ประกาศกรมกิจการผู้สูงอายุ
เรื่อง ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับปี พ.ศ. ๒๕๖๙ กรมกิจการผู้สูงอายุ

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ประกอบกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๓ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามที่กำหนดไว้ในแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ดำเนินการให้เป็นไปตามนโยบายและแผนตามมาตรา ๔๒

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ ประกอบมติที่ประชุมคณะทำงานเทคโนโลยีสารสนเทศ กรมกิจการผู้สูงอายุ ครั้งที่ ๒/๒๕๖๙ เมื่อวันที่ ๗ กรกฎาคม ๒๕๖๙ เห็นชอบข้อปฏิบัติดังกล่าว จึงประกาศข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับปี พ.ศ. ๒๕๖๙ กรมกิจการผู้สูงอายุ มีรายละเอียดแนบท้ายประกาศนี้ ตั้งแต่บัดนี้เป็นต้นไป

จึงประกาศให้ทราบและถือปฏิบัติอย่างเคร่งครัดโดยทั่วกัน

ประกาศ ณ วันที่ ๙ กันยายน พ.ศ. ๒๕๖๙

(นายโชคชัย วิเชียรชัยยะ)
อธิบดีกรมกิจการผู้สูงอายุ

ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ฉบับปี พ.ศ. 2569

กรมกิจการผู้สูงอายุ

คำนำ

ในยุคปัจจุบันที่เทคโนโลยีดิจิทัลเข้ามามีบทบาทสำคัญอย่างยิ่งต่อการขับเคลื่อนภารกิจของภาครัฐ กรมกิจการผู้สูงอายุได้มุ่งมั่นนำระบบสารสนเทศและนวัตกรรมดิจิทัลมาประยุกต์ใช้ เพื่อยกระดับการให้บริการ การบริหารจัดการ และการส่งเสริมคุณภาพชีวิตของผู้สูงอายุอย่างครอบคลุม ซึ่งการขับเคลื่อนภารกิจกรมกิจการผู้สูงอายุสู่การเป็นองค์กรดิจิทัล จำเป็นต้องอาศัยรากฐานด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ ควบคู่ไปกับมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่รัดกุม ท่ามกลางบริบทความเปลี่ยนแปลงทางเทคโนโลยีและภัยคุกคามทางไซเบอร์ที่เพิ่มสูงขึ้น มีความซับซ้อนและทวีความรุนแรงขึ้นอย่างต่อเนื่องในปัจจุบัน

กรมกิจการผู้สูงอายุ ได้เล็งเห็นถึงความสำคัญของการเปลี่ยนแปลงทางเทคโนโลยี จึงผลักดันให้เกิด **“ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับปี พ.ศ. 2569 กรมกิจการผู้สูงอายุ”** ฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางมาตรฐานในการปฏิบัติงานสำหรับบุคลากรทุกระดับ รวมถึงบุคคลภายนอกทุกภาคส่วนถือปฏิบัติร่วมกันอย่างเป็นรูปธรรม โดยมุ่งเน้นการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของระบบสารสนเทศและข้อมูลสำคัญ ตลอดจนการคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพและสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงมาตรฐานสากลที่เกี่ยวข้อง โดยหวังเป็นอย่างยิ่งว่า ข้อปฏิบัติฉบับนี้จะเป็นประโยชน์และเป็นคู่มือในการปฏิบัติงานที่สร้างความตระหนักรู้ ป้องกันความเสี่ยง และเสริมสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ของกรมกิจการผู้สูงอายุ ยกระดับมาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศและการปกป้องข้อมูลสำคัญขององค์กร และสร้างความเชื่อมั่นให้แก่ประชาชนและผู้รับบริการอย่างยั่งยืน

กองยุทธศาสตร์และแผนงาน
กันยายน 2569

สารบัญ

หน้า

บทนำ

ความเป็นมา

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 43 และมาตรา 44 ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามที่กำหนดไว้ในแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการให้เป็นไปตามนโยบายและแผนตามมาตรา 42

เพื่อให้การพัฒนาระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ จึงเห็นสมควรกำหนดข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ โดยให้ครอบคลุมการดำเนินการ ดังนี้

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(2) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ ทั้งนี้ จะต้องเผยแพร่ข้อปฏิบัติฯ ดังกล่าว ให้เจ้าหน้าที่ทุกระดับในกรมกิจการผู้สูงอายุและผู้เกี่ยวข้องได้รับทราบและถือปฏิบัติโดยเคร่งครัด และต้องดำเนินการทบทวนปรับปรุงข้อปฏิบัติฯ ให้เป็นปัจจุบันอยู่เสมอ องค์ประกอบของข้อปฏิบัติฯ ประกอบด้วย

เรื่องที่ 1 ข้อปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ
เรื่องที่ 2 ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
เรื่องที่ 3 ข้อปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน
เรื่องที่ 4 ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่าย
เรื่องที่ 5 ข้อปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)
เรื่องที่ 6 ข้อปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)
เรื่องที่ 7 ข้อปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
เรื่องที่ 8 ข้อปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)
เรื่องที่ 9 ข้อปฏิบัติในการควบคุมการเข้าถึงของหน่วยงานภายนอก (Outsource Control)
เรื่องที่ 10 ข้อปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศ
เรื่องที่ 11 ข้อปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
เรื่องที่ 12 ข้อปฏิบัติในการใช้งานอินเทอร์เน็ต
เรื่องที่ 13 ข้อปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)
เรื่องที่ 14 ข้อปฏิบัติในการใช้สื่อสังคมออนไลน์ (Social Media)

คำนิยามที่ใช้

(1) ผส. หมายความว่า กรมกิจการผู้สูงอายุ

(2) ผู้ใช้งาน หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้าง และบุคคลอื่นที่ได้รับอนุญาตให้ใช้งานเครือข่ายคอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต หรือ e-Mail ที่กรมกิจการผู้สูงอายุจัดสรรให้

(3) ผู้ดูแลระบบ หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบสารสนเทศ หรือระบบเครือข่าย หรือระบบคอมพิวเตอร์

(4) เจ้าหน้าที่ หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของกรมกิจการผู้สูงอายุ ผู้รับบริการ ผู้ใช้งานทั่วไป

(5) สิทธิ์ของผู้ใช้งาน หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของกรมกิจการผู้สูงอายุ

(6) สินทรัพย์/สินทรัพย์สารสนเทศ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับกรมกิจการผู้สูงอายุ เช่น เอกสาร สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์ เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง ระบบเครือข่าย และระบบสารสนเทศ

(7) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(8) ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

(9) เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนข้อปฏิบัติด้านความมั่นคงปลอดภัย

(10) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของกรมกิจการผู้สูงอายุถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(11) ระบบเครือข่าย หมายความว่า กลุ่มของคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่ายและสื่อนำสัญญาณ ที่ถูกนำมาเชื่อมต่อกันผ่านอุปกรณ์ด้านการสื่อสารหรือสื่ออื่นใด ซึ่งทางผู้ดูแลระบบเป็นผู้กำหนด และทำให้ผู้ใช้ในระบบเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยน และใช้อุปกรณ์หรือทรัพยากรต่าง ๆ ของเครือข่ายร่วมกันได้ โดยเครือข่ายคอมพิวเตอร์จะครอบคลุมทั้งเครือข่ายภายในหรือแลน (Local Area Network : LAN) แลนไร้สายหรือไวเลสแลน (Wireless LAN , WLAN) และเครือข่ายวงกว้างหรือแวน (Wide Area Network : WAN) ของกรมกิจการผู้สูงอายุ ผ่านการใช้บริการเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (DG-Link)

(12) ระบบสารสนเทศ หมายความว่า ระบบที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ Hardware, Software, User, Data และ Procedure ซึ่งทุกองค์ประกอบนี้ทำงานร่วมกัน เพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งาน เพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์ และติดตามผลการดำเนินงานของกรมกิจการผู้สูงอายุ

(13) การใช้งานอินเทอร์เน็ต หมายความว่า การใช้บริการต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ

(14) คอมพิวเตอร์ หมายความว่า คอมพิวเตอร์ที่มีการเชื่อมต่อเพื่อใช้งานเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตที่กรมกิจการผู้สูงอายุ

(15) ข้อมูล หมายความว่า สิ่งที่ป้อนเข้าไปในคอมพิวเตอร์ ไม่ว่าจะเป็นตัวเลข ข้อความ คำสั่ง ชุดคำสั่ง ซอฟต์แวร์ แฟ้มข้อมูล หรือรายละเอียดซึ่งอาจอยู่ในรูปแบบประเภทต่าง ๆ

(16) รหัสผ่าน (Password) หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(17) จดหมายอิเล็กทรอนิกส์ (e-Mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

(18) ชุดคำสั่งไม่พึงประสงค์ หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ทำให้ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(19) หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานที่กรมกิจการผู้สูงอายุอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของกรมกิจการผู้สูงอายุ โดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล หรือหน่วยงานที่กรมกิจการผู้สูงอายุดำเนินการส่งหรือเข้าถึงข้อมูลสารสนเทศ

(20) สื่อสังคมออนไลน์ (Social Media) หมายความว่า ช่องทางหรือสื่อใด ๆ ที่ใช้เผยแพร่ข้อมูลและแสดงความคิดเห็นบนโลกออนไลน์ที่เปิดโอกาสให้ผู้ใช้สามารถสร้างสรรค์เนื้อหาได้ด้วยตนเอง เช่น บล็อคเสรี (Blog) วิกิพีเดีย (Wikipedia) พันทิป (Pantip) เว็บเครือข่ายสังคม (Social Network) ต่าง ๆ รวมถึงวิดีโอและการทำ Live Stream เช่น Facebook, Instagram, LinkedIn, Flickr, Snapchat, Twitter, Vine, YouTube เป็นต้น

(21) โพสต์ (Post) หมายความว่า การส่งข้อความตัวอักษร ภาพ หรือวิดีโอคลิป เข้าสู่สื่อออนไลน์ เช่น เว็บไซต์ เพื่อแสดงความคิดเห็นหรือเผยแพร่ข้อมูลข่าวสาร

เรื่องที่ 1
ข้อปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดบทบาทและความรับผิดชอบของเจ้าหน้าที่ในสังกัดกรมกิจการผู้สูงอายุ ให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและการเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต รวมถึงกรณีที่ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุเกิดความเสียหายหรืออันตรายใด ๆ ต่อหน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. ผู้บริหาร

1.1 อธิบดีกรมกิจการผู้สูงอายุ (Chief Executive Officer : CEO)

1.2 รองอธิบดีกรมกิจการผู้สูงอายุ ที่ได้รับมอบหมายให้เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกรมกิจการผู้สูงอายุ (Department Chief Information Officer : DCIO)

2. ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ดังนี้

2.1 ผู้บังคับบัญชา : ผู้อำนวยการกองยุทธศาสตร์และแผนงาน

2.2 ผู้ดูแลระบบ : เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ในสังกัดกรมกิจการผู้สูงอายุทุกคน

ข้อปฏิบัติ

1. ผู้บริหารมีหน้าที่ความรับผิดชอบ ดังนี้

1.1 อธิบดีกรมกิจการผู้สูงอายุ (Chief Executive Officer : CEO) ให้ความเห็นชอบต่อข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ

1.2 รองอธิบดีกรมกิจการผู้สูงอายุ ที่ได้รับมอบหมายจากอธิบดีกรมกิจการผู้สูงอายุให้เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกรมกิจการผู้สูงอายุ (Department Chief Information Officer : DCIO)

1.2.1 กำหนดให้มีการจัดทำและทบทวนหรือปรับปรุงข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ

1.2.2 กำหนดให้ผู้รับผิดชอบและผู้เกี่ยวข้องมีการดำเนินงานตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ

1.2.3 กำหนดให้มีการตรวจสอบตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐหรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก

1.2.4 กำหนดให้มีการบริหารจัดการทรัพยากรอย่างเพียงพอต่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุในแต่ละปีงบประมาณ

2. ผู้ดูแลระบบมีหน้าที่ความรับผิดชอบ ดังนี้

2.1 ผู้ดูแลระบบ : เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

2.1.1 จัดทำบัญชีสินทรัพย์สารสนเทศของอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย และรายการระบบสารสนเทศให้ถูกต้อง และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.1.2 เก็บรักษาอุปกรณ์บริหารจัดการเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายในพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

2.1.3 ดูแล รักษา และตรวจสอบอุปกรณ์เครือข่าย ช่องทางการสื่อสารของระบบเครือข่าย และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งาน

2.1.4 ดูแล รักษา และตรวจสอบการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ดังนี้

(1) กรณีเกิดจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ ให้รีบแจ้งผู้ใช้งานนั้นยุติการกระทำในทันที

(2) กรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นต่อกรมกิจการผู้สูงอายุ ให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานดังกล่าวทันที

2.1.5 ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย และโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดี ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

2.1.6 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของกรมกิจการผู้สูงอายุ เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้งาน และต้องเก็บรักษาไว้อย่างครบถ้วนถูกต้อง ตามระยะเวลาที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 กำหนด และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย

2.1.7 กำหนดสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของผู้ใช้งานให้สามารถใช้งานได้ตามภารกิจและสิทธิ์ที่ได้รับ

2.1.8 ทบทวนและปรับปรุงบัญชีผู้ใช้งานตามสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

2.1.9 ควบคุมและตรวจสอบการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของผู้ใช้งานให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

2.1.10 ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานโดยไม่มีเหตุผลอันสมควร

2.1.11 ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

2.1.12 ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งาน หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

2.1.13 คืนสินทรัพย์สารสนเทศที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนโดยทันทีที่พ้นจากหน้าที่ให้กับผู้อำนวยการกองยุทธศาสตร์และแผนงานหรือผู้ที่ได้รับมอบหมาย เพื่อตรวจสอบการคืนสินทรัพย์สารสนเทศนั้น

3. ผู้ใช้งานมีหน้าที่ความรับผิดชอบ ดังนี้

เป็นผู้เข้าถึงและใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่าย และระบบสารสนเทศของกรมกิจการผู้สูงอายุตามสิทธิ์ที่ได้รับอนุญาต โดยต้องปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุอย่างเคร่งครัด ดังนี้

3.1 ผู้ใช้งานต้องปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุอย่างเคร่งครัดโดยไม่มีเงื่อนไข และจะอ้างว่าไม่ทราบข้อปฏิบัติฯ ดังกล่าวมิได้

3.2 ห้ามผู้ใช้งานกระทำการใด ๆ อันละเมิดหรือขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้อง หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานต้องรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรมกิจการผู้สูงอายุ

3.3 ผู้ใช้งานต้องรักษาบัญชีผู้ใช้งาน (Account) ของตนเองไว้เป็นความลับเฉพาะตัว และไม่อนุญาตให้ผู้อื่นเข้าถึงระบบด้วย Account ของตนเองในทุกกรณี เพื่อป้องกันการใช้งานโดยมิชอบ

3.4 ผู้ใช้งานต้องเป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้งานและการอนุญาตให้ผู้อื่นเข้าถึงระบบด้วย Account ในนามของตนเองโดยไม่สามารถปฏิเสธความผิดนั้นได้ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

3.5 ผู้ดูแลระบบมีสิทธิ์ระงับ เพิกถอน หรือกระทำการใด ๆ ต่อการใช้งานระบบของผู้ใช้งานเพื่อความมั่นคงปลอดภัยของระบบโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

