ประกาศกรมกิจการผู้สูงอายุ

เรื่อง ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๗ กรมกิจการผู้สูงอายุ

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ประกอบกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๓ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามที่กำหนดไว้ในแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการให้เป็นไปตามนโยบายและแผนตามมาตรา ๔๒

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ ประกอบมติที่ประชุมคณะทำงานเทคโนโลยีสารสนเทศ กรมกิจการผู้สูงอายุ ครั้งที่ ๓/๒๕๖๗ ในวันที่ ๑๕ กรกฎาคม ๒๕๖๗ จึงประกาศข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๗ กรมกิจการผู้สูงอายุ มีรายละเอียดแนบท้ายประกาศนี้ ตั้งแต่บัดนี้เป็นต้นไป

จึงประกาศให้ทราบและถือปฏิบัติอย่างเคร่งครัดโดยทั่วกัน

ประกาศ ณ วันที่ ๓๑ กรกฎาคม พ.ศ. ๒๕๖๗

(นางสาวแรมรุ้ง วรวัธ)

อธิบดีกรมกิจการผู้สูงอายุ

กรมกิจการผู้สูงอายุ
Department of Older Persons

ข้อปฏิบัติ
ในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศ

พ.ศ 2567

กรมกิจการผู้สูงอายุ

สารบัญ

หน้า

บทนำ

ความเป็นมา

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน เป็นลายลักษณ์อักษร

เพื่อให้การพัฒนาระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ และการดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล รวมทั้งเพื่อป้องกันปัญหา ที่อาจจะเกิดขึ้นจากการใช้ระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อกรมกิจการผู้สูงอายุ ดังนั้น จึงเห็นสมควรกำหนดข้อปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ โดยให้ครอบคลุมการดำเนินการ ดังนี้

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(2) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้ สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ ทั้งนี้จะต้องเผยแพร่ข้อปฏิบัติฯ ดังกล่าว ให้เจ้าหน้าที่ทุกระดับใน กรมกิจการผู้สูงอายุ และผู้เกี่ยวข้องได้รับทราบและถือปฏิบัติโดยเคร่งครัด และต้องดำเนินการทบทวนปรับปรุงข้อปฏิบัติฯ ให้เป็นปัจจุบันอยู่เสมอ

องค์ประกอบของข้อปฏิบัติประกอบด้วย

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 ที่กรมกิจการผู้สูงอายุ จัดสรรให้

(3) ผู้ดูแลระบบ หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบสารสนเทศ หรือระบบเครือข่าย หรือระบบคอมพิวเตอร์

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

(5) สิทธิ์ของผู้ใช้งาน หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับ ระบบสารสนเทศของ กรมกิจการผู้สูงอายุ

(6) สินทรัพย์/สินทรัพย์สารสนเทศ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับ กรมกิจการผู้สูงอายุ เช่น เอกสาร สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์ เครื่องคอมพิวเตอร์อุปกรณ์ต่อพ่วง ระบบเครือข่าย และระบบสารสนเทศ

(7) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

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

(9) เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนข้อปฏิบัติด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(10) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของกรมกิจการผู้สูงอายุ ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(11) ระบบเครือข่าย หมายความว่า กลุ่มของคอมพิวเตอร์อุปกรณ์คอมพิวเตอร์อุปกรณ์เครือข่ายและสื่อนำสัญญาณ ที่ถูกนำมาเชื่อมต่อกัน ผ่านอุปกรณ์ด้านการสื่อสารหรือสื่ออื่นใด ซึ่งทาง (ทนส. กยผ. ผส.) เป็นผู้กำหนด และทำให้ผู้ใช้ในระบบเครือข่ายสามารถติดต่อสื่อสารแลกเปลี่ยนและใช้อุปกรณ์หรือทรัพยากรต่างๆ ของเครือข่าย ร่วมกันได้โดยเครือข่ายคอมพิวเตอร์จะครอบคลุมทั้งเครือข่ายภายในหรือแลน (Local Area Network : LAN) แลนไร้สายหรือไวเลสแลน (Wireless LAN , WLAN) และเครือข่ายวงกว้างหรือแวน (Wide Area Network : WAN) ของ กรมกิจการผู้สูงอายุ ผ่านการใช้บริการเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN)

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

(13) การใช้งานอินเทอร์เน็ต หมายความว่า การใช้บริการต่างๆ ผ่านเครือข่ายอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ

(14) คอมพิวเตอร์หมายความว่า คอมพิวเตอร์ที่มีการเชื่อมต่อเพื่อใช้งานเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต ที่กรมกิจการผู้สูงอายุ

(15) ข้อมูล หมายความว่า สิ่งที่ป้อนเข้าไปในคอมพิวเตอร์ไม่ว่าจะเป็นตัวเลข ข้อความ คำสั่ง ชุดคำสั่ง ซอฟต์แวร์แฟ้มข้อมูล หรือรายละเอียดซึ่งอาจอยู่ในรูปแบบประเภทต่างๆ

(16) รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการ ตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัย ของข้อมูลและระบบเทคโนโลยีสารสนเทศ

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

(18) ชุดคำสั่งไม่พึงประสงค์หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตาม คำสั่งที่กำหนดไว้

(19) หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานที่ กรมกิจการผู้สูงอายุ อนุญาตให้มีสิทธิ์ในการเข้าถึง และใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของ กรมกิจการผู้สูงอายุ โดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจและต้องรับผิดชอบ ในการรักษาความลับของข้อมูล หรือหน่วยงานที่ กรมกิจการผู้สูงอายุดำเนินการส่งหรือเข้าถึงข้อมูลสารสนเทศ

(20) สื่อสังคมออนไลน์ (Social Media) หมายความว่า ช่องทางหรือสื่อใดๆ ที่ใช้เผยแพร่ข้อมูลและแสดงความคิดเห็นบนโลกออนไลน์ ที่เปิดโอกาสให้ผู้ใช้สามารถสร้างสรรค์เนื้อหาได้ด้วยตนเอง เช่น บล็อคเสรี (Blog) วิกิพีเดีย (Wikipedia) พันทิป (Pantip) เว็บเครือข่ายสังคม (Social Network) ต่างๆ รวมถึงวิดีโอและการทำ Live Stream เช่น Facebook, Instragram, LinkedIn, Flickr, Snapchat, Twitter, Vine, YouTube เป็นต้น

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

ข้อตกลงและเงื่อนไข

(1) ผู้ใช้งานต้องปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ อย่างเคร่งครัดโดยไม่มีเงื่อนไข และจะอ้างว่าไม่ทราบข้อปฏิบัติฯ ดังกล่าวมิได้

(2) ห้ามผู้ใช้งานกระทำการใดๆ อันละเมิดหรือขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งาน ต้องรับรองว่า หากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรมกิจการผู้สูงอายุ

(3) ผู้ใช้งานต้องรักษาบัญชีผู้ใช้งาน (Account) ของตนเองไว้เป็นความลับเฉพาะตัว และไม่อนุญาตให้ผู้อื่นเข้าถึงระบบด้วย Account ของตนเองในทุกกรณีเพื่อป้องกันการใช้งานโดยมิชอบ

(4) ผู้ใช้งานต้องเป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้งานและการอนุญาตให้ ผู้อื่นเข้าถึงระบบด้วย Account ในนามของตนเอง โดยไม่สามารถปฏิเสธความผิดนั้นได้ เว้นแต่จะพิสูจน์ได้ว่า ผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

(5) ผู้ดูแลระบบมีสิทธิ์ระงับ เพิกถอน หรือกระทำการใดๆ ต่อการใช้งานระบบของผู้ใช้งานเพื่อความมั่นคง ปลอดภัยของระบบ โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

เรื่องที่ 1

ข้อปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดบทบาทและความรับผิดชอบของเจ้าหน้าที่ในสังกัด กรมกิจการผู้สูงอายุ ให้เป็นไปตามหน้าที่ที่ได้รับ มอบหมาย เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่น และการเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต รวมถึงกรณีที่ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กรมกิจการผู้สูงอายุ เกิดความเสียหาย หรืออันตรายใดๆ ต่อหน่วยงานหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามข้อปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. ผู้บริหาร

1.1 อธิบดีกรมกิจการผู้สูงอายุ (Chief Executive Officer : CEO)

1.2 รองอธิบดีกรมกิจการผู้สูงอายุ ที่ได้รับมอบหมายให้เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ (Department Chief Information Officer : DCIO)

2. ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.) ดังนี้

2.1 ผู้บังคับบัญชา : ผู้อำนวยการกองยุทธศาสตร์และแผนงาน

2.2 ผู้ดูแลระบบ : เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ในสังกัด กรมกิจการผู้สูงอายุ ทุกคน

ข้อปฏิบัติ

1. ผู้บริหารมีหน้าที่ความรับผิดชอบ ดังนี้

1.1 อธิบดีกรมกิจการผู้สูงอายุ (Chief Executive Officer : CEO)

1.1.1 ให้ความเห็นชอบต่อข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ

1.1.2 รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

1.2 นางพรนิภา มาสิลีรังสี รองอธิบดีกรมกิจการผู้สูงอายุ ผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูงของกรมกิจการผู้สูงอายุ (Department Chief Information Officer : DCIO)

1.2.1 กำหนดให้มีการจัดทำและทบทวนหรือปรับปรุงข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ

1.2.2 กำหนดให้ผู้รับผิดชอบและผู้เกี่ยวข้อง มีการดำเนินงานตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ

1.2.3 กำหนดให้มีการตรวจสอบตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐหรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก

1.2.4 กำหนดให้มีการบริหารจัดการทรัพยากรอย่างเพียงพอต่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ ในแต่ละปีงบประมาณ

2. ผู้ดูแลระบบมีหน้าที่ความรับผิดชอบ ดังนี้

2.1 ผู้บังคับบัญชา : รองอธิบดีกรมกิจการผู้สูงอายุ ผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูงของกรมกิจการผู้สูงอายุ (Department Chief Information Officer : DCIO)

2.1.1 กำกับดูแลการจัดทำและทบทวนหรือปรับปรุงข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ และนโยบายสนับสนุนต่างๆ

2.1.2 กำหนดมาตรการและกำกับติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นไปตาม

2.2 ผู้ดูแลระบบ : เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ที่ได้รับมอบหมาย

