเก็บรักษาข้อมูลเท่าที่จาเป็น การใช้ เก็บรักษาและการเปิดเผย ความโปร่งใสและการแจ้งเตือนความรับผิดชอบต่อข้อมูล สถานที่จัดเก็บข้อมูล และการอานวยความสะดวกในการเข้าถึงข้อมูล ซึ่งมีสาระสำคัญดังต่อไปนี้

๖.๗.๑ แนวปฏิบัติตามมาตรฐานสากล นโยบาย แนวทางปฏิบัติ มาตรการ หรือมาตรฐานที่

สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๖.๗.๒ การระบุวัตถุประสงค์ ระบุวัตถุประสงค์และความยินยอมในการรวบรวม เก็บรักษา การใช้และการเปิดเผยข้อมูลให้ชัดเจน ทั้งนี้ ผู้ให้บริการควรระมัดระวังในการดำเนินการกับข้อมูลส่วนบุคคล

๖.๗.๓ การเก็บรักษาข้อมูลเท่าที่จำเป็น ระยะเวลาในการเก็บรักษาข้อมูลที่เหมาะสม และการกำหนดระยะเวลาในการเก็บรักษาข้อมูลหลังจากมีการแจ้งให้ทำลายข้อมูล

๖.๗.๔ การใช้ เก็บรักษา และการเปิดเผย การแจ้งผู้ใช้บริการทราบว่า ผู้ให้บริการจะไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บรวบรวมไว้ เว้นแต่ได้รับความยินยอมจากผู้ใช้บริการ หรือเป็นกรณีที่กฎหมายกำหนด หรือเป็นการเปิดเผยแก่หน่วยงานที่มีอำนาจตามกฎหมาย หรือตามคำสั่งศาล

๖.๗.๕ ความโปร่งใส และการแจ้งเตือน การแจ้งให้ผู้ใช้บริการทราบและให้ข้อมูลที่เพียงพอเกี่ยวกับความโปรงใส่ ในการดาเนินการกับข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

๖.๗.๖ ความรับผิดชอบต่อข้อมูล นโยบายและแนวปฏิบัติในกรณีการละเมิดข้อมูล และควรมีกระบวนการ เอกสารหลักฐานที่ได้ดำเนินการที่สอดคล้องกับแนวทางการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากความรับผิดชอบด้านสารสนเทศจะเป็นส่วนสำคัญในการตรวจสอบการละเมิดข้อมูลส่วนบุคคล

๖.๗.๗ สถานที่จัดเก็บข้อมูล การแสดงให้ผู้ใช้บริการทราบสถานที่ในการจัดเก็บข้อมูล หรือกาหนดให้ผู้ใช้บริการสามารถเลือกสถานที่จัดเก็บข้อมูลได้ เพื่อเป็นการลดความเสี่ยงในการถูกละเมิดเนื่องจากการประมวลผลข้อมูลส่วนบุคคลอาจจะถูกโอนย้ายข้อมูลไปยังต่างประเทศ ซึ่งอาจจะมีกฎหมาย กฎระเบียบหรือระดับการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน

๖.๗.๘ การอำนวยความสะดวกในการเข้าถึงข้อมูล การอำนวยความสะดวกแก่ผู้ใช้บริการในระยะเวลาที่เหมาะสมและมีประสิทธิภาพ ทั้งนี้ห้ามมิให้ผู้ให้บริการใช้ข้อกำหนดทางเทคนิคหรือข้อกำหนดขององค์กรเป็นอุปสรรคในการ ปฏิเสธสิทธิ์ของเจ้าของข้อมูล