3.6 ผู้ใช้งานต้องปกปิดข้อมูลส่วนบุคคล เช่น เลขบัตรประจำตัวประชาชน ชื่อ นามสกุล ที่อยู่ และการยกตัวอย่างในแบบฟอร์มต่าง ๆ เพื่อเป็นการคุ้มครองสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล รวมทั้งการให้ข้อมูลส่วนบุคคลต้องปกปิดด้วยเครื่องหมาย “x” จำนวน 5 ตัว ด้านหน้าหรือด้านหลังข้อมูล เพื่อให้มั่นใจว่าเอกสารที่จะเผยแพร่ต่อสาธารณะจะไม่ละเมิดสิทธิส่วนบุคคลของผู้เกี่ยวข้อง

3.7 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

3.7.1 ควรป้องกันไม่ให้ผู้อื่นเข้าใช้ระบบงาน/เครื่องคอมพิวเตอร์/เครื่องโน้ตบุ๊กของตนโดยให้ใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งาน

3.7.2 ควรตั้งค่าให้มีการล็อก (Lock) หน้าจอของอุปกรณ์โดยอัตโนมัติเมื่อไม่ได้ใช้งานนานเกินกว่า 15 นาที

3.7.3 ควรออกจากระบบงาน/เครื่องคอมพิวเตอร์/เครื่องโน้ตบุ๊กที่ใช้งานโดยทันทีเมื่อเสร็จสิ้นงาน

3.7.4 ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือไม่มีการใช้งานนานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องแม่ข่ายที่ให้บริการ

3.8 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

3.8.1 รับผิดชอบต่อสินทรัพย์ที่กรมกิจการผู้สูงอายุมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของตนเอง โดยต้องบันทึกรายการสินทรัพย์ที่ผู้ใช้งานรับผิดชอบ และตรวจสอบทุกครั้งเมื่อมีการรับหรือคืนสินทรัพย์โดยเจ้าหน้าที่ที่ได้รับมอบหมายของหน่วยงาน

3.8.2 มีสิทธิ์ใช้สินทรัพย์ที่กรมกิจการผู้สูงอายุจัดเตรียมไว้ให้เพื่อการใช้งานเท่านั้น ห้ามนำไปใช้ในกิจกรรมที่กรมกิจการผู้สูงอายุไม่ได้กำหนด โดยหากเกิดความเสียหายต่อหน่วยงานจากการละเมิดดังกล่าวให้ถือว่าเป็นความผิดส่วนบุคคล และผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นนั้น

3.8.3 หากสินทรัพย์เกิดการชำรุดหรือสูญหายจากความประมาทของผู้ใช้งาน ผู้ใช้งานต้องชดใช้ค่าเสียหายตามมูลค่าสินทรัพย์นั้น

3.8.4 กรณีที่ต้องทำงานนอกสถานที่ ผู้ใช้งานจะต้องดูแลและรับผิดชอบต่อสินทรัพย์ของกรมกิจการผู้สูงอายุที่อยู่ในความรับผิดชอบเป็นอย่างดี

3.8.5 ห้ามให้ผู้อื่นยืมสินทรัพย์ไม่ว่ากรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

3.8.6 ห้ามติดตั้งซอฟต์แวร์คอมพิวเตอร์ใด ๆ ลงบนเครื่องคอมพิวเตอร์ นอกเหนือจากที่กรมกิจการผู้สูงอายุอนุญาต หากจำเป็นต้องติดตั้งซอฟต์แวร์จะต้องแจ้งให้ผู้ดูแลระบบดำเนินการ

3.8.7 ไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์ก่อนได้รับอนุญาต และต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใด ๆ

3.8.8 หากจะนำอุปกรณ์สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์/USB ไปให้ผู้อื่นใช้งานต่อ จะต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อน โดยใช้วิธีการลบหรือการเขียนทับข้อมูลเดิมหลายรอบ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

3.8.9 หากจำเป็นต้องทำลายอุปกรณ์สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์ ให้ดำเนินการตามมาตรการดังนี้

มาตรการการทำลายข้อมูลและสื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์	
ประเภท	วิธีการทำลาย
กระดาษ	ใช้วิธีการย่อยทำลายด้วยเครื่องทำลายเอกสาร
แผ่น CD/DVD	ใช้วิธีการย่อยทำลายด้วยเครื่องทำลายเอกสาร
เทป DDS , DAT, LTO	1. ทำการลบข้อมูลทั้งม้วนเทป (Erase) ผ่าน Tape Device ก่อนการทำลายม้วนเทป 2. ทำลายด้วยวิธีการทุบหรือบดให้เสียหาย
ฮาร์ดดิสก์ (Hard Disk) หรือ Memory Devices เช่น USB flash drive , SD cards	1. ทำลายข้อมูลโดยใช้เทคโนโลยีซอฟต์แวร์ Wiping ที่สอดคล้องกับมาตรฐาน DoD 5220-22M ของกระทรวงกลาโหมสหรัฐอเมริกาว่าด้วยการลบข้อมูลในฮาร์ดดิสก์ ดังนี้ • ใช้ซอฟต์แวร์ Disk Wipe (http://www.diskwipe.org) ในการทำลายข้อมูลทั้ง Hard Disk หรือ Memory Devices โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://www.diskwipe.org/download.php • ใช้ซอฟต์แวร์ Eraser (http://eraser.heidi.ie) ในการลบแฟ้มข้อมูล/ไฟล์ข้อมูล โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://eraser.heidi.ie/download.php 2. ทำลายด้วยวิธีการทุบหรือบดให้เสียหาย
USB	จำกัดหรือห้ามการใช้ USB ที่ไม่ได้รับการอนุญาตการใช้ USB ต้องปฏิบัติตามมาตราฐานการรักษาความปลอดภัยที่ได้รับการกำหนด และจะต้องมีการตรวจสอบและควบคุมเพื่อรักษาความปลอดภัยของระบบและข้อมูลอย่างสม่ำเสมอ

3.8.10 มีส่วนร่วมในการบำรุงรักษาโปรแกรมป้องกันไวรัสที่ใช้ โดยตรวจสอบว่ามีการ Update โปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถ Update โปรแกรมป้องกันไวรัสให้ทันสมัยได้

3.8.11 สำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้ เช่น Flash Drive Memory Card ฮาร์ดดิสก์แบบพกพา หรือบนคลาวด์ เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

3.8.12 ไม่ปรับแต่งหรือยกเลิกการทำงานของโปรแกรมป้องกันไวรัสที่ผู้ดูแลระบบติดตั้งให้

3.8.13 แจ้งให้ผู้ดูแลระบบทราบทันทีเมื่อพบว่าคอมพิวเตอร์หรือโปรแกรมที่ใช้มีความผิดปกติหรือเมื่อสงสัยว่ามีการติดไวรัส

3.8.14 ตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นด้วยโปรแกรมป้องกันไวรัสทุกครั้งเมื่อมีการนำมาติดตั้งหรือใช้งาน และหากตรวจพบไวรัสจะต้องจัดการทำลายไวรัสโดยเร็วที่สุด

3.8.15 หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมที่นำมาใช้งานได้ ห้ามผู้ใช้งานทำการเปิดข้อมูลหรือติดตั้งโปรแกรมลงไปบนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เด็ดขาด

3.8.16 หากต้องการนำเครื่องคอมพิวเตอร์มาใช้งานภายใต้ระบบเครือข่ายของกรมกิจการผู้สูงอายุ จะต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องคอมพิวเตอร์ก่อน โดยซอฟต์แวร์นั้นต้องสามารถ Update ให้เป็นปัจจุบัน และตรวจจับ Malware อื่น ๆ ได้ เช่น Spyware หากไม่มีต้องแจ้งให้ผู้ดูแลระบบติดตั้งให้

3.8.17 การใช้งานระบบเครือข่ายของกรมกิจการผู้สูงอายุ ผู้ใช้งานจะต้องลงทะเบียนเพื่อขอใช้งานจากผู้ดูแลระบบก่อน โดยผู้ที่ได้รับสิทธิ์ให้เข้าใช้งานได้จะได้รับบัญชีผู้ใช้งาน (Account) ซึ่งประกอบด้วยรหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

3.8.18 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ก่อนเข้าใช้งานระบบเครือข่ายของกรมกิจการผู้สูงอายุทุกครั้ง ด้วยบัญชีผู้ใช้งาน (Account) ของตนเองเท่านั้น

3.8.19 ห้ามเข้าห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ ซึ่งเป็นพื้นที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์บริหารจัดการเครือข่ายโดยเด็ดขาด เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

3.8.20 ไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

3.8.21 ไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้ากับระบบเครือข่ายของกรมกิจการผู้สูงอายุเพื่อเปิดใช้งานเองในหน่วยงาน หรือประกอบธุรกิจส่วนบุคคล

3.8.22 กรณีที่ผู้ใช้งานพยายามเข้าถึงระบบโดยมิชอบ หรือโจมตีระบบ หรือมีพฤติกรรมการใช้งานที่ละเมิดต่อข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุหรือกฎหมายที่เกี่ยวข้อง ผู้ใช้งานนั้นจะถูกระงับหรือยกเลิกการใช้งานระบบเครือข่ายของกรมกิจการผู้สูงอายุทันที

3.8.23 กรณีที่ผู้ใช้งานได้กระทำการใด ๆ ที่มีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้อง หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อหน่วยงานหรือผู้หนึ่งผู้ใด ผู้ใช้งานนั้นจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

3.9 นำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ

3.9.1 ประเมินข้อมูลที่จำเป็นต้องป้องกัน โดยพิจารณาตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 เพื่อระบุระดับความสำคัญและระดับความลับที่เหมาะสม

3.9.2 เลือกวิธีการเข้ารหัสที่เป็นมาตรฐานสากลมาใช้กับข้อมูลที่จำเป็นต้องป้องกัน

3.9.3 การจัดเก็บรหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ของระบบสารสนเทศลงในฐานข้อมูลตามที่ผู้ดูแลระบบกำหนด

3.9.4 การเชื่อมต่อระบบสารสนเทศแบบ Web Application เพื่อส่งข้อมูลระหว่างเบราว์เซอร์และเว็บเซิร์ฟเวอร์ จะต้องเชื่อมต่อโดยการเข้ารหัส (SSL) ผ่านโปรโตคอล HTTPS

3.9.5 กำหนดช่องทางที่เหมาะสมในการรับ – ส่งข้อมูลสำคัญหรือข้อมูลลับ ดังนี้

(1) ระบบเครือข่ายแบบ LAN

(2) ระบบเครือข่ายแบบไร้สาย หรือ Wireless LAN

(3) สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์ที่สามารถถอดแยกจากตัวเครื่องคอมพิวเตอร์ได้

3.9.6 กำหนดวิธีการบริหารจัดการและการใช้งานกุญแจสำหรับการเข้ารหัส ดังนี้

(1) กำหนดผู้รับผิดชอบเพื่อทำหน้าที่เกี่ยวกับการเข้ารหัส เช่น การสร้างกุญแจ การควบคุมและดูแลกุญแจ การทำลายกุญแจ การใช้งานกุญแจ และการจัดการกรณีกุญแจเกิดการสูญหาย

(2) กำหนดวิธีการป้องกันกุญแจที่ใช้สำหรับการเข้ารหัส

(3) กำหนดวิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจเกิดการสูญหายหรือถูกทำให้เสียหาย

3.9.7 ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับหรือวิธีการรักษาความลับของข้อมูลดังนี้

(1) แสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

(2) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ ด้วยวิธีการเข้ารหัสตามมาตรฐานที่กรมกิจการผู้สูงอายุกำหนด

(3) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ด้วยการกำหนดรหัสผ่านให้กับไฟล์ข้อมูลลับนั้น

3.9.8 ห้ามแชร์ไฟล์ข้อมูลลับบนระบบเครือข่ายของกรมกิจการผู้สูงอายุเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

3.9.9 สำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

เรื่องที่ 2
ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

เพื่อเป็นมาตรการในการควบคุม ป้องกัน และรักษาความมั่นคงปลอดภัยเกี่ยวกับสถานที่ที่เป็นที่ตั้งและพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ปฏิบัติที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมายหรือที่มีสิทธิ์ในการเข้าออกพื้นที่

3. ผู้มาติดต่อ หมายถึง เจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มาติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ภายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ มีหน้าที่ความรับผิดชอบดังนี้

1.1 กำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

1.1.1 กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุให้ชัดเจน โดยสามารถแบ่งแยกได้เป็นพื้นที่ห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ พื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) และพื้นที่ติดตั้งอุปกรณ์กระจายสัญญาณเครือข่าย (Access Network Area) เป็นต้น

1.1.2 จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุและประกาศให้รับทราบโดยทั่วกัน

1.2 ควบคุมสินทรัพย์สารสนเทศ

1.2.1 พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

(1) มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ

(2) ผนังล้อมรอบศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุควรสร้างเป็นผนังทึบ

(3) ประตูหรือทางเข้าพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุต้องออกแบบเพื่อป้องกันการบุกรุกทางกายภาพ

(4) ประตูหรือทางเข้าของห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุต้องมีระบบที่สามารถล็อกได้เพื่อป้องกันการบุกรุกทางกายภาพ

(5) ให้เจ้าหน้าที่ที่ปฏิบัติงานภายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ ต้องปิดประตูและหน้าต่างให้ล็อกอยู่เสมอภายหลังเลิกงานและนอกเวลาราชการ

1.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน

(1) ติดตั้งระบบและอุปกรณ์สนับสนุนการทำงานที่เพียงพอต่อความต้องการใช้งานภายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ เช่น ระบบปรับอากาศ ระบบควบคุมอุณหภูมิและความชื้น ระบบไฟฟ้าสำรอง ระบบดับเพลิง ระบบควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control) หรืออุปกรณ์ที่สามารถป้องกันภัยคุกคามจากผู้บุกรุก และกล้องวงจรปิด (CCTV) เป็นต้น

(2) มีการใช้ระบบไฟฟ้าสำรองกับระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้า และต้องทดสอบระบบไฟฟ้าสำรองอย่างสม่ำเสมอ

(3) มีการตรวจสอบหรือทดสอบระบบและอุปกรณ์สนับสนุนการทำงานอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานได้ตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(4) มีการดูแลและบำรุงรักษาระบบและอุปกรณ์สนับสนุนการทำงานอย่างถูกต้องและสม่ำเสมอ โดยจัดให้มีการบำรุงรักษาอุปกรณ์อย่างน้อยปีละ 1 ครั้ง

1.2.3 การป้องกันอุปกรณ์

(1) แยกเก็บอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่งเพื่อดูแลความมั่นคงปลอดภัย

(2) มีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอนหรือไฟฟ้ากระชาก

(3) มีการตรวจสอบ สอดส่องระดับอุณหภูมิ และดูแลสภาพแวดล้อมภายในบริเวณพื้นที่ห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ เพื่อป้องกันความเสียหายต่ออุปกรณ์

(4) ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ภายในบริเวณพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ

(5) มีการกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศทุกครั้งเมื่อว่างเว้นจากการใช้งาน

2. เจ้าหน้าที่มีหน้าที่ความรับผิดชอบ ดังนี้

2.1 ควบคุมการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ

2.1.1 จัดทำคู่มือ/คำแนะนำ/วิธีปฏิบัติในการเข้าออกพื้นที่ และต้องประกาศให้รับทราบโดยทั่วกัน

2.1.2 จัดให้มีระบบจัดเก็บบันทึกการเข้าออกพื้นที่

2.1.3 จัดทำแบบบันทึกการเข้าออกพื้นที่ โดยต้องระบุรายละเอียดอย่างน้อยดังนี้ ชื่อ - นามสกุล ตำแหน่ง หน่วยงาน ประเภทสิทธิ์ เครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับสิทธิ์ รายละเอียดกิจกรรม และระยะเวลาดำเนินการ