2.2.1 จัดทำบัญชีสินทรัพย์สารสนเทศของอุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย และรายการระบบสารสนเทศให้ถูกต้อง และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.2.2 เก็บรักษาอุปกรณ์บริหารจัดการเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ในพื้นที่ศูนย์ปฏิบัติการ ระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

2.2.3 ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่าย ช่องทางการสื่อสารของระบบเครือข่ายและปิดช่องทาง การสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งาน

2.2.4 ดูแลรักษาและตรวจสอบการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย ให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันทีดังนี้

(1) กรณีเกิดจากการใช้งานของผู้ใช้งาน ที่ไม่เป็นไปตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ ให้รีบแจ้งผู้ใช้งานนั้นยุติการกระทำในทันที

(2) กรณีจำเป็น เพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นต่อ กรมกิจการผู้สูงอายุ ให้ผู้ดูแลระบบ พิจารณาระงับการใช้งานของผู้ใช้งานดังกล่าวทันที

2.2.5 ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย และโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดี (Malware) ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

2.2.6 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของกรมกิจการผู้สูงอายุ เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้งาน นับตั้งแต่เริ่มใช้งาน และต้องเก็บรักษาไว้

อย่างครบถ้วน ถูกต้อง ตามระยะเวลาที่กฎหมายกำหนด นับตั้งแต่การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจร ทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย

2.2.7 กำหนดสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของผู้ใช้งานให้สามารถ ใช้งานได้ตามภารกิจและสิทธิ์ที่ได้รับ

2.2.8 ทบทวนและปรับปรุงบัญชีผู้ใช้งานตามสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

2.2.9 ควบคุมและตรวจสอบการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของผู้ใช้งาน ให้เป็นไปตาม

2.2.10 ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งาน โดยไม่มีเหตุผลอันสมควร

2.2.11 ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่ง บุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

2.2.12 ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือมีข้อมูล ส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

2.2.13 คืนสินทรัพย์สารสนเทศที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนโดยทันทีที่พ้นจากหน้าที่ให้กับ ผู้อำนวยการกองยุทธศาสตร์และแผนงานหรือผู้ที่ได้รับมอบหมาย เพื่อตรวจสอบการคืนสินทรัพย์สารสนเทศนั้น

3. ผู้ใช้งานมีหน้าที่ความรับผิดชอบ ดังนี้

เป็นผู้เข้าถึงและใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่าย และระบบสารสนเทศของกรมกิจการผู้สูงอายุ ตามสิทธิ์ที่ได้รับอนุญาต โดยต้องปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ อย่างเคร่งครัด ดังนี้

3.1 การใช้งานรหัสผ่าน (Password Use)

3.1.1 ควรตั้งรหัสผ่านโดยมีความยาวอย่างน้อย 12 ตัวอักษร

3.1.2 ควรตั้งรหัสผ่านที่ประกอบด้วย ตัวอักษรที่เป็นตัวพิมพ์ปกติตัวพิมพ์ใหญ่ตัวเลขและอักขระพิเศษ

3.1.3 ควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วย อักขระที่เรียงกัน เช่น 123, abcd หรือกลุ่มของตัวอักขระที่เหมือนกันเช่น 111, aaa เป็นต้น

3.1.4 ควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

3.1.5 ควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

3.1.6 ไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

3.1.7 ควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีในครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบ

3.1.8 ควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

3.1.9 ควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด หรืออย่างน้อยทุกๆ 3 เดือน

3.1.10 ควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

3.1.11 ไม่ควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่ผู้อื่นมองเห็นได้ง่าย

3.1.12 ไม่เปิดเผยรหัสผ่านของตนเองกับผู้อื่น

3.1.13 ไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

3.1.14 ไม่ควรกำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเอง เมื่อทำการล็อกอินในภายหลัง

3.1.15 ควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกัน สำหรับระบบงานต่างๆ ที่ใช้งาน

3.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

3.2.1 ควรป้องกันไม่ให้ผู้อื่นเข้าใช้ระบบงาน/เครื่องคอมพิวเตอร์/เครื่องโน้ตบุ๊กของตน โดยให้ใส่รหัสผ่าน ให้ถูกต้องก่อนเข้าใช้งาน

3.2.2 ควรตั้งค่าให้มีการล็อก(Lock) หน้าจอของอุปกรณ์โดยอัตโนมัติเมื่อไม่ได้ใช้งานนานเกินกว่า 15 นาที

3.2.3 ควรออกจากระบบงาน/เครื่องคอมพิวเตอร์/เครื่องโน้ตบุ๊กที่ใช้งาน โดยทันทีเมื่อเสร็จสิ้นงาน

3.2.4 ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จสิ้น หรือไม่มีการใช้งานนานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องแม่ข่ายที่ให้บริการ

3.3 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

3.3.1 รับผิดชอบต่อสินทรัพย์ที่ กรมกิจการผู้สูงอายุ มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของตนเอง โดยต้อง บันทึกรายการสินทรัพย์ที่ผู้ใช้งานรับผิดชอบ และตรวจสอบทุกครั้งเมื่อมีการรับหรือคืนสินทรัพย์โดยเจ้าหน้าที่ ที่ได้รับมอบหมายของหน่วยงาน

3.3.2 มีสิทธิ์ใช้สินทรัพย์ที่ กรมกิจการผู้สูงอายุ จัดเตรียมไว้ให้เพื่อการใช้งานเท่านั้น ห้ามนำไปใช้ในกิจกรรมที่ กรมกิจการผู้สูงอายุ ไม่ได้กำหนด โดยหากเกิดความเสียหายต่อหน่วยงาน จากการละเมิดดังกล่าวให้ถือว่าเป็นความผิดส่วนบุคคล และผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นนั้น

3.3.3 หากสินทรัพย์เกิดการชำรุดหรือสูญหายจากความประมาทของผู้ใช้งาน ผู้ใช้งานต้องชดใช้ค่าเสียหาย ตามมูลค่าสินทรัพย์นั้น

3.3.4 กรณีที่ต้องทำงานนอกสถานที่ ผู้ใช้งานจะต้องดูแลและรับผิดชอบต่อสินทรัพย์ของกรมกิจการผู้สูงอายุ ที่อยู่ในความรับผิดชอบเป็นอย่างดี

3.3.5 ห้ามให้ผู้อื่นยืมสินทรัพย์ไม่ว่ากรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

3.3.6 ห้ามติดตั้งซอฟต์แวร์คอมพิวเตอร์ใดๆ ลงบนเครื่องคอมพิวเตอร์หากจำเป็นต้องติดตั้งจะต้อง แจ้งให้ (ทนส. กยผ. ผส.) ทราบ

3.3.7 ไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์ก่อนได้รับอนุญาต และต้องไม่ใช้หรือลบแฟ้มข้อมูล ของผู้อื่น ไม่ว่ากรณีใดๆ

3.3.8 หากจะนำอุปกรณ์สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์/USB ไปให้ผู้อื่นใช้งานต่อ จะต้องทำลายข้อมูล สำคัญในอุปกรณ์ก่อน โดยใช้วิธีการลบหรือการเขียนทับข้อมูลเดิมหลายรอบ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

3.3.9 หากจำเป็นต้องทำลายอุปกรณ์สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์ ให้ดำเนินการตามมาตรการ ดังนี้

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 ของกระทรวงกลาโหม สหรัฐอเมริกา ว่าด้วยการลบข้อมูลในฮาร์ดดิสก์ 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) ในการลบ แฟ้มข้อมูล/ไฟล์ข้อมูล โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://eraser.heidi.ie/download.php 2. ทำลายด้วยวิธีการทุบหรือบดให้เสียหาย
USB	ใช้ USB อย่างปลอดภัย จำกัดหรือห้ามการใช้ USB ที่ไม่ได้รับการอนุญาต การใช้ USB ต้องปฏิบัติตามมาตราฐานการรักษาความปลอดภัยที่ได้รับการกำหนดและจะต้องมีการตรวจสอบและควบคุมเพื่อรักษาความปลอดภัยของระบบและข้อมูลอย่างสม่ำเสมอ

3.3.10 มีส่วนร่วมในการบำรุงรักษาโปรแกรมป้องกันไวรัสที่ใช้โดยตรวจสอบว่า มีการ Update โปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้กลุ่มเทคโนโลยีสารสนเทศ กยผ. ผส. ทราบหากไม่สามารถ Update โปรแกรมป้องกัน ไวรัสให้ทันสมัยได้

3.3.11 สำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้เช่น บนแผ่น CD หรือ DVD หรือ Flash Drive หรือ Memory Card เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

3.3.12 ไม่ปรับแต่งหรือยกเลิกการทำงานของโปรแกรมป้องกันไวรัส ที่กลุ่มเทคโนโลยีสารสนเทศ กยผ. ผส. ติดตั้งให้

3.3.13 แจ้งให้กลุ่มเทคโนโลยีสารสนเทศ กยผ. ผส. ทราบทันทีเมื่อพบว่าคอมพิวเตอร์หรือโปรแกรมที่ใช้มีความผิดปกติหรือเมื่อสงสัยว่า มีการติดไวรัส

3.3.14 ตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นด้วยโปรแกรมป้องกันไวรัสทุกครั้งเมื่อมีการนำมา ติดตั้งหรือใช้งาน และหากตรวจพบไวรัสจะต้องจัดการทำลายไวรัสโดยเร็วที่สุด

3.3.15 หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมที่นำมาใช้งานได้ ห้ามผู้ใช้งานทำการ เปิดข้อมูลหรือติดตั้งโปรแกรมลงไปบนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เด็ดขาด

3.3.16 หากต้องการนำเครื่องคอมพิวเตอร์มาใช้งานภายใต้ระบบเครือข่ายของ กรมกิจการผู้สูงอายุ จะต้องติดตั้ง ซอฟต์แวร์ป้องกันไวรัสที่เครื่องคอมพิวเตอร์ก่อน โดยซอฟต์แวร์นั้น ต้องสามารถ Update ให้เป็นปัจจุบัน และตรวจจับ Malware อื่นๆ ได้ เช่น Spyware หากไม่มีต้องแจ้งให้(ทนส. กยผ. ผส.) ติดตั้งให้