2.1.4 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้มาติดต่อมีความจำเป็นต้องเข้าออกพื้นที่ หรือมิได้ขอสิทธิ์ในการเข้าออกพื้นที่ไว้ล่วงหน้า เจ้าหน้าที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนอนุญาต และจดบันทึกการเข้าออกพื้นที่ไว้เป็นหลักฐานทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่ โดยเจ้าหน้าที่จะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลาและต้องควบคุมอย่างเข้มงวด

2.1.5 กำกับและดูแลให้ผู้มาติดต่อปฏิบัติตามคู่มือ/คำแนะนำ/วิธีปฏิบัติในการเข้าออกพื้นที่อย่างเคร่งครัด

2.1.6 ตรวจสอบแบบบันทึกการเข้าออกพื้นที่เป็นประจำทุกวันหรือทุกครั้งที่มีการเข้าออก

2.2 กำหนดสิทธิ์การเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ

2.2.1 จัดทำแบบคำขอเข้าใช้งานห้อง Data Center หรือศูนย์ปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ

2.2.2 กำหนดสิทธิ์/ปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ทุกครั้งที่มีการเปลี่ยนแปลง และต้องทบทวนสิทธิ์อย่างน้อยปีละ 1 ครั้ง

2.2.3 จัดทำทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่

3. ผู้มาติดต่อมีหน้าที่ความรับผิดชอบ ดังนี้

3.1 การเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ

3.1.1 กรอกแบบคำขอเข้าใช้งานห้อง Data Center หรือศูนย์ปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ ก่อนได้รับอนุญาตเข้าพื้นที่

3.1.2 กรณีที่ต้องการนำอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายเข้ามาภายในบริเวณพื้นที่ จะต้องบันทึกรายการอุปกรณ์ที่นำเข้ามาลงในแบบบันทึกการเข้าออกพื้นที่ให้ถูกต้อง

3.1.3 ปฏิบัติตามคู่มือ/คำแนะนำ/วิธีปฏิบัติในการเข้าออกพื้นที่อย่างเคร่งครัด

3.2 การเข้าออกพื้นที่ห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ

3.2.1 ขออนุญาตเข้าออกพื้นที่ล่วงหน้าก่อนวันที่จะเข้าพื้นที่ โดยต้องกรอกแบบคำขอเข้าใช้งานห้อง Data Center หรือศูนย์ปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ

3.2.2 ต้องได้รับอนุมัติสิทธิ์ในการเข้าออกพื้นที่จากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ/ผู้แทนที่ได้รับมอบหมายก่อนเข้าพื้นที่

เรื่องที่ 3
ข้อปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน

วัตถุประสงค์

เพื่อให้เจ้าหน้าที่ใช้เป็นมาตรการในการควบคุมและบริหารจัดการการเข้าถึงของผู้ใช้งาน โดยอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุเท่านั้น

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน

1.1 เสริมเนื้อหาเพื่อสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเข้ากับหลักสูตรฝึกอบรมต่าง ๆ ตามแผนการฝึกอบรมของกรมกิจการผู้สูงอายุ

1.2 เผยแพร่ประชาสัมพันธ์และให้ความรู้ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ ในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยให้มีการปรับเปลี่ยนเกร็ดความรู้ให้ทันสมัยอยู่เสมอ

2. การลงทะเบียนผู้ใช้งาน (User Registration)

2.1 จัดเตรียมแบบฟอร์มลงทะเบียนผู้ใช้งานในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

2.2 ตรวจสอบและให้สิทธิ์ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุที่เหมาะสมต่อหน้าที่ความรับผิดชอบของผู้ใช้งาน

2.3 ระงับหรือเพิกถอนสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุโดยทันที เมื่อผู้ใช้งานนั้นเปลี่ยนแปลงหน้าที่ความรับผิดชอบหรือลาออก

3. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

3.1 การแจ้งขอเปลี่ยนแปลงสิทธิ์ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ จะต้องจัดทำเป็นลายลักษณ์อักษรและระบุเหตุผลความจำเป็น

3.2 กำหนดสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุเฉพาะการปฏิบัติงานในหน้าที่เท่านั้น โดยต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

3.3 กำหนดระดับสิทธิ์ที่เหมาะสมในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

3.4 พิจารณามอบหมายสิทธิ์ให้สอดคล้องตามข้อปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ

3.5 ผู้ใช้งานต้องรับทราบสิทธิ์และปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุอย่างเคร่งครัด

3.6 หากตรวจพบว่าผู้ใช้งานมีการกระทำความผิดหรือละเมิดต่อข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ เจ้าหน้าที่ต้องทำการระงับหรือเพิกถอนสิทธิ์ของผู้ใช้งานนั้นทันที

3.7 เมื่อผู้ใช้งานมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ เจ้าหน้าที่ต้องทำการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งานนั้นทันที

3.8 การเพิกถอนสิทธิ์ของผู้ใช้งานออกจากระบบ

3.8.1 กรณีเป็นเจ้าหน้าที่ของกรมกิจการผู้สูงอายุ ให้เพิกถอนเมื่อผู้ใช้งานนั้นมีการเปลี่ยนแปลงตำแหน่งหน้าที่ความรับผิดชอบ หรือลาออก หรือพ้นสภาพจากการเป็นเจ้าหน้าที่ของกรมกิจการผู้สูงอายุ เมื่อได้รับแจ้งจากส่วนที่เกี่ยวข้องโดยทันที

3.8.2 กรณีเป็นบุคคลจากหน่วยงานภายนอก ให้เพิกถอนตามวันที่ระบุในแบบฟอร์มลงทะเบียนผู้ใช้งานหรือเมื่อเสร็จสิ้นภารกิจโดยทันที

4. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

4.1 กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านให้มีความยากต่อการคาดเดาโดยผู้อื่น

4.2 การใช้งานรหัสผ่าน (Password Use)

4.2.1 ควรตั้งรหัสผ่านโดยมีความยาวอย่างน้อย 12 ตัวอักษร

4.2.2 ควรตั้งรหัสผ่านที่ประกอบด้วยตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ

4.2.3 ควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น 123, abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น 111, aaa เป็นต้น

4.2.4 ควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

4.2.5 ควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

4.2.6 ไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

4.2.7 ควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีในครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบ

4.2.8 ควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

4.2.9 ควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดหรืออย่างน้อยทุก ๆ 3 เดือน

4.2.10 ควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

4.2.11 ไม่ควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่ผู้อื่นมองเห็นได้ง่าย

4.2.12 ไม่เปิดเผยรหัสผ่านของตนเองกับผู้อื่น

4.2.13 ไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

4.2.14 ไม่ควรกำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง

4.2.15 ควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ใช้งาน

4.3 ส่งมอบรหัสผ่านให้กับผู้ใช้งานด้วยวิธีที่มีความมั่นคงปลอดภัย เช่น ในรูปแบบไฟล์เข้ารหัสไปรษณีย์อิเล็กทรอนิกส์ภาครัฐที่เข้ารหัสลับเฉพาะ เป็นต้น

4.4 กำหนดขั้นตอนปฏิบัติในการบริหารจัดการรหัสผ่านของผู้ใช้งานที่มีความมั่นคงปลอดภัย ดังนี้

4.4.1 ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

4.4.2 ผู้ใช้งานควรเปลี่ยนรหัสผ่านทุก ๆ 6 เดือน หรือตามที่ผู้ดูแลระบบกำหนด

4.4.3 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานแฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านระบบเครือข่ายคอมพิวเตอร์

5. การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

5.1 ทบทวนสิทธิ์และปรับปรุงบัญชีผู้ใช้งานในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงใด ๆ เช่น การเปลี่ยนแปลงตำแหน่ง ย้ายหน่วยงาน ลาออก หรือสิ้นสุดการจ้างงาน

5.2 ตรวจสอบและติดตามการใช้งานของผู้ใช้งานตามสิทธิ์ที่ได้รับในแต่ละระบบอย่างสม่ำเสมอ

เรื่องที่ 4
ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่าย

วัตถุประสงค์

เพื่อเป็นมาตรการในการติดตั้งและกำหนดค่าต่าง ๆ ของระบบเครือข่ายและอุปกรณ์เครือข่าย ได้แก่ ไฟร์วอลล์ (Firewall) ระบบตรวจจับและป้องกันการบุกรุก (IDPS) การป้องกันมัลแวร์และไวรัส (Anti-Malware/ Anti-Virus) และระบบเครือข่ายไร้สาย (Wireless LAN) โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ปฏิบัติที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเครือข่ายของกรมกิจการผู้สูงอายุ

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเครือข่ายของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. ผู้ดูแลระบบมีหน้าที่ความรับผิดชอบ ดังนี้

1.1 การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

1.1.1 ติดตั้ง กำหนดค่า และบริหารจัดการไฟร์วอลล์ เพื่อกำหนดค่าต่าง ๆ ให้เหมาะสมตามความต้องการในการปฏิบัติงาน และสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายภายในของกรมกิจการผู้สูงอายุ

1.1.2 ผู้ดูแลระบบหรือบริษัทที่บำรุงรักษาที่ได้รับมอบหมายเท่านั้นจึงจะสามารถเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ได้

1.1.3 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

1.1.4 ทุกเส้นทางที่เชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาต จะต้องถูกปฏิเสธโดยไฟร์วอลล์

1.1.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

1.1.6 สำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นทุกครั้งที่มีการเปลี่ยนแปลงค่า

1.1.7 ระบบเครื่องคอมพิวเตอร์แม่ข่ายสารสนเทศที่เข้าถึงบริการได้จากทั้งภายในและภายนอกทั้งหมด ต้องถูกติดตั้งใน Demilitarized Zone (DMZ) และต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

1.1.8 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่ออินเทอร์เน็ตโดยทั่วไปที่ไม่มีการป้องกัน

1.1.9 ให้บริการเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายโดยอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น และจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

1.1.10 ให้บริการเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์บนเครือข่ายตามที่ได้รับอนุมัติจากเจ้าหน้าที่/ผู้ดูแลระบบ โดยต้องแจ้งข้อมูลดังนี้

(1) หมายเลข Port ที่ต้องการขอให้เปิด

(2) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

(3) วัตถุประสงค์หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้น ๆ

(4) วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

(5) ผู้ดูแล/ผู้รับผิดชอบ/ผู้พัฒนาระบบ

1.1.11 ให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย โดยเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่ทางเจ้าหน้าที่/ผู้ดูแลระบบอนุญาตให้ใช้งานเท่านั้น หากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือจากที่กำหนด จะต้องได้รับการอนุมัติเจ้าหน้าที่/ผู้ดูแลระบบก่อน

1.1.12 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอก มายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายในของกรมกิจการผู้สูงอายุ จะต้องดำเนินการผ่าน VPN เท่านั้น และต้องได้รับการอนุมัติจากเจ้าหน้าที่/ผู้ดูแลระบบก่อน และต้องบันทึกรายการที่ได้ดำเนินการตามที่ขอไว้ด้วย

1.1.13 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยเป็นไปตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

1.1.14 ระงับการใช้งานระบบเครือข่ายและอินเทอร์เน็ตของกรมกิจการผู้สูงอายุของเครื่องคอมพิวเตอร์ลูกข่ายทันที หากพบว่ามีพฤติกรรมการใช้งานที่ขัดต่อประกาศหรือข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของกรมกิจการผู้สูงอายุ หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุจนกว่าจะได้รับการแก้ไข

1.1.15 ยกเลิกการให้บริการระบบเครือข่ายและอินเทอร์เน็ตของกรมกิจการผู้สูงอายุของผู้ใช้งานทันที หากพบว่าผู้ใช้งานมีเจตนาใช้งานที่ขัดต่อประกาศหรือข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของกรมกิจการผู้สูงอายุ หรือกฎหมาย หรือการทำงานของโปรแกรมที่อาจทำให้เกิดความเสี่ยงต่อความปลอดภัยหรือทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ

1.2 การรักษาความมั่นคงปลอดภัยของระบบตรวจจับและป้องกันการบุกรุก (IDPS Policy)

1.2.1 ติดตั้ง กำหนดค่า และบริหารจัดการระบบตรวจจับและป้องกันการบุกรุก เพื่อตรวจสอบความปลอดภัยของระบบเครือข่าย และป้องกันทรัพยากรระบบสารสนเทศและข้อมูลบนระบบเครือข่ายภายในของกรมกิจการผู้สูงอายุ ให้มีความมั่นคงปลอดภัย

1.2.2 ตรวจสอบและ Update Patch/Signature ของ IDPS เป็นประจำ

1.2.3 ตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายที่มีการติดตั้ง host-based IDPS เป็นประจำทุกวัน

1.2.4 ตรวจสอบเหตุการณ์ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลที่มีการเข้าใช้งานระบบเครือข่ายเป็นประจำ

1.2.5 บันทึกผลการตรวจสอบโฮสต์และระบบเครือข่ายทั้งหมดที่มีการส่งข้อมูลผ่าน IDPS

1.2.6 การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

1.2.7 ทำการลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ เพื่อลดความเสียหายและป้องกันเหตุการณ์ที่อาจเกิดขึ้นอีกในอนาคต

1.2.8 จัดทำรายงานแสดงผลการตรวจสอบการบุกรุกเป็นประจำ

1.2.9 IDPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงระบบเครือข่ายของระบบสารสนเทศตามปกติ

1.2.10 IDPS Policy จะต้องครอบคลุมทุกโฮสต์ในระบบเครือข่ายและระบบเครือข่ายข้อมูลของกรมกิจการผู้สูงอายุทั้งหมด รวมถึงเส้นทางซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทางที่ข้อมูลอาจเดินทาง

1.2.11 ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะ จะต้องผ่านการตรวจสอบจาก IDPS

1.2.12 หากตรวจพบว่าระบบมีการทำงานผิดปกติ จะต้องรายงานให้ผู้ดูแลระบบทราบทันทีที่ตรวจพบ

1.2.13 หากตรวจพบว่ามีพฤติกรรมการใช้งาน หรือกิจกรรม หรือเหตุการณ์ที่น่าสงสัย ซึ่งมีความเสี่ยงต่อการบุกรุกและการโจมตีระบบ หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องรายงานให้ผู้ดูแลระบบทราบทันทีที่ตรวจพบ

1.2.14 ยกเลิกการเชื่อมต่อระบบเครือข่ายของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า

1.3 การป้องกันมัลแวร์และไวรัส (Anti-Malware/Anti-Virus Policy)

1.3.1 จัดหาโปรแกรมบริหารจัดการระบบป้องกันไวรัสจากส่วนกลาง และโปรแกรมป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย

1.3.2 ติดตั้ง กำหนดค่า และบริหารจัดการโปรแกรมป้องกันไวรัสที่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย เพื่อป้องกันไม่ให้เกิดความเสียหายต่อข้อมูลในเครื่องคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ โดยโปรแกรมป้องกันไวรัสต้องมีคุณสมบัติตรวจจับและป้องกันไวรัส เวิร์ม โทรจัน สปายแวร์ได้เป็นอย่างน้อย

1.3.3 ปรับปรุงระบบฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอ เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์เสียหายจากไวรัสคอมพิวเตอร์

1.3.4 หากตรวจพบหรือมีปัญหาจากไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย จะต้องตัดการเชื่อมต่อกับระบบเครือข่ายทันที และดำเนินการตรวจสอบและแก้ไขปัญหาให้แล้วเสร็จ

1.3.5 จัดทำรายงานแสดงผลการป้องกันไวรัสของระบบคอมพิวเตอร์ของกรมกิจการผู้สูงอายุเป็นประจำ

1.4 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย (Wireless LAN Policy)

1.4.1 ติดตั้ง กำหนดค่า และบริหารจัดการระบบเครือข่ายไร้สาย เพื่อควบคุมการเข้าถึงและสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สายของกรมกิจการผู้สูงอายุ และได้รับการอนุญาตจากผู้ดูแลระบบทุกครั้ง

1.4.2 ผู้ดูแลระบบ/บริษัทที่บำรุงรักษาที่ได้รับมอบหมายเท่านั้น จึงจะสามารถเข้าถึงฟังก์ชันที่ใช้ในการตั้งค่าของจุดเชื่อมต่อระบบเครือข่ายไร้สายได้

1.4.3 จุดเชื่อมต่อระบบเครือข่ายไร้สาย จะต้องมีการกำหนดค่า Gateway ที่เป็นค่าที่กำหนดไว้ของระบบเครือข่ายส่วนนั้นเท่านั้น

1.4.4 ทุกจุดเชื่อมต่อระบบเครือข่ายไร้สายและอุปกรณ์ที่เกี่ยวข้อง เช่น Access Point จุดเชื่อมต่อสายสัญญาณ Switch จะต้องมีความปลอดภัย และมีรูปแบบในการจัดเก็บและเข้าถึงอุปกรณ์

1.4.5 SSID (Service Set Identifier) ที่กำหนดจะต้องถูกต้องตามรูปแบบที่ผู้ดูแลระบบกำหนดไว้ และจะต้องไม่มีการบ่งบอกหรือแสดงตำแหน่งของสายที่จุดเชื่อม LAN หรือชื่ออื่น ๆ

1.4.6 เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

1.4.7 SSID ที่ Broadcast จะให้บริการเฉพาะระบบเครือข่ายภายนอก ยกเว้นจุดที่ผู้ดูแลระบบอนุญาตให้ใช้ระบบเครือข่ายภายในของกรมกิจการผู้สูงอายุ จะต้องยกเลิกค่าการ Broadcast SSID

1.4.8 อุปกรณ์ที่ผู้ดูแลระบบอนุญาตให้ใช้ระบบเครือข่ายภายในของกรมกิจการผู้สูงอายุ จะต้องระบุ SSID ที่ถูกต้องจึงจะสามารถเข้าใช้งานได้

1.4.9 SNMP จะต้องถูกยกเลิกหากไม่จำเป็นสำหรับการบริหารจัดการระบบเครือข่าย หรือหากมีความจำเป็นต้องใช้จะต้องมีการเปลี่ยนแปลงค่าเริ่มต้น (Default) ของ Community String

1.4.10 กำหนดให้มีการ Authentication ทุกครั้งก่อนการใช้งาน ด้วยรหัสผู้ใช้ (User account) และรหัสผ่าน (User password)

1.4.11 กำหนดรายการ MAC Address ให้สามารถเข้าใช้ Access Point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามรหัสผู้ใช้ (User account) และรหัสผ่าน (User password) ที่กำหนดไว้เท่านั้น

1.4.12 ยกเลิกการเชื่อมต่อระบบเครือข่ายไร้สายของอุปกรณ์ทุกชนิดที่ไม่เป็นไปตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของกรมกิจการผู้สูงอายุ หรือมีความเสี่ยงต่อระบบโดยไม่ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า

1.4.13 ห้ามไม่ให้ผู้ดูแลระบบบอกค่าติดตั้งของระบบเครือข่ายไร้สายกับผู้ใช้งานหรือบุคคลภายนอก

1.4.14 ระบบเครือข่ายไร้สายสำหรับให้บริการระบบอินเทอร์เน็ต จะต้องติดตั้งโดยแยกระบบเครือข่ายไร้สายออกจากระบบเครือข่ายภายใน LAN เพื่อป้องกันการเข้าถึงจากบุคคลภายนอก

1.4.15 หากจำเป็นต้องเชื่อมต่อระบบเครือข่ายไร้สายกับระบบเครือข่ายภายใน LAN จะต้องเลือกใช้เทคโนโลยี Authentication และมีการกำหนดค่าการเข้ารหัสในการเชื่อมต่อแบบ WPA2 เป็นอย่างน้อย

1.4.16 อุปกรณ์ที่ใช้ในการเข้าถึงระบบเครือข่ายของกรมกิจการผู้สูงอายุ จะต้องรองรับมาตรฐาน IEEE 802.11g/n เป็นอย่างน้อย หากอุปกรณ์ที่ใช้เป็นเครื่องคอมพิวเตอร์ส่วนบุคคลจะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องด้วย

1.4.17 ตรวจสอบอุปกรณ์ติดตั้งการกำหนดค่าและจัดการจุดเชื่อมต่อระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

1.4.18 Wireless LAN Policy สามารถเปลี่ยนแปลงตามเทคโนโลยีใหม่ ๆ และกระบวนการที่สอดคล้องและเหมาะสมในอนาคตได้

2. ผู้ใช้งานมีหน้าที่ความรับผิดชอบ ดังนี้

2.1 ก่อนการใช้งานระบบเครือข่ายและอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ ผู้ใช้งานต้องมีการ Authentication ทุกครั้ง ด้วยรหัสผู้ใช้ (User account) และรหัสผ่าน (User password)

2.2 สำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้ เช่น บน Flash Drive หรือ Memory Card หรือระบบคลาวด์ (Cloud Computing) เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

2.3 ห้ามปรับแต่งหรือยกเลิกการทำงานของโปรแกรมป้องกันไวรัสที่กรมกิจการผู้สูงอายุติดตั้งให้

2.4 มีส่วนร่วมในการบำรุงรักษาโปรแกรมป้องกันไวรัสที่ใช้โดยตรวจสอบว่ามีการ Update โปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้ผู้แลระบบทราบหากไม่สามารถ Update โปรแกรมป้องกันไวรัสให้ทันสมัยได้

2.5 แจ้งให้ผู้ดูแลระบบทราบทันทีเมื่อพบว่าคอมพิวเตอร์หรือโปรแกรมที่ใช้มีความผิดปกติหรือเมื่อสงสัยว่ามีการติดไวรัส

2.6 ตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นด้วยโปรแกรมป้องกันไวรัสทุกครั้ง เมื่อมีการนำมาติดตั้งหรือใช้งาน และหากตรวจพบไวรัสจะต้องจัดการทำลายไวรัสโดยเร็วที่สุด

2.7 หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมที่นำมาใช้งานได้ ห้ามทำการเปิดข้อมูลหรือติดตั้งโปรแกรมลงไปบนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เด็ดขาด

2.8 ห้ามนำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access Point, Wireless Router, Wireless USB client หรือ Wireless Card

2.9 กรณีที่ผู้ใช้งานพยายามเข้าถึงระบบโดยมิชอบ หรือโจมตีระบบ หรือมีพฤติกรรมการใช้งานที่ขัดต่อประกาศ หรือข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของกรมกิจการผู้สูงอายุ ซึ่งอาจทำให้เกิดความเสี่ยงต่อความปลอดภัยและความเสียหายต่อระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ ผู้ใช้งานจะถูกระงับหรือยกเลิกการใช้งานระบบเครือข่าย และอินเทอร์เน็ตของกรมกิจการผู้สูงอายุทันที

2.10 กรณีที่ผู้ใช้งานได้กระทำการใดๆ ที่มีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติมหรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของกรมกิจการผู้สูงอายุ ผู้ใช้งานจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

เรื่องที่ 5
ข้อปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน ครุภัณฑ์ด้านฮาร์ดแวร์ ซอฟต์แวร์ตามระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ

2. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้สารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

2.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

(1) อ่านอย่างเดียว

(2) สร้างข้อมูล

(3) ป้อนข้อมูล

(4) แก้ไขข้อมูล

(5) อนุมัติ

(6) ไม่มีสิทธิ์

2.2 กำหนดเกณฑ์การระงับ/เพิกถอนสิทธิ์ให้เป็นไปตามข้อปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งานที่ได้กำหนดไว้

2.3 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้ดูแลระบบ

3. กำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

3.1 การควบคุมการเข้าถึงสารสนเทศโดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิ์ที่เกี่ยวข้องกับระบบสารสนเทศ

3.2 การปรับปรุงให้สอดคล้องกับการใช้งานตามภารกิจและด้านความมั่นคงปลอดภัย

เรื่องที่ 6
ข้อปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุ

1.1 ห้ามผู้ใดเข้าใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุโดยไม่ได้รับอนุญาต หากบุกรุกหรือพยายามบุกรุก ถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

1.2 ผู้ที่ประสงค์จะใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุ จะต้องขออนุญาตจากผู้ดูแลระบบก่อน

1.3 ผู้ใช้งานจะได้รับสิทธิ์ให้เข้าใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุ ได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

1.4 ผู้ใช้งานที่ได้รับสิทธิ์ให้เข้าใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุ จะได้รับบัญชีผู้ใช้งาน (Account) เป็นการเฉพาะบุคคลเท่านั้น ซึ่ง Account จะประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) โดยผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้

1.5 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งาน (Account) ทุกครั้งที่เข้าใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุ

1.6 ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภททำ Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

1.7 ห้ามผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

1.8 ห้ามผู้ใช้งานละเมิดต่อผู้อื่น เช่น ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว กรมกิจการผู้สูงอายุไม่มีส่วนร่วมรับผิดชอบต่อความเสียหายดังกล่าว

2. การใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุจากภายนอก

2.1 ผู้ใช้งานต้องขออนุญาตและได้รับอนุญาตจากผู้ดูแลระบบแล้วเท่านั้น จึงจะสามารถเข้าใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุจากภายนอกได้ และจะเข้าใช้ได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

2.2 ผู้ใช้งานที่เข้าใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุจากภายนอก หรือ Internet จะต้องเชื่อมต่อด้วยวิธีการ Remote Access ผ่าน VPN โดยต้องได้รับการอนุญาตจากผู้ดูแลระบบเท่านั้น

3. การระบุอุปกรณ์บนเครือข่าย

3.1 ระบุหมายเลขอุปกรณ์บนเครือข่าย ประกอบด้วย หมายเลขเทอร์มินัล หมายเลข MAC Address และหมายเลข IP Address

3.2 ใช้ไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่น ๆ เพื่อกำหนดว่าหมายเลขระบุอุปกรณ์ใดที่สามารถเข้าถึงเครือข่ายส่วนใดของกรมกิจการผู้สูงอายุ

3.3 อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

3.4 รักษาความมั่นคงปลอดภัยทางกายภาพต่ออุปกรณ์เครือข่ายหรืออุปกรณ์คอมพิวเตอร์เพื่อป้องกันการเปลี่ยนแปลงแก้ไขหมายเลขระบุอุปกรณ์เหล่านั้น

3.5 จัดเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

3.6 กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่

3.7 จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

3.8 ทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง

4. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

4.1 ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหา และตั้งค่าระบบทั้งทางกายภาพและโดยการล็อกอินเข้ามาใช้งาน

4.2 ยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

4.3 กำหนดการเปิด - ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงและก่อให้เกิดความเสียหายต่อระบบเครือข่าย

4.4 ติดตั้งระบบป้องกันและตรวจสอบการเข้าออกห้อง Data center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุอย่างปลอดภัย เช่น ระบบชีวภาพ (Biometric) หรือสมาร์ทการ์ด (Smartcard) และติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรกรรม เป็นต้น

4.5 ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้อง Data center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ หากมีความจำเป็นต้องแจ้งให้ผู้ดูแลระบบเป็นผู้รับผิดชอบอนุญาตเท่านั้น

5. การแบ่งแยกเครือข่าย

5.1 แยกกลุ่มเครือข่ายเป็น 7 ประเภทใหญ่ ๆ คือ 1) เครือข่ายภายนอก (External) 2) ส่วนที่มีการให้บริการสาธารณะ (Demilitarized Zone : DMZ) ที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก 3) เครือข่ายภายใน (Internal) 4) เครือข่ายสำหรับบริการเชื่อมต่อไร้สาย (Wireless Device) 5) เครือข่ายสำหรับงานบริหารจัดการศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ (DC) 6) เครือข่ายสำหรับ

ติดตั้งระบบงานสารสนเทศต่าง ๆ ของกรมกิจการผู้สูงอายุ (Applications) และ 7) เครือข่ายสำหรับติดตั้งระบบฐานข้อมูล (Database)

5.2 แยกวงเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่น ๆ ของกรมกิจการผู้สูงอายุ

5.3 ใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย

5.4 ใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอกกรมกิจการผู้สูงอายุ

5.5 กรองและจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อย

5.6 ผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่ง จะไม่สามารถเข้าถึงข้อมูลที่อยู่ในอีกวงเครือข่ายหนึ่งได้โดยตรง

5.7 จัดทำผังเครือข่ายที่แสดงถึงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก โดยมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง

6. การควบคุมการเชื่อมต่อทางเครือข่าย

6.1 ตรวจสอบและจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายให้เป็นไปตามนโยบายในการควบคุมการเข้าถึง และข้อกำหนดของระบบงาน

6.2 จำกัดสิทธิ์และความสามารถของผู้ใช้งานในการเชื่อมต่อเพื่อเข้าสู่ระบบเครือข่ายกรมกิจการผู้สูงอายุ

6.3 ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายกรมกิจการผู้สูงอายุ โดยไม่ได้รับอนุญาต

6.4 ระบุอุปกรณ์และเครื่องมือที่ใช้ในการควบคุมการเชื่อมต่อระบบเครือข่ายของกรมกิจการผู้สูงอายุ

6.5 ใช้ไฟร์วอลล์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่ายให้เป็นไปตามนโยบายในการควบคุมการเข้าถึง

6.6 ป้องกันเลขที่อยู่ของไอพี (IP Address) ของระบบเครือข่ายภายในของกรมกิจการผู้สูงอายุมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

6.7 ติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้ระบบเครือข่ายของกรมกิจการผู้สูงอายุในลักษณะที่ผิดปกติ

6.8 การเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกกรมกิจการผู้สูงอายุ จะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก ซึ่งมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware)

6.9 ห้ามเปิดช่องทางการเชื่อมต่อทางเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายในของกรมกิจการผู้สูงอายุ เพื่อให้สามารถเข้าถึงเครื่องแม่ข่ายสำหรับระบบงานได้จากระยะไกล ยกเว้นในกรณีที่มีความจำเป็นหรือมีความเร่งด่วนสูง ซึ่งจะต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนดำเนินการ

เรื่องที่ 7

ข้อปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. ขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

1.1 ผู้ที่ประสงค์จะเข้าถึงระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายของกรมกิจการผู้สูงอายุ จะต้องขออนุญาตและได้รับอนุมัติจากผู้ดูแลระบบก่อนทุกครั้ง

1.2 ผู้ใช้งานจะได้รับสิทธิ์ให้เข้าถึงระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายของกรมกิจการผู้สูงอายุได้แต่เพียงระบบที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

1.3 ผู้ใช้งานที่ได้รับสิทธิ์ให้เข้าถึงระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายของกรมกิจการผู้สูงอายุจะได้รับบัญชีผู้ใช้งาน (Account) เป็นการเฉพาะบุคคลเท่านั้น ซึ่ง Account จะประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) โดยผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้

1.4 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งาน (Account) ทุกครั้งที่เข้าถึงระบบปฏิบัติการของกรมกิจการผู้สูงอายุ

1.5 การใช้งานเครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบ ผู้ใช้งานต้องทำการกำหนดรหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ให้กับเครื่องคอมพิวเตอร์

1.6 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

1.7 ผู้ใช้งานต้องลงบันทึกออก (Logout) ทันที เมื่อเลิกใช้งานเครื่องคอมพิวเตอร์หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

1.8 ห้ามผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

1.9 ผู้ใช้งานสามารถขอใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ของกรมกิจการผู้สูงอายุได้ตามหน้าที่ความจำเป็นเท่านั้น