3.3.17 การใช้งานระบบเครือข่ายของ กรมกิจการผู้สูงอายุ ผู้ใช้งานจะต้องลงทะเบียนเพื่อขอใช้งานจากผู้ดูแล ระบบก่อน โดยผู้ที่ได้รับสิทธิ์ให้เข้าใช้งานได้ จะได้รับบัญชีผู้ใช้งาน (Account) ซึ่งประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

3.3.18 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ก่อนเข้าใช้งานระบบเครือข่ายของกรมกิจการผู้สูงอายุ ทุกครั้ง ด้วยบัญชีผู้ใช้งาน (Account) ของตนเองเท่านั้น

3.3.19 ห้ามเข้าศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ ซึ่งเป็นพื้นที่ที่ใช้สำหรับ ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์บริหารจัดการเครือข่ายโดยเด็ดขาด เว้นแต่จะได้รับอนุญาต จากผู้ดูแลระบบ

3.3.20 ไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

3.3.21 ไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมเข้ากับระบบเครือข่ายของ กรมกิจการผู้สูงอายุ เพื่อเปิดใช้งานเอง ในหน่วยงาน หรือประกอบธุรกิจส่วนบุคคล

3.3.22 กรณีที่ผู้ใช้งานพยายามเข้าถึงระบบโดยมิชอบ หรือโจมตีระบบ หรือมีพฤติกรรมการใช้งานที่ละเมิด ต่อข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ หรือกฎหมายที่เกี่ยวข้อง ผู้ใช้งานนั้น จะถูกระงับหรือยกเลิกการใช้งานระบบเครือข่ายของ กรมกิจการผู้สูงอายุ ทันที

3.3.23 กรณีที่ผู้ใช้งานได้กระทำการใดๆ ที่มีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหาย ต่อหน่วยงานหรือผู้หนึ่งผู้ใด ผู้ใช้งานนั้นจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

3.4 นำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ

3.4.1 ประเมินข้อมูลที่จำเป็นต้องป้องกัน โดยพิจารณาตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 เพื่อระบุระดับความสำคัญและระดับความลับที่เหมาะสม

3.4.2 เลือกวิธีการเข้ารหัสที่เป็นมาตรฐานสากล มาใช้กับข้อมูลที่จำเป็นต้องป้องกัน

3.4.3 การจัดเก็บรหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ของระบบสารสนเทศลงในฐานข้อมูลใดๆ จะต้องทำการเข้ารหัสด้วยอัลกอริทึม 3DES หรือ AES ใน field ของ Password ก่อนบันทึก ลงในฐานข้อมูลทุกครั้ง

3.4.4 การเชื่อมต่อระบบสารสนเทศแบบ Web Application เพื่อส่งข้อมูลระหว่างเบราว์เซอร์และเว็บเซิร์ฟเวอร์จะต้องเชื่อมต่อโดยการเข้ารหัส (SSL) ผ่านโปรโตคอล HTTPS

3.4.5 กำหนดช่องทางที่เหมาะสม ในการรับ - ส่งข้อมูลสำคัญหรือข้อมูลลับ ดังนี้

(1) ระบบเครือข่ายแบบ LAN

(2) ระบบเครือข่ายแบบไร้สาย หรือ Wireless LAN

(3) สื่อบันทึกข้อมูล/สื่ออิเล็กทรอนิกส์ที่สามารถถอดแยกจากตัวเครื่องคอมพิวเตอร์ได้

3.4.6 กำหนดวิธีการบริหารจัดการและการใช้งานกุญแจสำหรับการเข้ารหัส ดังนี้

(1) กำหนดผู้รับผิดชอบเพื่อทำหน้าที่เกี่ยวกับการเข้ารหัส เช่น การสร้างกุญแจ การควบคุมและดูแลกุญแจ การทำลายกุญแจ การใช้งานกุญแจ และการจัดการกรณีกุญแจเกิดการสูญหาย

(2) กำหนดวิธีการป้องกันกุญแจที่ใช้สำหรับการเข้ารหัส

(3) กำหนดวิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจเกิดการสูญหายหรือถูกทำให้เสียหาย

3.4.7 ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับหรือวิธีการรักษาความลับของข้อมูล ดังนี้

(1) แสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

(2) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ด้วยวิธีการเข้ารหัสตามมาตรฐานที่กรมกิจการผู้สูงอายุ กำหนด

(3) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ด้วยการกำหนดรหัสผ่านให้กับไฟล์ข้อมูลลับนั้น

3.4.8 ห้ามแชร์ไฟล์ข้อมูลลับบนระบบเครือข่ายของ กรมกิจการผู้สูงอายุ เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

3.4.9 ตรวจสอบการทำงานของระบบป้องกันไวรัสในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูล อย่างสม่ำเสมอเพื่อให้สามารถป้องกันไวรัสได้ตามปกติ

3.4.10 ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ ของซอฟต์แวร์หรือไม่

3.4.11 สำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

เรื่องที่ 2

ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

เพื่อเป็นมาตรการในการควบคุม ป้องกัน และรักษาความมั่นคงปลอดภัยเกี่ยวกับสถานที่ที่เป็นที่ตั้งและพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ปฏิบัติที่มีส่วนเกี่ยวข้อง กับการใช้งานระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ของ กลุ่มเทคโนโลยีสารสนเทศ กยผ. ผส. ที่ได้รับมอบหมายหรือที่มีสิทธิ์ในการเข้าออกพื้นที่

3. ผู้มาติดต่อ หมายถึง เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มาติดต่อขอเข้าถึงหรือใช้ข้อมูล หรือทรัพย์สินต่างๆ ภายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. ทนส. กยผ. ผส. มีหน้าที่ความรับผิดชอบ ดังนี้

1.1 กำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

1.1.1 กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ ให้ชัดเจน โดยสามารถแบ่งแยกได้เป็น พื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ พื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) และพื้นที่ติดตั้ง อุปกรณ์กระจายสัญญาณเครือข่าย (Access Network Area) เป็นต้น

1.1.2 จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ และประกาศ ให้รับทราบโดยทั่วกัน

1.2 ควบคุมสินทรัพย์สารสนเทศ

1.2.1 พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

(1) มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ

(2) ผนังล้อมรอบศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ ควรสร้างเป็นผนังทึบ

(3) ประตูหรือทางเข้าพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ ต้องออกแบบเพื่อป้องกัน การบุกรุกทางกายภาพ

(4) ประตูหรือทางเข้าของศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ ต้องมีระบบที่สามารถล็อกได้เพื่อป้องกันการบุกรุกทางกายภาพ

(5) ให้เจ้าหน้าที่ที่ปฏิบัติงานภายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ ของกรมกิจการผู้สูงอายุ ต้องปิดประตูและหน้าต่างให้ล็อกอยู่เสมอ ภายหลังเลิกงาน และนอกเวลาราชการ

1.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน

(1) ติดตั้งระบบและอุปกรณ์สนับสนุนการทำงานที่เพียงพอต่อความต้องการใช้งาน ภายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ เช่น ระบบปรับอากาศระบบควบคุมอุณหภูมิและความชื้น ระบบไฟฟ้าสำรอง ระบบดับเพลิง ระบบควบคุมการเข้าถึงระบบเทคโนโลยี สารสนเทศ (Access Control) หรืออุปกรณ์ที่สามารถป้องกันภัยคุกคามจากผู้บุกรุก และกล้องวงจรปิด (CCTV) เป็นต้น

(2) มีการใช้ระบบไฟฟ้าสำรองกับระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้า และต้องทดสอบระบบไฟฟ้าสำรองอย่างสม่ำเสมอ

(3) มีการตรวจสอบหรือทดสอบระบบและอุปกรณ์สนับสนุนการทำงานอย่างสม่ำเสมอ เพื่อให้มั่นใจ ได้ว่าระบบทำงานได้ตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(4) มีการดูแลและบำรุงรักษาระบบและอุปกรณ์สนับสนุนการทำงานอย่างถูกต้องและสม่ำเสมอ โดยจัดให้มีการบำรุงรักษาอุปกรณ์อย่างน้อยปีละ 1 ครั้ง

1.2.3 การป้องกันอุปกรณ์

(1) แยกเก็บอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่ง เพื่อดูแลความมั่นคงปลอดภัย

(2) มีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอนหรือไฟฟ้ากระชาก

(3) มีการตรวจสอบ สอดส่อง ระดับอุณหภูมิและดูแลสภาพแวดล้อมภายในบริเวณพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ เพื่อป้องกันความเสียหายต่ออุปกรณ์

(4) ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ ภายในบริเวณพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่าย และเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ

(5) มีการกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศทุกครั้ง เมื่อว่างเว้นจากการใช้งาน

2. เจ้าหน้าที่มีหน้าที่ความรับผิดชอบ ดังนี้

2.1 ควบคุมการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ

2.1.1 จัดทำคู่มือ/คำแนะนำ/วิธีปฏิบัติในการเข้าออกพื้นที่ และต้องประกาศให้รับทราบโดยทั่วกัน

2.1.2 จัดให้มีระบบจัดเก็บบันทึกการเข้าออกพื้นที่

2.1.3 จัดทำแบบบันทึกการเข้าออกพื้นที่ โดยต้องระบุรายละเอียดอย่างน้อย ดังนี้ชื่อ - นามสกุล ตำแหน่ง หน่วยงาน ประเภทสิทธิ์ เครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับสิทธิ์ รายละเอียดกิจกรรมและระยะเวลา ดำเนินการ

2.1.4 จัดทำบัตรผู้มาติดต่อ (Visitor) และให้ผู้มาติดต่อแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ หรือบัตรอนุญาตเข้าออกภายในอาคารที่ได้แลกมาก่อนหน้า เป็นต้น ในการเข้าออกพื้นที่

2.1.5 ให้ผู้มาติดต่อติดบัตรผู้มาติดต่อ (Visitor) ตรงจุดที่สามารถมองเห็นได้ชัดเจน ตลอดเวลาที่อยู่ภายในพื้นที่

2.1.6 รับคืนบัตรจากผู้มาติดต่อ (Visitor) โดยต้องตรวจสอบผู้มาติดต่อและอุปกรณ์ที่ได้รับสิทธิ์ทุกครั้ง หลังเลิกใช้งาน พร้อมลงบันทึกเวลาออกและรายการอุปกรณ์ในแบบบันทึกการเข้าออกพื้นที่ให้ถูกต้อง รวมทั้ง บันทึกลงในระบบจัดเก็บบันทึกการเข้าออกพื้นที่ไว้ด้วย