1.10 ซอฟต์แวร์ที่กรมกิจการผู้สูงอายุจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

1.11 ห้ามผู้ใช้งานใช้ทรัพยากรทุกประเภทที่เป็นของกรมกิจการผู้สูงอายุเพื่อประโยชน์ทางการค้า

1.12 ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

1.13 ในกรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม

1.14 ห้ามผู้ใช้งานใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุในการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาต

2. การระบุและยืนยันตัวตนของผู้ใช้งาน

2.1 ผู้ดูแลระบบต้องตั้งชื่อบัญชีผู้ใช้งาน (Account) แต่ละประเภทแตกต่างกัน เช่น บัญชีของผู้ใช้งานทั่วไป บัญชีของผู้ดูแลระบบ บัญชีของผู้ดูแลฐานข้อมูล บัญชีของผู้พัฒนาระบบ บัญชีของเจ้าหน้าที่ทางเทคนิคอื่น ๆ เป็นต้น

2.2 ผู้ใช้งานทุกคนต้องมีบัญชีผู้ใช้งาน (Account) เฉพาะของแต่ละบุคคลแยกจากกัน เพื่อใช้ในการพิสูจน์ตัวตน

2.3 สำหรับระบบที่มีความสำคัญสูง ต้องกำหนดให้ผู้ใช้งานพิสูจน์ตัวตนด้วยวิธีการทางเทคนิคที่มีความมั่นคงปลอดภัยสูง เช่น ใช้วิธีการเข้ารหัสข้อมูล วิธีการทางชีวภาพ (เช่น การใช้ลายนิ้วมือ ฝ่ามือ เสียง แสกนใบหน้า)

3. ระบบบริหารจัดการรหัสผ่าน

3.1 การกำหนดความปลอดภัยของรหัสผ่านให้เป็นไปตามเรื่องที่ 3 ข้อปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน ข้อ 4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

3.2 ให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๆ 3 เดือน

3.3 ให้มีการจัดเก็บรหัสผ่านเดิมที่ผู้ใช้งานเคยตั้งไปแล้ว เพื่อตรวจสอบไม่ให้นำกลับมาใช้ใหม่ตามระยะเวลาที่เหมาะสม

3.4 ไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอ ในขณะที่ผู้ใช้งานกำลังใส่ข้อมูลเพื่อเข้าใช้งานระบบ เช่น ให้แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอ เป็นต้น

3.5 ให้มีการป้องกันไฟล์ข้อมูลรหัสผ่านที่ได้มีการจัดเก็บไว้หรือที่จำเป็นต้องส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น ป้องกันโดยการเข้ารหัสข้อมูล (Encryption) พร้อมการคำนวณผลรวม (Hash) เพื่อซ่อนข้อมูลไว้

3.6 การจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานจะต้องแยกต่างหากจากข้อมูลของระบบงาน

4. การใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้

4.1 การจัดเก็บโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ต้องแยกจัดเก็บไว้ต่างหาก เช่น แยกไว้ในไดเรกทอรีที่ต่างจากไดเรกทอรีของซอฟต์แวร์ระบบงาน

4.2 จัดทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ที่อนุญาตให้ใช้งานได้

4.3 ห้ามผู้ใช้งานทั่วไปใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้โดยจำกัดสิทธิ์ให้เฉพาะผู้ดูแลระบบหรือผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

4.4 ผู้ใช้งานที่ต้องการใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ต้องขออนุญาตจากผู้ดูแลระบบก่อน โดยระบุเหตุผลความจำเป็นหรือความต้องการใช้งาน

4.5 ยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ที่ไม่มีความจำเป็นต้องใช้งานแล้ว

เรื่องที่ 8
ข้อปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
(Application and Information Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การจำกัดการเข้าถึงสารสนเทศ

1.1 กำหนดการควบคุมการเข้าถึงกับระบบงาน

1.1.1 ตรวจสอบข้อมูลการล็อกอิน หลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว

1.1.2 บันทึกข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ

1.1.3 แสดงวันเวลาของการล็อกอินครั้งที่แล้วทั้งที่สำเร็จและไม่สำเร็จ

1.1.4 แสดงข้อมูลพื้นฐานเท่าที่จำเป็นเพื่อให้ผู้ใช้งานได้รับทราบข้อมูล

1.1.5 จำกัดสิทธิ์การเข้าถึงจากอีกระบบหนึ่ง โดยให้สามารถเข้าถึงได้เฉพาะข้อมูลและฟังก์ชันที่จำเป็นต้องใช้งานเท่านั้น

1.1.6 จำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อทันทีเมื่อพ้นช่วงเวลาที่กำหนด

1.1.7 เปลี่ยนรหัสผ่านของระบบตามระยะเวลาที่กำหนด

1.2 กำหนดขั้นตอนและแบบฟอร์มในการเข้าถึงและใช้งานระบบ เพื่อกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงข้อมูลและฟังก์ชันต่าง ๆ ของระบบ และใช้ในการตรวจสอบและยืนยันตัวตนของผู้ใช้งาน เช่น สิทธิ์ในการอ่าน เขียน ลบ หรือสั่งให้โปรแกรมทำงาน โดยแบบฟอร์มต้องระบุข้อมูลอย่างน้อยดังนี้ ชื่อและนามสกุล ตำแหน่ง หน่วยงาน เหตุผล และระยะเวลาที่ขอเข้าถึงและใช้งานระบบ

1.3 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ตามมาตรฐานสากล

2. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

2.1 ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์หรือไม่

2.2 ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

2.3 เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้วให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

2.4 เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนให้อยู่ในสภาพพร้อมใช้งาน

2.5 หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

3. การปฏิบัติงานจากภายนอกสำนักงานสำหรับผู้ดูแลระบบ

3.1 ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ

3.2 ตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนดหรือไม่

3.3 กำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่าง ๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

3.4 กำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการขอยกเลิกการกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

เรื่องที่ 9
ข้อปฏิบัติในการควบคุมการเข้าถึงของหน่วยงานภายนอก (Outsource Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงของหน่วยงานภายนอก (outsource control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การเข้าออกห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ

1.1 ผู้ใช้งานต้องขออนุญาตล่วงหน้าก่อนวันที่จะเข้าออกพื้นที่ โดยต้องกรอกแบบฟอร์มคำขอเข้าใช้งานห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ และข้อมูลความต้องการและรายละเอียดตามแบบฟอร์มที่ทางผู้ดูแลระบบกำหนด

1.2 ผู้ใช้งานต้องได้รับอนุมัติสิทธิ์ในการเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุจากผู้ดูแลระบบหรือเจ้าหน้าที่ได้รับมอบหมายก่อนจึงจะเข้าออกพื้นที่ได้

1.3 ผู้ใช้งานจะถูกบันทึกรายละเอียดข้อมูลลงในทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่ห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ

1.4 ผู้ใช้งานต้องแลกบัตรที่ใช้ระบุตัวตนของแต่ละบุคคล เช่น บัตรประจำตัวประชาชนหรือใบอนุญาตขับขี่ หรือบัตรอนุญาตเข้าออกภายในอาคารที่ได้แลกมาก่อนหน้า เป็นต้น เพื่อรับบัตรผู้มาติดต่อ (Visitor) และบันทึกข้อมูลลงในแบบบันทึกการเข้าออกพื้นที่ห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุทุกครั้งที่มีการเข้าออก

1.5 ผู้ใช้งานต้องติดบัตรผู้มาติดต่อ (Visitor) ตรงจุดที่สามารถมองเห็นได้ชัดเจนตลอดเวลาที่อยู่ภายในพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ

1.6 กรณีที่ต้องการนำอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่าย เข้ามาภายในบริเวณพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ จะต้องได้รับอนุญาตจากผู้ดูแลระบบ

1.7 ผู้ใช้งานต้องคืนบัตรผู้มาติดต่อ (Visitor) ณ จุดแลกบัตรจุดเดิม โดยผู้ดูแลระบบจะตรวจสอบแต่ละบุคคลลงบันทึกเวลาออกในแบบบันทึกการเข้าออกพื้นที่ห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ ทุกครั้งที่มีการเข้าออก

1.8 กรณีที่จะเข้ามาปฏิบัติงานในห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ ในวันหยุดหรือนอกเวลาราชการ จะต้องขออนุญาตจากผู้ดูแลระบบล่วงหน้าก่อนทุกครั้ง และการดำเนินงานจะต้องอยู่ในการกำกับดูแลของผู้ดูแลระบบเท่านั้น

2. การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

2.1 ผู้ใช้งานต้องขออนุญาตไว้ล่วงหน้าเป็นลายลักษณ์อักษรก่อนเข้าถึงระบบทุกครั้ง พร้อมทั้งแจ้งให้ผู้ดูแลระบบทราบ โดยต้องระบุข้อมูลอย่างน้อยดังนี้ ชื่อและนามสกุล ตำแหน่ง หน่วยงาน เหตุผล โครงการที่รับจ้าง และระยะเวลาที่ขอเข้าถึงและใช้งานระบบตามแบบฟอร์มคำขอเข้าใช้งานห้อง Data Center หรือศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ

2.2 ผู้ใช้งานต้องได้รับอนุญาตจากผู้ดูแลระบบแล้วเท่านั้น จึงจะสามารถดำเนินการบำรุงรักษาบริหารจัดการพอร์ตของอุปกรณ์เครือข่ายบริหารจัดการผ่านระบบเครือข่าย และการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุได้ และจะดำเนินการได้เฉพาะรายการที่ได้รับอนุญาตเท่านั้น

2.3 ผู้ใช้งานต้องทำการสำรองค่า Config ของอุปกรณ์ทุกชนิดภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ โปรแกรม/โมดูลของระบบงานสารสนเทศ และโครงสร้างฐานข้อมูลทุกครั้งก่อนแก้ไขหรือเปลี่ยนแปลงค่า รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไข หากการแก้ไขมีปัญหาเกิดขึ้นทำให้ไม่สามารถใช้งานระบบได้ผู้ใช้งานจะต้องเรียกคืนข้อมูลที่ได้สำรองไว้กลับมา เพื่อให้ระบบสามารถใช้งานได้ตามสภาพเดิม

2.4 การเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายคอมพิวเตอร์ของกรมกิจการผู้สูงอายุ จะต้องดำเนินการ ดังนี้

2.4.1 ขออนุญาตและได้รับอนุญาตจากผู้ดูแลระบบแล้วเท่านั้น จึงจะสามารถเชื่อมต่อจากภายนอกได้ โดยจะต้องระบุบริการที่ขออนุญาต วัน เวลา และระยะเวลาในการเชื่อมต่อให้ชัดเจน

2.4.2 จะต้องเชื่อมต่อด้วยวิธีการ Remote Access VPN

2.5 กรณีที่ผู้ใช้งานประมาททำให้อุปกรณ์และระบบสารสนเทศของกรมกิจการผู้สูงอายุ ได้รับความเสียหายหรือสูญหาย ผู้ใช้งานจะต้องรับผิดชอบในการซ่อมแซมแก้ไขหรือเปลี่ยนใหม่ให้อยู่ในสภาพที่สามารถใช้งานได้ดังเดิม

2.6 หากมีการเปลี่ยนแปลงรายชื่อผู้ใช้งาน จะต้องแจ้งให้ผู้ดูแลระบบทราบล่วงหน้าเป็นลายลักษณ์อักษรก่อนมีการเปลี่ยนแปลงทุกครั้ง

เรื่องที่ 10
ข้อปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศ

วัตถุประสงค์

เพื่อให้หน่วยงานมีระบบสำรองข้อมูลและสารสนเทศที่เหมาะสม และมีการเตรียมความพร้อมกรณีฉุกเฉินหากไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้เพื่อให้หน่วยงานสามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

ข้อปฏิบัติ

1. การสำรองและทดสอบกู้คืนข้อมูล

1.1 จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูลเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับระบบสารสนเทศของกรมกิจการผู้สูงอายุลงในแผนปฏิบัติการดิจิทัลของกรมกิจการผู้สูงอายุ

1.2 พิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นตามลำดับความสำคัญเพื่อจัดทำระบบสำรอง

1.3 กำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ และความถี่ในการสำรอง

1.4 กำหนดสื่อที่ใช้ในการเก็บข้อมูลและรูปแบบของการสำรองข้อมูล ซึ่งมี 2 ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Back up) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

1.5 รายการที่ต้องสำรองข้อมูลและความถี่อย่างน้อย ดังนี้

- เว็บไซต์หน่วยงาน : สำรองข้อมูลที่เผยแพร่บนเว็บไซต์ 1 ครั้ง/เดือน Web Application
- Servers : สำรองข้อมูลที่เผยแพร่บนเว็บไซต์ 1 ครั้ง/เดือน
- Database Servers : สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ
- Firewall Server : สำรองข้อมูล Rule ของ Firewall
- Server อื่น ๆ : สำรองข้อมูลบนเซิร์ฟเวอร์อื่น ๆ

1.6 มีการสำรองข้อมูลเครื่องแม่ข่ายทั้งระบบ (Full System Backup) อย่างน้อยปีละ 1 ครั้ง

1.7 รายละเอียดที่ปรากฏในแผนการสำรองและทดสอบกู้คืนข้อมูล ต้องมีหัวข้อสำคัญอย่างน้อย ดังนี้

- รายการที่ต้องสำรองข้อมูล
- การสำรองข้อมูล
- การทดสอบกู้คืนข้อมูล
- ปฏิทินการสำรองและทดสอบกู้คืนข้อมูล
- ผู้รับผิดชอบ
- การติดตามประเมินผล

1.8 ติดตามประเมินผล และทบทวน/ปรับปรุงแผนการสำรองและทดสอบกู้คืนข้อมูล ปีละ 1 ครั้ง

เรื่องที่ 11
ข้อปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้หน่วยงานมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจจะเกิดขึ้น ทำให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน โดยการตรวจสอบและประเมินความเสี่ยงนั้น จะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

ข้อปฏิบัติ

1. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

1.1 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของกรมกิจการผู้สูงอายุ โดยดำเนินการให้สอดคล้องตามแผนและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล กรมกิจการผู้สูงอายุ และกฎหมายที่เกี่ยวข้อง

1.2 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของกรมกิจการผู้สูงอายุ ให้ดำเนินการโดยคณะทำงานเทคโนโลยีสารสนเทศ กรมกิจการผู้สูงอายุ

1.3 กำหนดขอบเขตและขั้นตอนปฏิบัติสำหรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของกรมกิจการผู้สูงอายุ

1.4 จัดทำแผนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กรมกิจการผู้สูงอายุ ดังนี้

1.4.1 การทดสอบหาช่องโหว่ของระบบ (Vulnerability Assessment)

1.4.2 การทบทวนนโยบายอุปกรณ์ที่ใช้ในการป้องกันภัยคุกคามในการใช้งานอินเทอร์เน็ตที่ใช้งานอยู่ (Firewall Review)

1.4.3 การตรวจประเมินการตั้งค่าของอุปกรณ์เครือข่าย (Configuration Assessment)

1.4.4 การพัฒนาการตอบสนองต่อเหตุไม่คาดฝัน (Incident handling improvement)

1.4.5 จัดฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Awareness Training)

1.4.6 การตรวจสอบการรั่วไหลของข้อมูล ใน Dark web

1.4.7 การทดสอบการเจาะระบบ (Penetration Testing)

1.4.8 การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

1.4.9 การตรวจสอบความมั่นคงปลอดภัยซอร์สโค้ด (Security source code review)

1.4.10 การตรวจสอบเครื่องเป้าหมายที่อาจมีความเสี่ยงที่จะถูกยึดครอง (Compromised Assessment)