2.1.7 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้มาติดต่อ มีความจำเป็นต้องเข้าออกพื้นที่ หรือมิได้ขอสิทธิ์ในการเข้าออก พื้นที่ไว้ล่วงหน้า เจ้าหน้าที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนอนุญาต และจดบันทึกการเข้าออกพื้นที่ ไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่ โดยเจ้าหน้าที่จะต้องอยู่กับบุคคลที่มาติดต่อ ตลอดเวลาและต้องควบคุมอย่างเข้มงวด

2.1.8 กำกับและดูแลให้ผู้มาติดต่อปฏิบัติตามคู่มือ/คำแนะนำ/วิธีปฏิบัติในการเข้าออกพื้นที่อย่างเคร่งครัด

2.1.9 ตรวจสอบแบบบันทึกการเข้าออกพื้นที่เป็นประจำทุกวันหรือทุกครั้งที่มีการเข้าออก

2.1.10 ตรวจสอบประวัติการเข้าออกพื้นที่เป็นประจำอย่างน้อยเดือนละ 1 ครั้ง

2.2 กำหนดสิทธิ์การเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ

2.2.1 กำหนดสิทธิ์ของแต่ละบุคคลตามลำดับความสำคัญ โดยสิทธิ์นั้นต้องได้รับการอนุมัติจากผู้อำนวยการ กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ หรือเจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมาย เป็นลายลักษณ์อักษร

2.2.2 จัดทำแบบกำหนดสิทธิ์การเข้าออกพื้นที่ โดยต้องระบุรายละเอียดอย่างน้อยดังนี้ ชื่อ - นามสกุล ตำแหน่ง หน่วยงาน หน้าที่และความรับผิดชอบ ระยะเวลาดำเนินการ และประเภทสิทธิ์

2.2.3 กำหนดสิทธิ์/ปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ทุกครั้งที่มีการเปลี่ยนแปลง และต้องทบทวนสิทธิ์ อย่างน้อยปีละ 1 ครั้ง

2.2.4 จัดทำทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่

3. ผู้มาติดต่อมีหน้าที่ความรับผิดชอบ ดังนี้

3.1 การเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ

3.1.1 แลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ หรือบัตรอนุญาตเข้าออก ภายในอาคารที่ได้แลกมาก่อนหน้า เป็นต้น เพื่อรับบัตรผู้มาติดต่อ (Visitor) และบันทึกข้อมูลลงในแบบบันทึก การเข้าออกพื้นที่ทุกครั้งที่มีการเข้าออก

3.1.2 ติดบัตรผู้มาติดต่อ (Visitor) ตรงจุดที่สามารถมองเห็นได้ชัดเจน ตลอดเวลาที่อยู่ภายในพื้นที่

3.1.3 กรณีที่ต้องการนำอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพา หรืออุปกรณ์ เครือข่าย เข้ามาภายในบริเวณพื้นที่ จะต้องบันทึกรายการอุปกรณ์ที่นำเข้ามาลงในแบบบันทึกการเข้าออกพื้นที่ ให้ถูกต้อง

3.1.4 คืนบัตรผู้มาติดต่อ (Visitor) กับเจ้าหน้าที่ โดยเจ้าหน้าที่จะตรวจสอบผู้มาติดต่อและอุปกรณ์ พร้อมลงบันทึกเวลาออกและรายการอุปกรณ์ในแบบบันทึกการเข้าออกพื้นที่ทุกครั้งที่มีการเข้าออก

3.1.5 ปฏิบัติตามคู่มือ/คำแนะนำ/วิธีปฏิบัติในการเข้าออกพื้นที่อย่างเคร่งครัด

3.2 การเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ

3.2.1 ขออนุญาตเข้าออกพื้นที่ล่วงหน้าก่อนวันที่จะเข้าพื้นที่ โดยต้องกรอกข้อมูลความต้องการและรายละเอียดตามแบบกำหนดสิทธิ์การเข้าออกพื้นที่ที่ทาง ทนส. กยผ. ผส. กำหนด

3.2.2 ต้องได้รับอนุมัติสิทธิ์ในการเข้าออกพื้นที่ จากผู้อำนวยการกองยุทธศาสตร์และแผนงาน หรือเจ้าหน้าที่ของ ทนส. กยผ. ผส. ที่ได้รับมอบหมายก่อน จึงจะเข้าออกพื้นที่ได้

3.2.3 ผู้มาติดต่อจะถูกบันทึกรายละเอียดข้อมูลลงในทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่

เรื่องที่ 3

ข้อปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน

วัตถุประสงค์

เพื่อให้เจ้าหน้าที่ใช้เป็นมาตรการในการควบคุมและบริหารจัดการการเข้าถึงของผู้ใช้งาน โดยอนุญาตให้เฉพาะผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ เท่านั้น ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ ทนส. กยผ. ผส. ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน

1.1 เสริมเนื้อหาเพื่อสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเข้ากับหลักสูตร ฝึกอบรมต่างๆ ตามแผนการฝึกอบรมของ กรมกิจการผู้สูงอายุ

1.2 เผยแพร่ประชาสัมพันธ์และให้ความรู้ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ ในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยให้มีการปรับเปลี่ยน เกร็ดความรู้ให้ทันสมัยอยู่เสมอ

1.3 จัดฝึกอบรมผู้ใช้งานเพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กรมกิจการผู้สูงอายุ ได้อย่างถูกต้อง รวมถึงให้ตระหนักและเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานโดยไม่ระมัดระวัง

2. การลงทะเบียนผู้ใช้งาน (User Registration)

2.1 จัดเตรียมแบบฟอร์มลงทะเบียนผู้ใช้งาน ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของ กรมกิจการผู้สูงอายุ โดยต้องระบุข้อมูลพื้นฐานอย่างน้อย ดังนี้ ชื่อและนามสกุล ตำแหน่งหน่วยงาน

2.2 ตรวจสอบและให้สิทธิ์ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ ที่เหมาะสมต่อหน้าที่ความรับผิดชอบของผู้ใช้งาน

2.3 ระงับหรือเพิกถอนสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ โดยทันที เมื่อผู้ใช้งานนั้นเปลี่ยนแปลงหน้าที่ความรับผิดชอบหรือลาออก

3. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

3.1 การแจ้งขอเปลี่ยนแปลงสิทธิ์ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ จะต้องจัดทำเป็นลายลักษณ์อักษร และระบุเหตุผลความจำเป็น

3.2 กำหนดสิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ เฉพาะการปฏิบัติงาน ในหน้าที่เท่านั้น โดยต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

3.3 กำหนดระดับสิทธิ์ที่เหมาะสมในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

3.4 พิจารณามอบหมายสิทธิ์ให้สอดคล้องตามข้อปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ

3.5 กรณีจำเป็นต้องให้สิทธิ์พิเศษหรือสิทธิ์สูงสุดกับผู้ใช้งาน พิจารณา ดังนี้

3.5.1 ผู้ใช้งานนั้นต้องได้รับความเห็นชอบจากผู้อำนวยการกองยุทธศาสตร์และแผนงาน

3.5.2 กำหนดระดับการเข้าถึงและใช้งานระบบอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

3.5.3 กำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง

3.5.4 กำหนดรหัสผ่านให้ต่างจากรหัสผู้ใช้งานตามปกติและให้เปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น เปลี่ยนรหัสผ่านทุกครั้งหลังจากหมดความจำเป็นในการใช้งาน หรือหากมีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

3.6 ผู้ใช้งานต้องรับทราบสิทธิ์และปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมกิจการผู้สูงอายุ อย่างเคร่งครัด

3.7 หากตรวจพบว่าผู้ใช้งานมีการกระทำความผิดหรือละเมิดต่อข้อปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของ กรมกิจการผู้สูงอายุ เจ้าหน้าที่ต้องทำการระงับหรือเพิกถอนสิทธิ์ของผู้ใช้งานนั้นทันที

3.8 เมื่อผู้ใช้งานมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ เจ้าหน้าที่ต้องทำการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งานนั้นทันที

3.9 การเพิกถอนสิทธิ์ของผู้ใช้งานออกจากระบบ

3.9.1 กรณีเป็นเจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ ให้เพิกถอนเมื่อผู้ใช้งานนั้นมีการเปลี่ยนแปลงตำแหน่งหน้าที่ ความรับผิดชอบหรือลาออกหรือพ้นสภาพจากการเป็นเจ้าหน้าที่ของกรมกิจการผู้สูงอายุ หรือเมื่อไม่มีการเข้าใช้งาน เป็นระยะเวลาติดต่อกันเกิน 90 วัน

3.9.2 กรณีเป็นบุคคลจากหน่วยงานภายนอก ให้เพิกถอนตามวันที่ระบุในแบบฟอร์มลงทะเบียนผู้ใช้งาน หรือเมื่อไม่มีการเข้าใช้งานเป็นระยะเวลาติดต่อกันเกิน 30 วัน

4. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

4.1 กำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการคาดเดาโดยผู้อื่นและแตกต่างกัน

4.2 กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่าน ให้มีความยากต่อการคาดเดาโดยผู้อื่น

4.3 ส่งมอบรหัสผ่านให้กับผู้ใช้งานด้วยวิธีที่มีความมั่นคงปลอดภัย โดยหลีกเลี่ยงการใช้อีเมลฟรีของเอกชน เป็นช่องทางในการส่งมอบ

4.4 กำหนดขั้นตอนปฏิบัติในการบริหารจัดการรหัสผ่านของผู้ใช้งานที่มีความมั่นคงปลอดภัย ดังนี้

4.4.1 รหัสผ่านควรมีความยาวอย่างน้อย 12 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ

4.4.2 ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคล ที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

4.4.3 ผู้ใช้งานควรเปลี่ยนรหัสผ่านทุกๆ 6 เดือน หรือตามที่ผู้ดูแลระบบกำหนด

4.4.4 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานแฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านระบบเครือข่ายคอมพิวเตอร์

4.4.5 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

4.4.6 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

4.5 กรณีตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูกนำไปใช้โดยผู้อื่น ผู้ใช้งานรายนั้นจะถูกระงับสิทธิ์การใช้งานชั่วคราว จนกว่าจะดำเนินการเปลี่ยนรหัสผ่านเป็นที่เรียบร้อยแล้ว

5. การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

5.1 ทบทวนสิทธิ์และปรับปรุงบัญชีผู้ใช้งาน ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของ กรมกิจการผู้สูงอายุ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเปลี่ยนแปลง ตำแหน่งย้ายหน่วยงาน ลาออก หรือสิ้นสุดการจ้างงาน

5.2 ทบทวนสิทธิ์และปรับปรุงบัญชีผู้ใช้งาน สำหรับผู้ใช้งานที่มีสิทธิ์ในระดับสูง ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น สิทธิ์ในระดับผู้ดูแลระบบ

5.3 ตรวจสอบและติดตามการใช้งานของผู้ใช้งานตามสิทธิ์ที่ได้รับในแต่ละระบบอย่างสม่ำเสมอ

เรื่องที่ 4

ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่าย

วัตถุประสงค์

เพื่อเป็นมาตรการในการติดตั้งและกำหนดค่าต่างๆ ของระบบเครือข่ายและอุปกรณ์เครือข่าย ได้แก่ ไฟร์วอลล์ (Firewall) ระบบตรวจจับและป้องกันการบุกรุก (IDPS) การป้องกันมัลแวร์และไวรัส (Anti-Malware/ Anti-Virus)และระบบเครือข่ายไร้สาย (Wireless LAN) โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ปฏิบัติที่มีส่วนเกี่ยวข้อง กับการใช้งานระบบเครือข่ายของ กรมกิจการผู้สูงอายุ

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเครือข่ายของ กรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. ผู้ดูแลระบบมีหน้าที่ความรับผิดชอบ ดังนี้

1.1 การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

1.1.1 ติดตั้ง กำหนดค่า และบริหารจัดการไฟร์วอลล์ เพื่อกำหนดค่าต่างๆ ให้เหมาะสมตามความต้องการ ในการปฏิบัติงาน และสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย ภายในของกรมกิจการผู้สูงอายุ

1.1.2 ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น จึงจะสามารถเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ได้

1.1.3 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

1.1.4 ทุกเส้นทางที่เชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาต จะต้องถูกปฏิเสธโดยไฟร์วอลล์

1.1.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์เช่น ค่าพารามิเตอร์การกำหนดค่าใช้บริการและการเชื่อมต่อ ที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

1.1.6 สำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

1.1.7 ระบบเครื่องคอมพิวเตอร์แม่ข่ายสารสนเทศที่เข้าถึงบริการได้จากทั้งภายในและภายนอกทั้งหมด ต้องถูกติดตั้งใน Demilitarized Zone (DMZ) และต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้ง และเปิดให้บริการ

1.1.8 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อ เพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

1.1.9 ให้บริการเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายโดยอนุญาตเฉพาะพอร์ตการเชื่อมต่อ ที่จำเป็นต่อการให้บริการเท่านั้น และจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

1.1.10 ให้บริการเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์บนเครือข่าย ตามที่ได้รับอนุมัติจากผู้อำนวยการ กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ หรือเจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร โดยต้องระบุข้อมูล ดังนี้

(1) หมายเลข Port ที่ต้องการขอให้เปิด

(2) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

(3) วัตถุประสงค์หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้นๆ

(4) วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

(5) ผู้ดูแล/ผู้รับผิดชอบ/ผู้พัฒนาระบบ

1.1.11 ให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย โดยเปิดพอร์ตการเชื่อมต่อพื้นฐานของ โปรแกรมทั่วไปที่ทาง (ทนส. กยผ. ผส.) อนุญาตให้ใช้งานเท่านั้น หากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อ นอกเหนือจากที่กำหนด จะต้องได้รับการอนุมัติจากผู้อำนวยการกองยุทธศาสตร์และแผนงาน หรือเจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมายก่อน

1.1.12 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอก มายังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายภายในของ กรมกิจการผู้สูงอายุ จะต้องดำเนินการผ่าน VPN เท่านั้น และต้องได้รับการอนุมัติ จากผู้อำนวยการกองยุทธศาสตร์และแผนงาน หรือเจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมายก่อน และต้องบันทึกรายการที่ได้ดำเนินการตามที่ขอไว้ด้วย

1.1.13 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยเป็นไปตามประกาศประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔

1.1.14 ระงับการใช้งานระบบเครือข่ายและอินเทอร์เน็ต กรมกิจการผู้สูงอายุ ของเครื่องคอมพิวเตอร์ลูกข่ายทันที หากพบว่า มีพฤติกรรมการใช้งานที่ขัดต่อประกาศหรือข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่าย ของ กรมกิจการผู้สูงอายุ หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย ของระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ จนกว่าจะได้รับการแก้ไข

1.1.15 ยกเลิกการให้บริการระบบเครือข่ายและอินเทอร์เน็ต กรมกิจการผู้สูงอายุ ของผู้ใช้งานทันที หากพบว่า ผู้ใช้งานมีเจตนาใช้งานที่ขัดต่อประกาศหรือข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ กรมกิจการผู้สูงอายุ หรือกฎหมาย หรือการทำงานของโปรแกรมที่อาจทำให้เกิดความเสี่ยงต่อความปลอดภัยหรือทำให้เกิดความเสียหาย ต่อระบบเทคโนโลยีสารสนเทศของ กรมกิจการผู้สูงอายุ

1.2 การรักษาความมั่นคงปลอดภัยของระบบตรวจจับและป้องกันการบุกรุก (IDPS Policy)

1.2.1 ติดตั้ง กำหนดค่า และบริหารจัดการระบบตรวจจับและป้องกันการบุกรุก เพื่อตรวจสอบความปลอดภัยของระบบเครือข่าย และป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนระบบเครือข่ายภายใน ของ กรมกิจการผู้สูงอายุ ให้มีความมั่นคงปลอดภัย

1.2.2 ตรวจสอบ และ Update Patch/Signature ของ IDPS เป็นประจำ

1.2.3 ตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายที่มีการติดตั้ง host-based IDPS เป็นประจำทุกวัน

1.2.4 ตรวจสอบเหตุการณ์ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลที่มี การเข้าใช้งานระบบเครือข่าย เป็นประจำทุกวัน

1.2.5 บันทึกผลการตรวจสอบโฮสต์และระบบเครือข่ายทั้งหมดที่มีการส่งข้อมูลผ่าน IDPS

1.2.6 การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

1.2.7 ทำการลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ เพื่อลดความเสียหายและป้องกันเหตุการณ์ที่อาจเกิดขึ้นอีก ในอนาคต

1.2.8 จัดทำรายงานแสดงผลการตรวจสอบการบุกรุก เป็นประจำทุกเดือน

1.2.9 IDPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงระบบเครือข่ายของระบบสารสนเทศตามปกติ

1.2.10 IDPS Policy จะต้องครอบคลุมทุกโฮสต์ในระบบเครือข่ายและระบบเครือข่ายข้อมูลของกรมกิจการผู้สูงอายุ ทั้งหมด รวมถึงเส้นทางซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทางที่ข้อมูลอาจเดินทาง

1.2.11 ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะ จะต้องผ่านการตรวจสอบ จาก IDPS

1.2.12 หากตรวจพบว่าระบบมีการทำงานผิดปกติจะต้องรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมายทราบ ทันทีที่ตรวจพบ

1.2.13 หากตรวจพบว่ามีพฤติกรรมการใช้งาน หรือกิจกรรม หรือเหตุการณ์ที่น่าสงสัย ซึ่งมีความเสี่ยง ต่อการบุกรุกและการโจมตีระบบ หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องรายงานให้ผู้อำนวยการกองยุทธศาสตร์และแผนงาน หรือเจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับ มอบหมายทราบ ทันทีที่ตรวจพบ

1.2.14 ยกเลิกการเชื่อมต่อระบบเครือข่ายของเครื่องคอมพิวเตอร์ลูกข่าย ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า

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

1.3.1 จัดหาโปรแกรมบริหารจัดการระบบป้องกันไวรัสจากส่วนกลาง และโปรแกรมป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย

1.3.2 ติดตั้ง กำหนดค่า และบริหารจัดการโปรแกรมป้องกันไวรัสที่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย เพื่อป้องกันไม่ให้เกิดความเสียหายต่อข้อมูลในเครื่องคอมพิวเตอร์และระบบ

เครือข่าย อินเทอร์เน็ตของ กรมกิจการผู้สูงอายุ โดยโปรแกรมป้องกันไวรัสต้องมีคุณสมบัติตรวจจับและป้องกันไวรัส เวิร์ม โทรจัน สปายแวร์ได้เป็นอย่างน้อย

1.3.3 ติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่อง ที่มีการเชื่อมต่อกับระบบเครือข่ายของ กรมกิจการผู้สูงอายุ

1.3.4 ปรับปรุงระบบฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอ เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์เสียหาย จากไวรัสคอมพิวเตอร์

1.3.5 หากโปรแกรมป้องกันไวรัสมีการปรับเปลี่ยนรุ่น จะต้องดำเนินการปรับเปลี่ยนรุ่นตามโปรแกรมล่าสุด ให้กับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายทั้งหมด

1.3.6 หากตรวจพบหรือมีปัญหาจากไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ ลูกข่าย จะต้องตัดการเชื่อมต่อกับระบบเครือข่ายทันที และดำเนินการตรวจสอบและแก้ไขปัญหาให้แล้วเสร็จ

1.3.7 จัดทำรายงานแสดงผลการป้องกันไวรัสของระบบคอมพิวเตอร์ กรมกิจการผู้สูงอายุเป็นประจำทุกเดือน

1.4 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย (Wireless LAN Policy)

1.4.1 ติดตั้ง กำหนดค่า และบริหารจัดการระบบเครือข่ายไร้สาย เพื่อควบคุมการเข้าถึงและสร้างความมั่นคง ปลอดภัยของการใช้งานระบบเครือข่ายไร้สายของ กรมกิจการผู้สูงอายุ

1.4.2 การติดตั้งอุปกรณ์เครือข่ายไร้สายในพื้นที่ กรมกิจการผู้สูงอายุ ต้องได้รับความเห็นชอบจาก (ทนส. กยผ. ผส.) ก่อ