1.4.11 ปรับปรุงระบบหรือปิดช่องโหว่ของระบบสารสนเทศ หรือเครือข่ายที่ตรวจพบ

1.4.12 ด้านอื่น ๆ ที่เกี่ยวข้อง

2. เป็นสรุปรายงานผลตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของกรมกิจการผู้สูงอายุและรายงานต่อคณะทำงานเทคโนโลยีสารสนเทศ เพื่อทราบต่อไป

3. ทบทวน/ปรับปรุงแผนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กรมกิจการผู้สูงอายุอย่างน้อยปีละครั้ง

เรื่องที่ 12
ข้อปฏิบัติในการใช้งานอินเทอร์เน็ต

วัตถุประสงค์

เพื่อเป็นมาตรการควบคุมการใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุให้มีความมั่นคงปลอดภัย และลดความเสี่ยงหรือผลกระทบที่อาจจะเกิดจากการใช้งานอินเทอร์เน็ตของผู้ใช้งาน ตลอดจนป้องกันมิให้ผู้ใช้งานละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การลงทะเบียนผู้ใช้งาน

1.1 ผู้ขอใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ จะต้องลงทะเบียนเพื่อขอใช้งานจากผู้ดูแลระบบก่อน โดยการกรอกข้อมูลส่วนบุคคลในแบบฟอร์มลงทะเบียนผู้ใช้งานที่กรมกิจการผู้สูงอายุจัดเตรียมไว้

1.2 ผู้ขอใช้งานที่ได้รับสิทธิ์ให้เข้าใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุจะได้รับบัญชีผู้ใช้งานอินเทอร์เน็ต (Account) ซึ่งประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่านชั่วคราว (Password)

2. การใช้งานบัญชีผู้ใช้งานอินเทอร์เน็ต (Account)

2.1 ผู้ใช้งานต้องเปลี่ยน Password โดยทันทีหลังจากที่ได้รับ Account จากผู้ดูแลระบบ

2.2 ผู้ใช้งานควรตั้ง Password โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ และควรมีความยาวอย่างน้อย 12 ตัวอักษร

2.3 ผู้ใช้งานควรเปลี่ยน Password ทุก ๆ 3 เดือน หรือตามที่ผู้ดูแลระบบกำหนด

2.4 ผู้ใช้งานควรเปลี่ยน Password ใหม่ทันที หากถูกเปิดเผยหรือสงสัยว่าถูกผู้อื่นนำ Password ไปใช้

2.5 ผู้ใช้งานต้องใช้ Account ของตนเองเท่านั้น ในการเข้าใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ

2.6 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้ Account ในนามของตนเองไม่ว่ากรณีใด ๆ

2.7 ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดจากการใช้งาน Account ในนามของตนเอง

2.8 ผู้ใช้งานต้องทำการ Logout ออกจากคอมพิวเตอร์ทันทีเมื่อเลิกใช้งานอินเทอร์เน็ต หรือเมื่อไม่อยู่ที่หน้าจอคอมพิวเตอร์นานเกิน 15 นาที

3. การเข้าใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ

3.1 ผู้ใช้งานสามารถเข้าใช้งานได้ภายในบริเวณพื้นที่ที่อยู่ในความรับผิดชอบของกรมกิจการผู้สูงอายุ

3.2 ผู้ใช้งานสามารถเข้าใช้งานได้ 2 ช่องทาง ดังนี้

3.2.1 เชื่อมต่อกับระบบเครือข่ายแบบ LAN

3.2.2 เชื่อมต่อกับระบบเครือข่ายแบบไร้สาย หรือ Wireless LAN

3.3 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งานอินเทอร์เน็ต (Account) ที่ได้รับจากการลงทะเบียนผู้ใช้งาน

4. การใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุอย่างปลอดภัย

4.1 การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเทอร์เน็ต ควรเชื่อมต่อผ่านระบบรักษาความมั่นคงปลอดภัยที่กรมกิจการผู้สูงอายุจัดสรรไว้เท่านั้น

4.2 ผู้ใช้งานต้องไม่ใช้อินเทอร์เน็ตของกรมกิจการผู้สูงอายุในการเผยแพร่หรือใช้งานโดยมีวัตถุประสงค์ดังนี้

4.2.1 ก่อให้เกิดความเสียหายต่อกรมกิจการผู้สูงอายุและบุคคลอื่น หรือละเมิดสิทธิ์ หรือสร้างความรำคาญต่อผู้อื่น เช่น การตัดต่อภาพของผู้อื่นแล้วนำมาเผยแพร่ทำให้เกิดความอับอาย ลักลอบแก้ไขข้อมูลส่วนบุคคลของผู้อื่น การแสดงความเห็นดูหมิ่นผู้อื่นบนเว็บไซต์ เป็นต้น

4.2.2 หาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือการพาณิชย์ เช่น การจำลอง Mail Server เพื่อส่ง mail จำนวนมาก และการจำลอง Web Server เพื่อจัดทำเว็บไซต์สำหรับค้าขาย เป็นต้น

4.2.3 การกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน เช่น การเข้าสู่เว็บไซต์ที่ไม่เหมาะสม การใช้ข้อความที่สร้างความตื่นตระหนกกับสังคมโดยรวม เป็นต้น

4.2.4 เปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาต ซึ่งได้มาจากกรมกิจการผู้สูงอายุหรือผู้ที่มีสิทธิ์ในข้อมูลดังกล่าว

4.3 ผู้ใช้งานไม่ควรดาวน์โหลดหรือใช้งานข้อมูลมัลติมีเดีย ที่มีลักษณะยึดครองช่องสัญญาณการสื่อสารข้อมูลตลอดเวลา (Consume Bandwidth) ผ่านอินเทอร์เน็ตของกรมกิจการผู้สูงอายุในเวลาราชการ เช่น เล่นเกม/ดูหนัง/ฟังเพลงออนไลน์ ดูคลิปวิดีโอผ่านเว็บไซต์ ดาวน์โหลดซอฟต์แวร์ที่มีขนาดใหญ่ผ่านเว็บไซต์ เป็นต้น

4.4 ผู้ใช้งานไม่ควรดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือหรือไม่มั่นใจว่าปลอดภัย เช่น Freeware โปรแกรมรักษาจอภาพ เกมส์และโปรแกรมที่ลงท้ายด้วย exe หรือ com หากมีความจำเป็นต้องดาวน์โหลด ต้องมีการตรวจสอบด้วยโปรแกรมป้องกันไวรัสก่อนการนำไปใช้ทุกครั้ง

4.5 หากผู้ใช้งานมีความจำเป็นต้องส่งข้อมูลที่มีขนาดใหญ่ ให้ติดต่อผู้ดูแลระบบดำเนินการเท่านั้น

4.6 ผู้ใช้งานที่มีความจำเป็นต้องนำคอมพิวเตอร์โน้ตบุ๊กไปเชื่อมต่อเข้ากับอินเทอร์เน็ตอื่นที่มิใช่กรมกิจการผู้สูงอายุ จะต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่คอมพิวเตอร์โน้ตบุ๊กดังกล่าว และต้อง Update ซอฟต์แวร์ป้องกันไวรัสให้เป็นปัจจุบันอยู่เสมอ

4.7 ผู้ใช้งานควรแจ้งข้อเท็จจริงต่อผู้ดูแลระบบ หากพบเห็นการใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุไปในทางที่ไม่เหมาะสม หรือพบเห็นการบุกรุก หรือการละเมิดสิทธิ์ของกรมกิจการผู้สูงอายุ

5. การใช้งานเครือข่ายสังคมออนไลน์

5.1 ผู้ใช้งานต้องตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับหน่วยงานอันเกิดจากการใช้งานเครือข่ายสังคมออนไลน์

5.2 ผู้ใช้งานต้องรับผิดชอบทั้งด้านสังคมและกฎหมาย เนื่องจากการโพสต์ข้อความหรือแสดงความคิดเห็นเพื่อให้เผยแพร่บนเครือข่ายสังคมออนไลน์ เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ

5.3 ผู้ใช้งานไม่ควรเปิดเผยข้อมูลส่วนตัวมากเกินไป รวมถึงข้อมูลทางการเงิน

5.4 ผู้ใช้งานไม่ควรโพสต์ข้อความที่บอกสถานะความเคลื่อนไหวของตนเอง เพราะจะทำให้ผู้ไม่หวังดีวางแผนมาทำร้ายหรือขโมยทรัพย์สินได้

5.5 ผู้ใช้งานต้องระมัดระวังอย่างยิ่งในการโพสต์หรือเผยแพร่ ส่งต่อข้อความ รูปภาพ วิดีโอ ที่อาจทำให้ผู้อื่นเสียหาย เช่น ภาพหลุด คลิปหลุด หรือโพสต์รูปภาพที่สื่อถึงอบายมุขต่าง ๆ และไม่ควรใช้ถ้อยคำหยาบคาย ถ้อยคำลามก อนาจาร ดูหมิ่น ส่อเสียด เสียดสีให้ร้ายผู้อื่นในทางเสียหาย หรือสร้างความแตกแยกในสังคม

5.6 ผู้ใช้งานต้องระมัดระวังอย่างยิ่งที่จะไว้ใจหรือเชื่อใจคนที่รู้จักผ่านอินเทอร์เน็ตในการแลกเปลี่ยนข้อมูลส่วนตัว เช่น ชื่อ อีเมล หมายเลขโทรศัพท์ ที่อยู่ เพราะอาจถูกหลอกลวงหรือล่อลวงไปทำอันตรายได้

5.7 ผู้ใช้งานต้องระมัดระวังการเช็คอิน (Check-in) โดยใช้กล้องโทรศัพท์ถ่ายภาพ ระบุพิกัดและเวลา เพราะภาพทุกภาพการโพสต์ทุกอย่างจะอยู่บนอินเทอร์เน็ตอย่างถาวรไม่สามารถถูกลบได้อย่างแท้จริง

6. การระงับ/เพิกถอนบัญชีผู้ใช้งานอินเทอร์เน็ต (Account)

6.1 ผู้ดูแลระบบมีสิทธิ์ระงับ Account ของผู้ใช้งานได้ทันที หากได้รับแจ้งหรือตรวจพบการกระทำใดที่อาจก่อให้เกิดปัญหาความมั่นคงปลอดภัย หรือการกระทำที่ละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้อง

6.2 ผู้ดูแลระบบมีสิทธิ์เพิกถอน Account ของผู้ใช้งานออกจากระบบได้ทันที หากไม่มีการติดต่อภายในระยะเวลา 90 วันนับจากวันที่ถูกระงับ Account หรือไม่มีการร้องขอขยายสิทธิ์การใช้งาน

6.3 ผู้ดูแลระบบมีสิทธิ์เพิกถอน Account ของผู้ใช้งานออกจากระบบได้ ดังนี้

6.3.1 กรณีเป็นเจ้าหน้าที่ของกรมกิจการผู้สูงอายุ ให้เพิกถอนเมื่อผู้ใช้งานนั้นลาออกหรือพ้นสภาพจากการเป็นเจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือเมื่อไม่มีการเข้าใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุเป็นระยะเวลาติดต่อกันเกิน 90 วัน

6.3.2 กรณีเป็นบุคคลจากหน่วยงานภายนอก ให้เพิกถอนตามวันที่ระบุในแบบฟอร์มลงทะเบียนผู้ใช้งาน หรือเมื่อไม่มีการเข้าใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุต้องแจ้งผู้ดูแลระบบทันที

6.4 ผู้ใช้งานสามารถร้องขอขยายสิทธิ์การใช้งาน Account ได้ เพื่อคงสิทธิ์เดิมไว้เมื่อต้องพ้นสภาพจากการเป็นเจ้าหน้าที่ของกรมกิจการผู้สูงอายุ โดยยื่นคำร้องส่งถึงผู้ดูแลระบบ

เรื่องที่ 13
ข้อปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)

วัตถุประสงค์

ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) ภายใต้ชื่อโดเมน @dop.mail.go.th ให้บริการเพื่อสนับสนุนการดำเนินงานของเจ้าหน้าที่ในสังกัดกรมกิจการผู้สูงอายุสำหรับใช้ติดต่อสื่อสารงานราชการให้มีความปลอดภัยและเชื่อถือได้ รวมถึงมีข้อปฏิบัติที่สอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่หรือหน่วยงานในสังกัดกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การลงทะเบียนผู้ใช้งาน

1.1 ผู้ขอใช้งานจะต้องลงทะเบียนเพื่อขอใช้งาน e-Mail จากผู้ดูแลระบบก่อน โดยการกรอกข้อมูลในแบบฟอร์มลงทะเบียนผู้ใช้งานที่ผู้ดูแลระบบจัดเตรียมไว้

1.2 ผู้ขอใช้งานที่ได้รับสิทธิ์ให้เข้าใช้งาน e-Mail ได้ จะได้รับบัญชีผู้ใช้งาน (Account) ภายใต้ชื่อโดเมน @dop.mail.go.th ซึ่งประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่านชั่วคราว (Password)

1.3 ผู้ใช้งาน e-Mail จะได้รับพื้นที่ใช้งาน จำนวน 10 GB และแนบไฟล์ได้ 25 MB

2. การเข้าใช้งาน e-Mail

2.1 ผู้ใช้งานสามารถเข้าใช้งาน e-Mail ได้ที่เว็บไซต์ http://dop.mail.go.th หรือ https://www.workd.go.th

2.2 ผู้ใช้งานควรเปลี่ยนรหัสผ่านทันทีที่เข้าใช้งานครั้งแรก (เนื่องจากรหัสผ่านที่ได้รับจากผู้ดูแลระบบเป็นรหัสผ่านชั่วคราวเท่านั้น)

3. การใช้งานบัญชีผู้ใช้งาน e-Mail

3.1 ผู้ใช้งานต้องเปลี่ยน Password โดยทันทีหลังจากที่ได้รับ Account จากผู้ดูแลระบบ

3.2 ผู้ใช้งานควรตั้ง Password ให้มีความยาวอย่างน้อย 12 ตัวอักษร และต้องประกอบด้วยตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ พิมพ์เล็ก และตัวเลข

3.3 ผู้ใช้งานควรเปลี่ยน Password ทุก ๆ 3 เดือน หรือตามที่ผู้ดูแลระบบกำหนด

3.4 ผู้ใช้งานควรเปลี่ยน Password ใหม่ทันที หากถูกเปิดเผยหรือสงสัยว่าถูกผู้อื่นนำ Password ไปใช้

3.5 ผู้ใช้งานต้องใช้ Account ของตนเองหรือที่ได้รับมอบหมายเท่านั้นในการเข้าใช้งาน e-Mail

3.6 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้ Account ในนามของตนเองไม่ว่ากรณีใด ๆ

3.7 ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดจากการใช้งาน Account ในนามของตนเอง

3.8 ผู้ใช้งานต้องทำการ Logout ออกจากการใช้งาน e-Mail ทันทีเมื่อเลิกใช้งาน หรือเมื่อไม่อยู่ที่หน้าจอคอมพิวเตอร์นานเกิน 15 นาที

3.9 ผู้ใช้งานจะต้องใช้งาน e-Mail อย่างต่อเนื่องเป็นประจำทุกเดือน หากไม่มีความเคลื่อนไหวจะถูกระงับการใช้งานทันที

4. การรับ - การส่ง e-Mail

4.1 ผู้ใช้งาน e-Mail ต้องตรวจสอบไวรัสกับไฟล์ที่แนบมาพร้อม e-Mail ทุกครั้ง

4.2 หากผู้ใช้งาน e-Mail ต้องการส่ง e-Mail ถึงผู้ใช้งานทุกคนหรือส่งแบบกลุ่มควรแจ้งให้ผู้ดูแลระบบทราบ เนื่องจากผู้ดูแลระบบได้สร้างบัญชีผู้ใช้งานแบบกลุ่มไว้แล้วเพื่ออำนวยความสะดวก และป้องกันการส่ง e-Mail ในลักษณะ Spam mail

4.3 ห้ามผู้ใช้งาน ใช้ e-Mail ในลักษณะดังต่อไปนี้

4.3.1 ไม่ควรเปิดหรือส่งต่อ e-Mail ที่ไม่ทราบแหล่งที่มาหรือไม่น่าเชื่อถือ

4.3.2 การใช้ e-Mail เพื่อลงทะเบียนสมัครงานบนเว็บไซต์สมัครงาน

4.3.3 การใช้ e-Mail เพื่อแสดงความคิดเห็นบนเว็บไซต์ขายสินค้า

4.3.4 การใช้ e-Mail เพื่อประกอบธุรกิจส่วนตัว หรือเพื่อบุคคลอื่น

4.3.5 การปลอมแปลงหรือดัดแปลงชื่อผู้ส่งให้เข้าใจผิดว่า e-Mail นั้น ๆ ส่งมาจากบุคคลอื่น

4.3.6 การปลอมแปลงหรือดัดแปลงส่วนหัวจดหมาย เช่น เส้นทาง วันเวลาการส่ง

4.3.7 การปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง

4.3.8 การส่ง e-Mail เพื่อเผยแพร่จดหมายลูกโซ่

4.3.9 การส่ง e-Mail เพื่อเผยแพร่ข้อมูลชั้นความลับของกรมกิจการผู้สูงอายุ

4.3.10 การส่ง e-Mail เพื่อเผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่กล่าวร้ายต่อบุคคลหรือกลุ่มบุคคล

4.3.11 การส่ง e-Mail เพื่อเผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่ดูหมิ่น เหยียดหยาม หรือแบ่งแยกทางศาสนา เชื้อชาติ หรือเพศ

4.3.12 การส่ง e-Mail เพื่อเผยแพร่ข้อความ ภาพ วิดีโอเสียง ที่มีลักษณะหยาบคายหรือลามกอนาจาร

4.3.13 การส่ง e-Mail เพื่อเผยแพร่โปรแกรมหรือรหัสสำหรับใช้ในการเข้าถึงโปรแกรมในลักษณะที่ละเมิดลิขสิทธิ์

4.3.14 การส่ง e-Mail เพื่อกระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

4.3.15 การส่ง e-Mail เพื่อโฆษณาสินค้า ผลิตภัณฑ์ หรือส่งข้อความในลักษณะ Spam Mail ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

4.3.16 การส่ง e-Mail ซึ่งส่งผลกระทบทำให้ระบบ e-Mail หรือระบบเครือข่ายลดทอนประสิทธิภาพลง

4.3.17 การส่ง e-Mail เพื่อกระจายไวรัสหรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบ

4.3.18 การส่ง e-Mail ต้องไม่เข้าข่ายการกระทำความผิดหรือขัดต่อกฎหมายอื่น ๆ ที่เกี่ยวข้อง

5. การส่ง e-Mail ผ่านบัญชีผู้ใช้งานแบบกลุ่ม

5.1 ผู้ดูแลระบบจัดให้มีระบบบัญชีผู้ใช้งาน e-Mail แบบกลุ่มตามคำร้องขอของหน่วยงาน ทั้งนี้ผู้ดูแลระบบขอสงวนสิทธิ์ในการอนุมัติการขอจดทะเบียนชื่อกลุ่ม ตลอดจนการตั้งชื่อกลุ่มโดยจะต้องตั้งชื่อกลุ่มตามหลักการที่ได้กำหนดไว้ หรือตามความเหมาะสมเป็นกรณี ๆ ไป

5.2 ผู้ดูแลระบบใช้เพื่อแจ้งเตือนหรือแจ้งข่าวที่เกี่ยวข้องกับความมั่นคงปลอดภัยหรือการรักษาประสิทธิภาพของระบบคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

5.3 ผู้ใช้งานใช้เพื่อส่งข้อมูลหรือเผยแพร่ข่าวสารประชาสัมพันธ์เพื่อการดำเนินงานตามภารกิจหรือสิทธิประโยชน์ต่าง ๆ ที่ควรทราบ

6. การระงับ/เพิกถอน บัญชีผู้ใช้งาน e-Mail

6.1 ผู้ดูแลระบบสามารถระงับบัญชีผู้ใช้งาน e-Mail นั้นได้ หากผู้ใช้งานพ้นสภาพจากการสังกัดกรมกิจการผู้สูงอายุ

6.2 ผู้ใช้งานสามารถร้องขอการขยายสิทธิ์การใช้งานบัญชีผู้ใช้ได้ เพื่อคงสิทธิ์เดิมไว้เมื่อต้องพ้นสภาพจากการสังกัดกรมกิจการผู้สูงอายุ โดยยื่นคำร้องส่งถึงผู้ดูแลระบบ

6.3 ผู้ดูแลระบบสามารถเพิกถอนบัญชีผู้ใช้งาน e-Mail ออกจากระบบได้ โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า หากตรวจพบว่าบัญชี e-Mail ของผู้ใช้งานนั้นไม่มีการใช้งานหรือความเคลื่อนไหวใด ๆ เป็นระยะเวลาเกิน 1 เดือน

6.4 ผู้ดูแลระบบสามารถระงับบัญชีผู้ใช้งาน e-Mail นั้นได้ หากได้รับแจ้งหรือตรวจพบการกระทำใดที่อาจก่อให้เกิดปัญหาความมั่นคงปลอดภัย หรือการกระทำที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง

เรื่องที่ 14
ข้อปฏิบัติในการใช้สื่อสังคมออนไลน์ (Social Media)

วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแลการเผยแพร่ข้อมูลและการเข้าถึงสื่อเครือข่ายสังคมออนไลน์ของกรมกิจการผู้สูงอายุ ตลอดจนการแสดงความคิดเห็นของบุคลากรในหน่วยงานผ่านสื่อเครือข่ายสังคมออนไลน์ให้เป็นไปอย่างถูกต้อง เหมาะสม เพื่อรักษาภาพลักษณ์ของบุคลากรและการดำเนินงานของหน่วยงานให้มีความเป็นระเบียบเรียบร้อยและเกิดประโยชน์สูงสุด ตลอดจนป้องกันมิให้เกิดการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ

2. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ รับผิดชอบในการให้บริการอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ

3. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การใช้สื่อสังคมออนไลน์ทั่วไป

1.1 หลักการและแนวปฏิบัติทั่วไป

1.1.1 กรมกิจการผู้สูงอายุ อนุญาตให้ใช้ระบบเครือข่ายสำหรับเข้าถึงสื่อสังคมออนไลน์ประเภทเว็บไซต์ที่ไม่มีเนื้อหาขัดต่อกฎหมาย ศีลธรรม และหลักจรรยาบรรณของหน่วยงาน

1.1.2 หน่วยงานภายในกรมกิจการผู้สูงอายุ บุคลากรสามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์เพื่อประโยชน์ในการเผยแพร่ประชาสัมพันธ์ที่เกี่ยวข้องกับกรมกิจการผู้สูงอายุในการติดต่อสื่อสารระหว่างกันได้ แต่ต้องแยกแยะให้ชัดเจนว่าข้อความใดเป็น “ข่าวประชาสัมพันธ์” “ความคิดเห็น” “ความคิดเห็นส่วนบุคคล” “การแลกเปลี่ยนข่าวสารส่วนตัว” “การเผยแพร่ข่าวสารเรื่องงาน” หรืออื่น ๆ และความคิดเห็นดังกล่าวควรคำนึงถึงประโยชน์สาธารณะด้วย

1.1.3 การเผยแพร่ประชาสัมพันธ์ในนามของหน่วยงาน ผู้เผยแพร่ต้องแสดงตำแหน่ง หน้าที่สังกัด ให้ชัดเจน เพื่อความน่าเชื่อถือ และเพื่อให้ผู้ที่ติดตามสามารถใช้ดุลพินิจในการติดตามได้

1.1.4 พึงระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น หรือหมิ่นประมาทบุคคลอื่น และควรใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์

1.1.5 พึงงดเว้นการโต้ตอบด้วยความรุนแรง ในกรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง การละเว้นไม่โต้ตอบจะทำให้ความขัดแย้งไม่บานปลายจนหาที่สิ้นสุดไม่ได้

1.1.6 พึงงดเว้นการใช้สื่อสังคมออนไลน์วิพากษ์วิจารณ์ ตลอดจนแสดงความคิดเห็นในเรื่องที่เป็นข้อมูลภายในหน่วยงานหรืออาจส่งผลกระทบต่อหน่วยงานได้

1.1.7 พึงใช้รูปแสดงตัวตนที่แท้จริง และพึงงดเว้นการนำรูปบุคคลอื่น รูปบุคคลสาธารณะมาแสดงว่าเป็นรูปของตนเอง

1.1.8 หน่วยงานที่สังกัด อาจใช้รูปสัญลักษณ์ เครื่องหมายแสดงสังกัดได้ แต่ต้องคำนึงถึงความเหมาะสมในการใช้งาน

1.1.9 พึงระมัดระวังข้อความที่ส่งผลกระทบต่อเด็ก สตรี หรือละเมิดสิทธิมนุษยชน

1.1.10 การใช้สื่อสังคมออนไลน์ที่แสดงสังกัดภายในหน่วยงาน ควรแจ้งให้ผู้บังคับบัญชาทราบก่อนทุกครั้ง

1.2 หลักการส่งต่อข้อมูล

1.2.1 ควรส่งข้อมูลข่าวสารเฉพาะบุคคลที่รู้จัก แสดงตัวตน ตำแหน่ง หน้าที่การงาน สถานะที่ชัดเจนเท่านั้น

1.2.2 ละเว้นการส่งข้อมูลที่เป็นข่าวลือข่าวไม่ปรากฏที่มาหรือเป็นเพียงการคาดเดา

1.2.3 งดเว้นการส่งต่อข้อความที่เกี่ยวข้องกับหน่วยงานทุกกรณี ยกเว้นข้อความนั้น ๆ เป็นที่เผยแพร่ต่อสาธารณะแล้ว

1.2.4 พึงระลึกเสมอว่าการส่งต่อข้อความที่เป็นเท็จหรือข้อความที่เจ้าของประสงค์จะกระจายข่าวเพื่อสร้างความสับสนวุ่นวายในบ้านเมืองเท่ากับตกเป็นเครื่องมือของบุคคลเหล่านั้น

1.2.5 ควรงดเว้นการส่งต่อข้อความเรื่องบุคคลเสียชีวิตเว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้ว

1.2.6 การส่งต่อข้อความเชิญชวนไปร่วมชุมนุมหรือกระทำกิจกรรมทางสังคมใด ๆ ต้องตรวจสอบข้อเท็จจริงให้แน่ชัดเสียก่อน

1.3 หลักความรับผิดชอบ

1.3.1 ควรแสดงความรับผิดชอบด้วยการขอโทษแสดงความเสียใจทันทีเมื่อรู้ว่ามีการเผยแพร่ข้อมูลที่ผิดพลาดหรือกระทบต่อบุคคลอื่น

1.3.2 กรณีการส่งต่อข้อความข่าวลือหรือข่าวเท็จ ต้องแก้ไขข้อความนั้นโดยทันที หากสามารถตรวจสอบข้อเท็จจริงได้ พึงแสดงข้อเท็จจริงให้เป็นที่ประจักษ์

1.3.3 หากพบข้อมูลที่ไม่ถูกต้องควรดำเนินการแก้ไขอย่างรวดเร็ว และแสดงให้เห็นอย่างชัดเจนว่าเป็นผู้ดำเนินการดังกล่าว

1.3.4 หากพบข้อมูลใด ๆ ที่ไม่เหมาะสม (เช่น สิ่งที่เป็นลิขสิทธิ์ของผู้อื่นหรือการแสดงความคิดเห็นที่เป็นการหมิ่นประมาท) ควรดำเนินการอย่างรวดเร็วโดยลบข้อความดังกล่าวออกทันทีเพื่อลดโอกาสที่จะเกิดข้อขัดแย้งทางกฎหมาย และผลกระทบด้านลบต่อหน่วยงาน

1.4 การพบข้อร้องเรียนและประเด็นขัดแย้ง หากพบเห็นข้อร้องเรียนหรือการบิดเบือนข้อเท็จจริงเกี่ยวกับบริการอิเล็กทรอนิกส์ของหน่วยงานหรือพบเห็นข้อร้องเรียนอื่น ๆ ที่เกี่ยวข้องกับหน่วยงาน ควรหลีกเลี่ยงการถกเถียงหรือโต้ตอบ ซึ่งนำไปสู่การกระตุ้นให้เกิดอารมณ์รุนแรง และพาดพิงไปยังผู้อื่น

1.5 การไม่เปิดเผยข้อมูลที่เป็นความลับ การพูดคุยแลกเปลี่ยนกับชุมชนออนไลน์ รวมถึงการโพสต์ข้อความที่เกี่ยวข้องกับงานประจำ เป็นสิ่งที่บุคคลสามารถกระทำได้ ถ้าไม่ขัดต่อหลักจรรยาบรรณของหน่วยงาน เว้นแต่ข้อมูลนั้นเป็นข้อมูลที่มีความสำคัญหรือเป็นความลับของหน่วยงาน ซึ่งห้ามเปิดเผยโดยเด็ดขาด เช่น รายละเอียดของโครงการงบลงทุนข้อมูล สำคัญทางการเงิน งานวิจัย เป็นต้น

1.6 ความน่าเชื่อถือของข้อมูล ไม่โพสต์ข้อความที่เป็นเท็จหรือก่อให้เกิดความเข้าใจผิด และระบุที่มาของข้อมูลนั้นอย่างชัดเจน การโพสต์ข้อความใด ๆ ควรพิจารณาเนื้อหาอย่างรอบคอบและระมัดระวัง โดยเฉพาะการเปิดเผยข้อมูลส่วนบุคคล

1.7 ไม่ละเมิดกฎหมายลิขสิทธิ์และทรัพย์สินทางปัญญา ไม่ละเมิดกฎหมายลิขสิทธิ์การใช้งานใด ๆ ที่เป็นลิขสิทธิ์ของผู้อื่น รวมทั้งของหน่วยงานเอง ทั้งนี้ การอ้างอิงคำพูดหรือข้อมูลของผู้อื่น ควรใช้ข้อความที่คัดลอกมาสั้น ๆ เท่านั้น และควรระบุถึงที่มาของแหล่งข้อมูลหรือเจ้าของผลงานเสมอ การเชื่อมลิงก์ไปยังงานของเจ้าของข้อมูล ถือเป็นการปฏิบัติที่เหมาะสมกว่าการคัดลอกข้อมูลมาใช้งาน

1.8 คำนึงถึงผู้เข้าชมและผู้เกี่ยวข้อง บุคลากรของหน่วยงานไม่ควรโพสต์ข้อมูลใด ๆ ที่ขัดแย้งกับข้อกำหนดของหน่วยงาน รวมถึงละเว้นการแสดงออกถึงความคิดเห็นที่ก้าวร้าว หมิ่นประมาท ดูถูกเป็นการส่วนตัว ลามกอนาจาร และอื่น ๆ ที่ไม่เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วยุหรือขัดต่อจริยธรรม เช่น การเมือง ศาสนา ชนชาติ เป็นต้น การแสดงความคิดเห็นต่าง ๆ ที่โพสต์โดยบุคลากรของหน่วยงานโดยที่ไม่ได้รับมอบหมายอย่างเป็นทางการ ถือเป็นการแสดงความเห็นส่วนบุคคลเท่านั้น ไม่ได้เป็นความคิดเห็นอย่างเป็นทางการของหน่วยงาน