1.4.3 ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้น จึงจะสามารถเข้าถึงฟังก์ชันที่ใช้ในการตั้งค่าของจุดเชื่อมต่อ ระบบเครือข่ายไร้สายได้

1.4.4 จุดเชื่อมต่อระบบเครือข่ายไร้สาย จะต้องมีการกำหนดค่า Gateway ที่เป็นค่าที่กำหนดไว้ของ ระบบเครือข่ายส่วนนั้นเท่านั้น

1.4.5 ทุกจุดเชื่อมต่อระบบเครือข่ายไร้สายและอุปกรณ์ที่เกี่ยวข้อง เช่น Access Point จุดเชื่อมต่อสายสัญญาณ Switch จะต้องมีความปลอดภัย และมีรูปแบบในการจัดเก็บและเข้าถึงอุปกรณ์

1.4.6 SSID (Service Set Identifier) ที่กำหนด จะต้องถูกต้องตามรูปแบบที่ (ทนส. กยผ. ผส.) กำหนดไว้ และจะต้องไม่มีการบ่งบอกหรือแสดงตำแหน่งของสาย ที่จุดเชื่อม LAN หรือชื่ออื่นๆ

1.4.7 เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจาย สัญญาณ (Access Point) มาใช้งาน

1.4.8 SSID ที่ Broadcast จะให้บริการเฉพาะระบบเครือข่ายภายนอก ยกเว้นจุดที่ (ทนส. กยผ. ผส.) อนุญาตให้ ใช้ระบบเครือข่ายภายใน กรมกิจการผู้สูงอายุ จะต้องยกเลิกค่าการ Broadcast SSID

1.4.9 อุปกรณ์ที่ (ทนส. กยผ. ผส.) อนุญาตให้ใช้ระบบเครือข่ายภายใน กรมกิจการผู้สูงอายุ จะต้องระบุ SSID ที่ถูกต้อง จึงจะสามารถเข้าใช้งานได้

1.4.10 SNMP จะต้องถูกยกเลิกหากไม่จำเป็นสำหรับการบริหารจัดการระบบเครือข่าย หรือหากมีความจำเป็นต้องใช้จะต้องมีการเปลี่ยนแปลงค่าเริ่มต้น (Default) ของ Community String

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

1.4.12 กำหนดรายการ MAC Address ให้สามารถเข้าใช้ Access Point ได้ เฉพาะเครื่องคอมพิวเตอร์ ที่อนุญาตเท่านั้น และตามรหัสผู้ใช้ (User account) และรหัสผ่าน (User password) ที่กำหนดไว้เท่านั้น

1.4.13 ยกเลิกการเชื่อมต่อระบบเครือข่ายไร้สายของอุปกรณ์ทุกชนิด ที่ไม่เป็นไปตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ กรมกิจการผู้สูงอายุ หรือมีความเสี่ยงต่อระบบ โดยไม่ต้องมีการแจ้งให้ผู้ใช้งาน ทราบล่วงหน้า

1.4.14 ห้ามไม่ให้ผู้ดูแลระบบ บอกค่าติดตั้งของระบบเครือข่ายไร้สายกับผู้ใช้งานหรือบุคคลภายนอก

1.4.15 ระบบเครือข่ายไร้สายสำหรับให้บริการระบบอินเทอร์เน็ต จะต้องติดตั้งโดยแยกระบบเครือข่ายไร้สาย ออกจากระบบเครือข่ายภายใน LAN เพื่อป้องกันการเข้าถึงจากบุคคลภายนอก

1.4.16 หากจำเป็นต้องเชื่อมต่อระบบเครือข่ายไร้สายกับระบบเครือข่ายภายใน LAN จะต้องเลือกใช้ เทคโนโลยีAuthentication และมีการกำหนดค่าการเข้ารหัสในการเชื่อมต่อแบบ WPA2 เป็นอย่างน้อย

1.4.17 การเข้าถึงระบบเครือข่ายไร้สาย ต้องแบ่งแยกการใช้งานให้แตกต่างกันตามความจำเป็นของผู้ใช้งาน และกำหนดรหัสการเข้าใช้งานตามวัตถุประสงค์ของการใช้งาน

1.4.18 อุปกรณ์ที่ใช้ในการเข้าถึงระบบเครือข่ายของ กรมกิจการผู้สูงอายุ จะต้องรองรับมาตรฐาน IEEE 802.11g/n เป็นอย่างน้อย หากอุปกรณ์ที่ใช้เป็นเครื่องคอมพิวเตอร์ส่วนบุคคล จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัส ที่เครื่องด้วย

1.4.19 ตรวจสอบอุปกรณ์ติดตั้งการกำหนดค่าและจัดการจุดเชื่อมต่อระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

1.4.20 Wireless LAN Policy สามารถเปลี่ยนแปลงตามเทคโนโลยีใหม่ๆ และกระบวนการที่สอดคล้อง และเหมาะสมในอนาคตได้

2. ผู้ใช้งานมีหน้าที่ความรับผิดชอบ ดังนี้

2.1 ก่อนการใช้งานระบบเครือข่ายและอินเทอร์เน็ตของ กรมกิจการผู้สูงอายุ ผู้ใช้งานต้องมีการ Authentication ทุกครั้ง ด้วยรหัสผู้ใช้ (User account) และรหัสผ่าน (User password)

2.2 สำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้เช่น บนแผ่น CD หรือ DVD หรือ Flash Drive หรือ Memory Card เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

2.3 ห้ามปรับแต่งหรือยกเลิกการทำงานของโปรแกรมป้องกันไวรัส ที่ กรมกิจการผู้สูงอายุ ติดตั้งให้

2.4 มีส่วนร่วมในการบำรุงรักษาโปรแกรมป้องกันไวรัสที่ใช้โดยตรวจสอบว่า มีการ Update โปรแกรม ป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้ (ทนส. กยผ. ผส.) ทราบ หากไม่สามารถ Update โปรแกรมป้องกันไวรัส ให้ทันสมัยได้

2.5 แจ้งให้ (ทนส. กยผ. ผส.) ทราบทันทีเมื่อพบว่าคอมพิวเตอร์หรือโปรแกรมที่ใช้มีความผิดปกติ หรือเมื่อสงสัยว่า มีการติดไวรัส

2.6 ตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นด้วยโปรแกรมป้องกันไวรัสทุกครั้ง เมื่อมีการนำมาติดตั้ง หรือใช้งาน และหากตรวจพบไวรัสจะต้องจัดการทำลายไวรัสโดยเร็วที่สุด

2.7 หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมที่นำมาใช้งานได้ ห้ามทำการเปิดข้อมูลหรือติดตั้ง โปรแกรมลงไปบนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เด็ดขาด

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

2.9 กรณีที่ผู้ใช้งานพยายามเข้าถึงระบบโดยมิชอบ หรือโจมตีระบบ หรือมีพฤติกรรมการใช้งานที่ขัดต่อประกาศ หรือข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยบนเครือข่ายของ กรมกิจการผู้สูงอายุ ซึ่งอาจทำให้เกิดความเสี่ยงต่อความปลอดภัย และความเสียหายต่อระบบเทคโนโลยีสารสนเทศของกรมกิจการผู้สูงอายุ ผู้ใช้งานจะถูกระงับหรือยกเลิกการใช้งานระบบเครือข่าย และอินเทอร์เน็ตของกรมกิจการผู้สูงอายุ ทันที

2.10 กรณีที่ผู้ใช้งานได้กระทำการใดๆ ที่มีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์(ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของ กรมกิจการผู้สูงอายุ ผู้ใช้งานจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

เรื่องที่ 5

ข้อปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ ได้อย่างเหมาะสม ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน จำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนด กลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

2. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้สารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

2.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

(1) อ่านอย่างเดียว

(2) สร้างข้อมูล

(3) ป้อนข้อมูล

(4) แก้ไขข้อมูล

(5) อนุมัติ

(6) ไม่มีสิทธิ์

2.2 กำหนดเกณฑ์การระงับ/เพิกถอนสิทธิ์ ให้เป็นไปตามข้อปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งานที่ได้กำหนดไว้

2.3 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับ การพิจารณาอนุญาตจากผู้อำนวยการกองยุทธศาสตร์และแผนงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

3. กำหนดเกณฑ์ในการควบคุมการใช้งานสารสนเทศ ดังนี้

3.1 จัดแบ่งประเภทของระบบสารสนเทศ

(1) ด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลคำรับรอง ข้อมูลงบประมาณการเงินและบัญชี และข้อมูลระบบบริหารราชการ (Back Office)

(2) ด้านการให้บริการ ได้แก่ ข้อมูลผู้รับบริการทางสังคม

3.2 จัดแบ่งลำดับความสำคัญของระบบสารสนเทศ

(1) มากที่สุด

(2) ปานกลาง

(3) น้อย

3.3 จัดแบ่งลำดับชั้นความลับของระบบสารสนเทศ

(1) ลับที่สุด

(2) ลับมาก

(3) ลับ

3.4 จัดแบ่งระดับชั้นการเข้าถึงของระบบสารสนเทศ

(1) เข้าถึงได้เฉพาะผู้ใช้งานที่มีสิทธิ์สูงสุด

(2) เข้าถึงได้เฉพาะผู้ใช้งานที่ได้รับอนุมัติสิทธิ์เท่านั้น

(3) เข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง

(4) เข้าถึงได้ทุกกลุ่มผู้ใช้งาน

3.5 กำหนดเวลาในการเข้าถึงระบบสารสนเทศ

(1) ในเวลาราชการ (08.30 - 16.30 น.)

(2) นอกเวลาราชการ (นอกช่วงเวลา 08.30 - 16.30 น.)