1.9 การปกป้องผู้มีส่วนได้ส่วนเสีย หน่วยงานพันธมิตร และผู้มีส่วนเกี่ยวข้อง ไม่ควรอ้างอิงหรือเปิดเผยถึงข้อมูลผู้มีส่วนได้ส่วนเสีย และหน่วยงานพันธมิตร ตลอดจนผู้มีส่วนเกี่ยวข้องอย่างเปิดเผยก่อนได้รับอนุญาต และไม่พาดพิงถึงรายละเอียดที่เป็นความลับเกี่ยวกับข้อผูกพันกับผู้มีส่วนได้ส่วนเสีย ทั้งนี้ ควรพึงระวังการใช้งานเครือข่ายสังคมออนไลน์เป็นเครื่องมือในการทำธุรกรรมทางการค้ากับผู้มีส่วนได้ส่วนเสีย หน่วยงานพันธมิตร รวมถึงผู้มีส่วนเกี่ยวข้องกับหน่วยงาน

1.10 การคำนึงถึงผลกระทบจากการใช้งาน คำนึงถึงผลกระทบของการโพสต์ข้อความในเว็บบล็อคส่วนตัว โดยเฉพาะข้อความที่อาจจะก่อให้เกิดความขัดแย้งกับหน่วยงาน ดังนั้น จึงควรระมัดระวังในการถูกนำข้อความในเว็บบล็อคส่วนตัวมาเป็นข้อมูลอ้างอิง

1.11 การคำนึงถึงผลกระทบต่อการปฏิบัติงาน การใช้สื่อเครือข่ายสังคมออนไลน์จะต้องไม่รบกวนการปฏิบัติงานหรือหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

1.12 การฝ่าฝืนและบทลงโทษ

1.12.1 หน่วยงานไม่รับผิดชอบต่อผลของการกระทำที่เกิดจากผู้ใช้งาน และ/หรือบัญชีผู้ใช้งานที่ฝ่าฝืนต่อนโยบายนี้

1.12.2 หากหน่วยงานตรวจสอบแล้วพบว่าบัญชีผู้ใช้งานใดละเมิดต่อนโยบายนี้ หน่วยงานขอสงวนสิทธิ์ในการระงับ และ/หรือยกเลิกบัญชีผู้ใช้งานอินเทอร์เน็ต และ/หรือหยุดให้บริการแก่ผู้ใช้งานนั้น

1.12.3 หากการกระทำอันฝ่าฝืนต่อนโยบายนี้เป็นความผิดตามกฎหมายให้หน่วยงานดำเนินคดีตามกฎหมายโดยลำดับต่อไป

2. การใช้สื่อสังคมออนไลน์ในระดับบุคคล

การนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรในหน่วยงานมีข้อปฏิบัติดังนี้

2.1 กรณีใช้ชื่อบัญชีผู้ใช้งาน (user account) ที่ระบุถึงต้นสังกัด ผู้ใช้งานพึงใช้ความระมัดระวังในการปฏิบัติตามข้อบังคับจริยธรรม หลักเกณฑ์ และข้อปฏิบัติของหน่วยงานตามที่ได้ระบุไว้ โดยเฉพาะความถูกต้อง และการใช้ภาษาที่เหมาะสม

2.2 กรณีใช้ชื่อบัญชีผู้ใช้งานที่ระบุถึงตัวตนอันอาจทำให้ผู้ติดตาม (followers) หรือเพื่อนในเครือข่าย (friends) เข้าใจได้ว่าเป็นบุคลากรในหน่วยงาน ผู้ใช้งานพึงระมัดระวังการนำเสนอข้อมูลข่าวสารและการแสดงความคิดเห็นที่อาจนำไปสู่การละเมิดจริยธรรมของผู้อื่น

2.3 ในการรวบรวมข้อมูลข่าวสารการนำเสนอและการแสดงความคิดเห็นผู้ใช้งาน พึงระวังการละเมิดสิทธิส่วนบุคคล ศักดิ์ศรีความเป็นมนุษย์ สิทธิเด็กและสตรี ภาพลามกอนาจาร

2.4 หากการนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรในหน่วยงานเกิดความผิดพลาดจนก่อให้เกิดความเสียหายต่อบุคคลหรือหน่วยงานอื่น ผู้ใช้งานต้องดำเนินการแก้ไขข้อความที่มีปัญหาโดยทันที พร้อมทั้งแสดงถ้อยคำขอโทษต่อบุคคลหรือหน่วยงานที่ได้รับความเสียหาย ทั้งนี้ ต้องให้ผู้ที่ได้รับความเสียหายได้มีโอกาสชี้แจงข้อมูลข่าวสารในด้านของตนด้วย

3. การใช้สื่อสังคมออนไลน์ในระดับหน่วยงาน

3.1 การจัดทำสื่อสังคมออนไลน์ในระดับหน่วยงานควรที่จะคำนึงถึงหลักการพื้นฐานและวัตถุประสงค์ของการจัดทำแนวทางการใช้งานสื่อสังคมออนไลน์เพื่อช่วยพัฒนาและดำเนินงานของหน่วยงาน

3.2 การนำเสนอข่าวโดยการใช้สื่อสังคมออนไลน์ของหน่วยงาน ควรมีหลักในการอ้างอิงถึงหน่วยงานดังต่อไปนี้

3.2.1 ชื่อหน่วยงานที่เผยแพร่ข้อมูลข่าวสาร

3.2.2 รายละเอียด สัญลักษณ์ หรือชื่อย่อ ที่แสดงถึงหน่วยงาน

3.2.3 มาตรการทางเทคนิคที่ยืนยันถึงสถานะและความมีตัวตนของหน่วยงาน (ถ้ามี)

3.2.4 ชื่อตัวแทนหน่วยงานที่นำเสนอข่าวสาร (ถ้ามี)

3.3 การปกป้องข้อมูลที่เป็นความลับของหน่วยงาน ในกรณีที่มีบัญชีผู้ใช้งานของหน่วยงาน ควรมีการตั้งค่าความเป็นส่วนตัว (Privacy) เพื่อป้องกันไม่ให้บุคคลอื่นโพสต์ข้อความหรือเข้าถึงข้อมูลที่มีความสำคัญหรือเป็นความลับของหน่วยงานซึ่งห้ามเปิดเผยโดยเด็ดขาด เช่น รายละเอียดของโครงการงบลงทุน ข้อมูลสำคัญทางการเงิน งานวิจัย เป็นต้น โดยมีการกำหนดให้อยู่ในวงจำกัดเท่านั้น และควรให้ความระมัดระวังในการโพสต์ข้อความเฉพาะกลุ่มหรือส่วนบุคคลที่ไม่ต้องการเผยแพร่ให้สาธารณชนรับรู้

3.4 การนำเสนอข้อมูลข่าวสารของหน่วยงานผ่านสื่อสังคมออนไลน์ ควรเป็นไปตามข้อบังคับจริยธรรม หลักเกณฑ์ และข้อปฏิบัติของหน่วยงานตามที่ได้ระบุไว้ และต้องไม่เป็นการสร้างความเกลียดชังระหว่างคนในชาติจนอาจนำไปสู่ความขัดแย้งและเสียหายรุนแรงขึ้นในสังคม

3.5 หน่วยงานต้องให้ความเคารพและยอมรับข้อมูลข่าวสารหรือภาพข่าวที่ผลิตโดยบุคคลอื่นผ่านสื่อสังคมออนไลน์ การคัดลอกข้อความใด ๆ จากสื่อสังคมออนไลน์พึงได้รับการอนุญาตจากเจ้าของข้อความนั้น ๆ ตามแต่กรณีจำเป็นเพื่อประโยชน์ในการเผยแพร่ข้อมูลข่าวสาร ต้องอ้างอิงถึงแหล่งที่มาของข้อความและข่าวสารนั้น โดยรับรู้ถึงสิทธิหรือลิขสิทธิ์ของหน่วยงานหรือบุคคลผู้เป็นเจ้าของข้อมูลดังกล่าว

3.6 หลีกเลี่ยงการสื่อสาร ควรหลีกเลี่ยงการสื่อสารข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง และข้อมูลใด ๆ ของหน่วยงานหรือที่เกี่ยวข้องกับหน่วยงาน ที่ก่อให้เกิดความขัดแย้งหรือโต้แย้งในสังคม ขัดต่อหลักกฎหมายทั้งในประเทศและในระดับสากล หรือการเสนอเรื่องราวตลก ไร้สาระ เพ้อฝัน ไร้ศีลธรรม เกินความจริง ไม่ให้เกียรติ ดูถูกเหยียดหยาม และลอกเลียนแบบผู้อื่น

3.7 ไม่เผยแพร่ข้อมูลที่เป็นความลับของหน่วยงาน ไม่นำข้อมูลที่เป็นความลับทุกระดับชั้นของหน่วยงานมาเผยแพร่ผ่านสื่อสังคมออนไลน์ทุกประเภท

3.8 การเผยแพร่ข้อมูลส่วนบุคคลที่อยู่ในความรับผิดชอบของหน่วยงานบนช่องทางสาธารณะให้ตระหนักถึงความเสี่ยงและดำเนินการป้องกัน รวมถึงระมัดระวังการเผยพร่เอกสารที่มีข้อมูลส่วนบุคคล

4. การใช้งานเครื่องคอมพิวเตอร์และเครือข่าย

4.1 ห้ามนำข้อมูลส่วนตัวที่ไม่เกี่ยวข้องกับงานของหน่วยงานมาเก็บไว้ในเครื่องคอมพิวเตอร์ของหน่วยงาน

4.2 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขายหรือเผยแพร่สิ่งที่ผิดกฎหมาย การตั้งกระทู้หรือตอบกระทู้บนกระดานถาม-ตอบ หรือบนเว็บไซต์ประเภท Social network หรือบริการบล็อค (Blog) เพื่อเผยแพร่สิ่งที่ผิดกฎหมาย และขัดต่อศีลธรรม เป็นต้น

4.3 ห้ามเข้าใช้เครือข่ายคอมพิวเตอร์ด้วยบัญชีของผู้อื่น ทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของบัญชี

4.4 ห้ามเข้าถึงระบบคอมพิวเตอร์และข้อมูลที่มีมาตรการป้องกันการเข้าถึงของผู้อื่น เพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม เช่น มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นเข้ามาใช้เครื่องคอมพิวเตอร์หรือเข้าดูข้อมูล เป็นต้น

4.5 ห้ามเผยแพร่ข้อมูลของผู้ใช้งานหรือหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้ที่เป็นเจ้าของหรือเป็นผู้จัดทำข้อมูลนั้น ๆ

4.6 ห้ามก่อกวน ขัดขวาง ชะลอหรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของหน่วยงานและระบบเครือข่ายอื่นเกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ เพื่อให้เกิดผลชะลอการทำงาน การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์ช้าลง

4.7 ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมประเภทที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะโดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์ หรือเพื่อนำไปใช้เป็นเครื่องมือในการกระทำผิดบนเครือข่ายคอมพิวเตอร์

4.8 ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของหน่วยงานและของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์

4.9 ห้ามส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-Mail) ในรูปแบบภาพนิ่ง ภาพเคลื่อนไหว ภาพที่เกิดจากการสร้างขึ้น ตัดต่อ ดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ และข้อความที่เกี่ยวกับการลามกอนาจาร การละเมิดทรัพย์สินทางปัญหา การหมิ่นพระบรมเดชานุภาพ การสร้างปัญหาความมั่นคงของประเทศ หรือการทำให้บุคคลเสียชื่อเสียงหรือได้รับความอับอาย การปลอมแปลงหรือแอบอ้างชื่อเป็นบุคคลอื่นเพื่อสร้างความเข้าใจผิด การส่งอีเมลมากจนล้นระบบเครือข่ายคอมพิวเตอร์ของบุคคลอื่นจนทำให้เกิดความยุ่งยากในการใช้งานระบบเครือข่ายคอมพิวเตอร์

4.10 ห้ามเผยแพร่หรือเข้าถึงสื่อที่เกี่ยวกับเรื่องลามกอนาจาร การละเมิดทรัพย์สินทางปัญญา การหมิ่นพระบรมเดชานุภาพ การสร้างปัญหาความมั่นคงของประเทศ หรือการทำให้บุคคลเสียชื่อเสียงหรือได้รับความอับอาย

4.11 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์เพื่อประกอบธุรกิจการค้า หรือเปิดให้บริการใด ๆ นอกจากจะได้รับอนุญาตจากหน่วยงานหรือผู้รับผิดชอบทรัพยากรและเครือข่ายคอมพิวเตอร์

4.12 ห้ามกระทำการเคลื่อนย้าย หรือทำการใด ๆ ต่อทรัพยากรและเครือข่ายคอมพิวเตอร์ของหน่วยงานโดยพลการ นอกจากได้รับอนุญาตจากหน่วยงานหรือผู้รับผิดชอบทรัพยากรและเครือข่ายคอมพิวเตอร์

4.13 ห้ามการส่ง SMS หรือข้อความสั้น และอีเมลแนบลิงก์ให้กับประชาชน เพื่อควบคุมต้นทางของการหลอกลวงประชาชนและลดความเสียที่มีต่อประชาชน รวมทั้งแก้ปัญหาอาชญากรรมออนไลน์

4.14 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์อื่นใดที่ขัดต่อนโยบาย ระเบียบ ข้อบังคับและประกาศของหน่วยงาน

5. การใช้งานแบนด์วิดท์เครือข่ายที่เหมาะสม

5.1 รณรงค์ให้ผู้ใช้งานเครือข่ายใช้งานระบบอีเมลที่หน่วยงานจัดให้ เนื่องจากการที่ผู้ใช้งานเครือข่ายใช้ระบบอีเมลจากภายนอก เช่น Hotmail Gmail เป็นต้น ทำให้ผู้ใช้งานนั้นต้องเชื่อมต่อเครื่องลูกข่ายของตนไปยังเครื่องแม่ข่ายภายนอก ส่งผลให้มีการใช้งานแบนด์วิดท์ของเครือข่ายหน่วยงานเป็นจำนวนมาก ทำให้เหลือแบนด์วิดท์เพื่อการใช้งานแอปพลิเคชันอื่นน้อยลง

5.2 หลีกเลี่ยงการสำรองข้อมูลขึ้นระบบ Cloud Computing หรือการดาวน์โหลดไฟล์ขนาดใหญ่ในช่วงเวลาปฏิบัติงาน กรณีตั้งค่าการสำรองข้อมูลขึ้นระบบ Cloud อัตโนมัติควรตั้งเวลาที่เหมาะสม เช่น ระหว่างเวลา 23.00 – 03.00 น. เป็นต้น

5.3 ควรใช้พร็อกซี่ (Proxy) ในการเข้าใช้งานเว็บไซต์ เนื่องจากเครื่องลูกข่ายไม่ต้องเชื่อมโยงเข้ากับเครื่องแม่ข่ายที่อยู่ระยะไกลทุกครั้งที่มีการเรียกใช้เว็บไซต์ ทำให้ลดการใช้งานแบนด์วิดท์ของเครือข่ายลงได้

5.4 หน่วยงานขอสงวนสิทธิ์ในการตรวจจับแบนด์วิดท์ของแพ็กเกจ ทั้งการจราจรขาเข้า (Inbound Traffic) และการจราจรขาออก (Outbound Traffic) ของบัญชีผู้ใช้งานโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

5.5 กรณีที่หน่วยงานตรวจสอบแล้วพบว่า บัญชีผู้ใช้งานใดมีพฤติกรรมสุ่มเสี่ยง เช่น โหลดบิต เป็นต้น หน่วยงานขอสงวนสิทธิ์ในการระงับ และ/หรือยกเลิกบัญชีผู้ใช้งานอินเทอร์เน็ต และ/หรือหยุดให้บริการแก่ผู้ใช้งานนั้น