(3) ในช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนขัตฤกษ์)

(4) ในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงเวลาการเข้าถึง)

3.6 กำหนดช่องทางการเข้าถึงระบบสารสนเทศ

(1) ระบบเครือข่ายบริเวณเฉพาะที่ (LAN) ในลักษณะ Client Server

(2) ระบบอินทราเน็ต (Intranet) ในลักษณะ Web Base Application

(3) ระบบอินเทอร์เน็ต (Internet) ในลักษณะ Web Base Application

(4) ระบบอินเทอร์เน็ต (Internet) ในลักษณะ VPN

ตารางสรุปการควบคุมการใช้งานสารสนเทศของกรมกิจการผู้สูงอายุ

เวลาการเข้าถึง	ประเภทของระบบสารสนเทศ	ลำดับความสำคัญ	ลำดับชั้นความลับ	ระดับชั้นการเข้าถึง	ช่องทางการเข้าถึง
ในเวลาราชการ (08.30-16.30 น.)	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด - ปานกลาง - น้อย	-	- กลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้งาน	- ระบบเครือข่ายบริเวณ เฉพาะที่ (LAN) - ระบบอินทราเน็ต (Intranet) - ระบบอินเทอร์เน็ต (Internet) ในลักษณะ VPN
นอกเวลาราชการ (นอกช่วงเวลา 08.30-16.30 น.)	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด - ปานกลาง - น้อย	-	- กลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้งาน	- ระบบอินเทอร์เน็ต (Internet) ในลักษณะ Web Base Application - ระบบอินเทอร์เน็ต (Internet) ในลักษณะ VPN
ในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และ วันหยุดนขัตฤกษ์)	- ด้านการบริหาร - ด้านการให้บริการ	- ปานกลาง - น้อย	-	- กลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้งาน	- ระบบอินเทอร์เน็ต (Internet) ในลักษณะ Web Base Application - ระบบอินเทอร์เน็ต (Internet) ในลักษณะ VPN
ในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุ ช่วงเวลาการเข้าถึง)	- ด้านการบริหาร - ด้านการให้บริการ	มากที่สุด	ลับที่สุด	- ผู้ใช้งานที่มีสิทธิ์สูงสุด - ผู้ใช้งานที่ได้รับอนุมัติสิทธิ์เท่านั้น	- ระบบเครือข่ายบริเวณ เฉพาะที่ (LAN) - ระบบอินเทอร์เน็ต (Internet) ในลักษณะ VPN

4. กำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ

4.1 การควบคุมการเข้าถึงสารสนเทศ โดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิ์ ที่เกี่ยวข้องกับระบบสารสนเทศ

4.2 การปรับปรุงให้สอดคล้อง กับการใช้งานตามภารกิจและด้านความมั่นคงปลอดภัย

เรื่องที่ 6

ข้อปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ ได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การใช้งานบริการเครือข่ายของ กรมกิจการผู้สูงอายุ

1.1 ห้ามผู้ใดเข้าใช้งานบริการเครือข่ายของ กรมกิจการผู้สูงอายุ โดยไม่ได้รับอนุญาต หากบุกรุกหรือพยายามบุกรุก ถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

1.2 ผู้ที่ประสงค์จะใช้งานบริการเครือข่ายของ กรมกิจการผู้สูงอายุ จะต้องขออนุญาตจากผู้ดูแลระบบก่อน

1.3 ผู้ใช้งานจะได้รับสิทธิ์ให้เข้าใช้งานบริการเครือข่ายของ กรมกิจการผู้สูงอายุ ได้แต่เพียงบริการที่ได้รับอนุญาต ให้เข้าถึงเท่านั้น

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

1.5 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งาน (Account) ทุกครั้งที่เข้าใช้งาน บริการเครือข่ายของ กรมกิจการผู้สูงอายุ

1.6 ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภทำPeer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่ จะได้รับอนุญาตจากผู้ดูแลระบบ

1.7 ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมออนไลน์เพื่อความบันเทิงทุกประเภทำในเวลาราชการ

1.8 ห้ามผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์ และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการ ค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไป เพื่อแสวงหากำไร

1.9 ห้ามผู้ใช้งานละเมิดต่อผู้อื่น เช่น ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่ มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (Account) ของผู้อื่น การเผยแพร่ ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพ

หรือการเขียนข้อความที่ทำให้ ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว กรมกิจการผู้สูงอายุ ไม่มีส่วนร่วม รับผิดชอบต่อความเสียหายดังกล่าว

2. การใช้งานบริการเครือข่ายของ กรมกิจการผู้สูงอายุ จากภายนอก

2.1 ผู้ใช้งานต้องขออนุญาตและได้รับอนุญาตจากผู้ดูแลระบบแล้วเท่านั้น จึงจะสามารถเข้าใช้งานบริการ เครือข่ายของ กรมกิจการผู้สูงอายุ จากภายนอกได้และจะเข้าใช้ได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

2.2 ผู้ใช้งานที่เข้าใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุ จากภายนอก หรือ Internet จะต้องเชื่อมต่อด้วยวิธีการ Remote Access ผ่าน VPN

2.3 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งาน (Account) ของตนเองเพื่อยืนยันตัวตน ทุกครั้งที่เข้าใช้งานบริการเครือข่ายของกรมกิจการผู้สูงอายุ จากภายนอก

3. การระบุอุปกรณ์บนเครือข่าย

3.1 ระบุหมายเลขอุปกรณ์บนเครือข่าย ประกอบด้วย หมายเลขเทอร์มินัล หมายเลข MAC Address และหมายเลข IP Address

3.2 ใช้ไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อกำหนดว่าหมายเลขระบุอุปกรณ์ใดที่สามารถเข้าถึงเครือข่าย ส่วนใดของ กรมกิจการผู้สูงอายุ

3.3 อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

3.4 รักษาความมั่นคงปลอดภัยทางกายภาพต่ออุปกรณ์เครือข่ายหรืออุปกรณ์คอมพิวเตอร์เพื่อป้องกัน การเปลี่ยนแปลงแก้ไขหมายเลขระบุอุปกรณ์เหล่านั้น

3.5 จัดเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

3.6 กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อ กับเครือข่ายภายในได้หรือไม่

3.7 จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

3.8 ทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง

4. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

4.1 ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ทั้งทางกายภาพและโดยการ ล็อกอินเข้ามาใช้งาน

4.2 ล็อกอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่า Configuration ด้วยกุญแจ เพื่อป้องกันการเข้าถึง ทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

4.3 ยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

4.4 กำหนดการเปิด- ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยจะปิดพอร์ตที่เสี่ยงและก่อให้เกิดความเสียหายต่อระบบเครือข่าย

4.5 ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ หรืออย่างน้อย สัปดาห์ละ 2 ครั้ง

4.6 ติดตั้งระบบป้องกันและตรวจสอบการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ อย่างปลอดภัย เช่น ระบบชีวภาพ (Biometric) หรือสมาร์ทการ์ด (Smartcard) และติดตั้งกล้องโทรทัศน์วงจรปิด ป้องกันการโจรกรรม เป็นต้น

4.7 ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ หากมีความจำเป็น ต้องแจ้งให้ผู้ดูแลระบบเป็นผู้รับผิดชอบนำพาเข้าไปเท่านั้น

4.8 กำหนดสิทธิ์บุคคลในการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ โดยให้เฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องเท่านั้น

5. การแบ่งแยกเครือข่าย

5.1 แยกกลุ่มเครือข่ายเป็น 7 ประเภทใหญ่ๆ คือ 1) เครือข่ายภายนอก (External) 2) ส่วนที่มีการให้บริการ สาธารณะ (Demilitarized Zone : DMZ) ที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก 3) เครือข่ายภายใน (Internal) 4) เครือข่ายสำหรับบริการเชื่อมต่อไร้สาย (Wireless Device) 5) เครือข่ายสำหรับงานบริหารจัดการ ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ (DC) 6) เครือข่ายสำหรับติดตั้งระบบงานสารสนเทศต่างๆ ของ กรมกิจการผู้สูงอายุ (Applications) และ 7) เครือข่ายสำหรับติดตั้งระบบฐานข้อมูล (Database)

5.2 แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

5.3 แบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบงานต่างๆ ของกรมกิจการผู้สูงอายุ

5.4 แยกวงเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ ของ กรมกิจการผู้สูงอายุ

5.5 ใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ

5.6 ใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอก กรมกิจการผู้สูงอายุ

5.7 กรองและจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อยๆ

5.8 ผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่ง จะไม่สามารถเข้าถึงข้อมูลที่อยู่ในอีกวงเครือข่ายหนึ่งได้โดยตรง

5.9 ควบคุมการเข้าถึงทางกายภาพสำหรับเครือข่ายย่อย เพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อย และป้องกันการเปลี่ยนแปลงแก้ไขสายสัญญาณ ดักแอบดูข้อมูลบนเครือข่าย หรืออื่นๆ โดยไม่ได้รับอนุญาต

5.10 จัดทำผังเครือข่ายที่แสดงถึงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก โดยมีการปรับปรุงให้เป็นปัจจุบัน อยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง

6. การควบคุมการเชื่อมต่อทางเครือข่าย

6.1 ตรวจสอบและจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่าย ให้เป็นไปตามนโยบายในการควบคุมการเข้าถึง และข้อกำหนดของระบบงาน

6.2 จำกัดสิทธิ์และความสามารถของผู้ใช้งานในการเชื่อมต่อเพื่อเข้าสู่ระบบเครือข่าย กรมกิจการผู้สูงอายุ

6.3 จำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานต่อระบบงานต่างๆ ของ กรมกิจการผู้สูงอายุ อาทิ ระบบงานที่ใช้ในการ ส่งข้อความ (Messaging applications) เช่น ระบบอีเมล ระบบงานสำหรับการโอนย้ายไฟล์ ระบบงานต่างๆ สำหรับใช้งานภายใน กรมกิจการผู้สูงอายุ

6.4 จำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งาน ตามวันที่ เวลา หรือช่วงเวลาที่อนุญาตให้ใช้งาน

6.5 ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่าย กรมกิจการผู้สูงอายุ โดยไม่ได้รับอนุญาต

6.6 ระบุอุปกรณ์และเครื่องมือที่ใช้ในการควบคุมการเชื่อมต่อระบบเครือข่าย กรมกิจการผู้สูงอายุ

6.7 ใช้ไฟร์วอลล์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย ให้เป็นไปตามนโยบายในการควบคุมการเข้าถึง

6.8 ป้องกันเลขที่อยู่ของไอพี (IP Address) ของระบบเครือข่ายภายใน กรมกิจการผู้สูงอายุ มิให้หน่วยงานภายนอก ที่เชื่อมต่อสามารถมองเห็นได้

6.9 ติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้ระบบเครือข่ายของ กรมกิจการผู้สูงอายุ ในลักษณะที่ผิดปกติ

6.10 การเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก กรมกิจการผู้สูงอายุ จะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก ซึ่งมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware)

6.11 ห้ามเปิดช่องทางการเชื่อมต่อทางเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายในกรมกิจการผู้สูงอายุ เพื่อให้สามารถ เข้าถึงเครื่องแม่ข่ายสำหรับระบบงานได้จากระยะไกล ยกเว้นในกรณีที่มีความจำเป็น หรือมีความเร่งด่วนสูง ซึ่งจะต้องได้รับอนุมัติจากผู้อำนวยการกองยุทธศาสตร์และแผนงาน หรือผู้ดูแลระบบก่อนดำเนินการ

6.12 กำหนดระยะเวลาที่แน่นอนของการเชื่อมต่อจากระยะไกล เช่น ให้ใช้ในระยะเวลา 7 วัน และหลังจาก ที่สิ้นสุดการใช้งาน ให้ทำการปิดช่องทางการเชื่อมต่อนั้นโดยทันที

7. การควบคุมการจัดเส้นทางบนเครือข่าย

7.1 ใช้เกตเวย์หรืออุปกรณ์เครือข่ายเพื่อตรวจสอบ IP Address ของทั้งต้นทางและปลายทาง และควบคุม การไหลของข้อมูลผ่านเครือข่ายต่างๆ จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง

7.2 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย IP Address

7.3 กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อยหรือเครือข่ายภายใน และภายนอก

7.4 จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย โดยไม่อนุญาตให้ผู้ใช้บริการ สามารถใช้เส้นทางอื่นๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

7.5 กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการเข้าใช้บริการระบบเครือข่าย กรมกิจการผู้สูงอายุ

เรื่องที่ 7

ข้อปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ ได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. ขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

1.1 ผู้ที่ประสงค์จะเข้าถึงระบบปฏิบัติการของ กรมกิจการผู้สูงอายุ จะต้องขออนุญาตและได้รับอนุมัติจากผู้อำนวยการ กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุหรือผู้ดูแลระบบอย่างเป็นลายลักษณ์อักษรก่อน

1.2 ผู้ใช้งานจะได้รับสิทธิ์ให้เข้าถึงระบบปฏิบัติการของ กรมกิจการผู้สูงอายุ ได้แต่เพียงระบบที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

1.3 ผู้ใช้งานที่ได้รับสิทธิ์ให้เข้าถึงระบบปฏิบัติการของ กรมกิจการผู้สูงอายุ จะได้รับบัญชีผู้ใช้งาน (Account) เป็นการเฉพาะบุคคลเท่านั้น ซึ่ง Account จะประกอบด้วย รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) โดยผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้

1.4 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งาน (Account) ทุกครั้งที่เข้าถึง ระบบปฏิบัติการของ กรมกิจการผู้สูงอายุ

1.5 จำกัดระยะเวลาและจำนวนครั้งในการป้อนรหัสผ่าน เช่น หากผู้ใช้งานป้อนรหัสผ่านผิดเกิน 3 ครั้ง ระบบจะต้องทำการล็อกสิทธิ์ไม่ให้ผู้ใช้งานนั้นเข้าถึงระบบปฏิบัติการได้ จนกว่าผู้ดูแลระบบจะดำเนินการปลดล็อกให้

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

1.7 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้รหัสผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

1.8 ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อล็อกหน้าจอคอมพิวเตอร์ เมื่อไม่มีการใช้งาน และกำหนดให้ต้องใส่รหัสผ่าน เมื่อต้องการเข้าใช้งานใหม่

1.9 ผู้ใช้งานต้องลงบันทึกออก(Logout) ทันที เมื่อเลิกใช้งานเครื่องคอมพิวเตอร์หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

1.10 ห้ามผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

1.11 ผู้ใช้งานสามารถขอใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ของ กรมกิจการผู้สูงอายุ ได้ตามหน้าที่ความจำเป็นเท่านั้น

1.12 ซอฟต์แวร์ที่ กรมกิจการผู้สูงอายุ จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

1.13 ห้ามผู้ใช้งานใช้ทรัพยากรทุกประเภทที่เป็นของ กรมกิจการผู้สูงอายุ เพื่อประโยชน์ทางการค้า

1.14 ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภทำPeer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่ จะได้รับอนุญาตจากผู้ดูแลระบบ

1.15 ในกรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม

1.16 ห้ามผู้ใช้งานใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมกิจการผู้สูงอายุในการควบคุมคอมพิวเตอร์ หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาต

2. การระบุและยืนยันตัวตนของผู้ใช้งาน

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

2.2 ผู้ใช้งานทุกคนต้องมีบัญชีผู้ใช้งาน (Account) เฉพาะของแต่ละบุคคลแยกจากกัน เพื่อใช้ในการพิสูจน์ตัวตน

2.3 สำหรับระบบที่มีความสำคัญสูง ต้องกำหนดให้ผู้ใช้งานพิสูจน์ตัวตนด้วยวิธีการทางเทคนิคที่มีความมั่นคง ปลอดภัยสูง เช่น ใช้วิธีการเข้ารหัสข้อมูล วิธีการทางชีวภาพ (อาทิ การใช้ลายนิ้วมือ เรตินา ฝ่ามือ เสียง)

3. ระบบบริหารจัดการรหัสผ่าน

3.1 ให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับบัญชีผู้ใช้งาน (Account) จากผู้ดูแลระบบหรือเมื่อเข้าใช้งานระบบเป็นครั้งแรก

3.2 ให้ผู้ใช้งานสามารถตั้งหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนการยืนยันรหัสผ่านใหม่ที่ตั้งอีกครั้ง

3.3 ให้ผู้ใช้งานสามารถตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่นได้ เช่น ไม่ใช้ชื่อ นามสกุล วันเดือนปีเกิด หมายเลขโทรศัพท์คำจากพจนานุกรม เป็นต้น

3.4 ให้มีการแจ้งเตือนข้อผิดพลาดในการตั้งรหัสผ่านของผู้ใช้งาน เช่น รหัสผ่านมีความยาวของตัวอักขระ น้อยกว่าที่กำหนด มีรหัสผู้ใช้งานอยู่ในรหัสผ่าน เป็นต้น

3.5 ให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุกๆ 3 เดือน

3.6 ให้มีการจัดเก็บรหัสผ่านเดิมที่ผู้ใช้งานเคยตั้งไปแล้ว เพื่อตรวจสอบไม่ให้นำกลับมาใช้ใหม่ตามระยะเวลา ที่เหมาะสม

3.7 ไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอ ในขณะที่ผู้ใช้งานกำลังใส่ข้อมูลเพื่อเข้าใช้งานระบบ เช่น ให้แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอ เป็นต้น

3.8 ให้มีการป้องกันไฟล์ข้อมูลรหัสผ่านที่ได้มีการจัดเก็บไว้หรือที่จำเป็นต้องส่งไปในเครือข่าย เพื่อป้องกัน การเข้าถึงโดยไม่ได้รับอนุญาต เช่น ป้องกันโดยการเข้ารหัสข้อมูล (Encryption) พร้อมการคำนวณผลรวม (Hash) เพื่อซ่อนข้อมูลไว้

3.9 การจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานจะต้องแยกต่างหากจากข้อมูลของระบบงาน

4. การใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้

4.1 การจัดเก็บโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ต้องแยกจัดเก็บไว้ต่างหาก เช่น แยกไว้ใน ไดเรกทอรีที่ต่างจากไดเรกทอรีของซอฟต์แวร์ระบบงาน

4.2 จัดทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ที่อนุญาตให้ใช้งานได้

4.3 ห้ามผู้ใช้งานทั่วไปใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ โดยจำกัดสิทธิ์ให้เฉพาะ ผู้ดูแลระบบหรือผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

4.4 ผู้ใช้งานที่ต้องการใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ต้องขออนุญาตจาก ผู้ดูแลระบบก่อน โดยระบุเหตุผลความจำเป็นหรือความต้องการใช้งาน และต้องให้ผู้บังคับบัญชาของผู้ใช้งาน ลงนามให้ความเห็นชอบเป็นลายลักษณ์อักษร

4.5 ผู้ใช้งานต้องขออนุญาตใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้เป็นรายครั้ง และสามารถใช้งานได้ตามระดับสิทธิ์ที่ กรมกิจการผู้สูงอายุ กำหนดเท่านั้น

4.6 มีการบันทึกข้อมูลล็อก(Log) เพื่อแสดงการใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้

4.7 ยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ที่ไม่มีความจำเป็นต้องใช้งานแล้ว

5. การหมดเวลาใช้งานระบบสารสนเทศ

5.1 ให้มีการเคลียร์หน้าจอคอมพิวเตอร์เพื่อป้องกันไม่ให้ผู้อื่นเห็นข้อมูล หลังจากไม่มีกิจกรรมการใช้งาน ระบบสารสนเทศเป็นระยะเวลาเกิน 10 นาที

5.2 เมื่อไม่มีกิจกรรมการใช้งานระบบสารสนเทศในระยะเวลาหนึ่ง ต้องกำหนดให้มีการตัดและหมดเวลา การใช้งานระบบสารสนเทศ เช่น ตัดการใช้งานระบบทันทีหลังจากไม่มีการใช้งานเป็นระยะเวลาเกิน 10 นาที

5.3 สำหรับระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูง ต้องจำกัดระยะเวลาการเชื่อมต่อของระบบ สารสนเทศนั้น เช่น ตัดการเชื่อมต่อของระบบทันทีหลังจากใช้งานเป็นระยะเวลาเกิน 30 นาที ต่อการพิสูจน์ตัวตน (Authentication) เข้าใช้งาน

5.4 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานระบบสารสนเทศอีกครั้ง หลังจากที่ ระบบได้หมดเวลาการใช้งานไปแล้ว

เรื่องที่ 8

ข้อปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ของ กรมกิจการผู้สูงอายุ ได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การจำกัดการเข้าถึงสารสนเทศ

1.1 กำหนดการควบคุมการเข้าถึงกับระบบงาน

1.1.1 แสดงข้อความเตือน เพื่อห้ามผู้ไม่มีสิทธิ์เข้าถึงระบบ

1.1.2 จำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลผิดในการล็อกอินได้

1.1.3 จำกัดช่วงระยะเวลาที่นานที่สุด ที่ผู้ใช้งานต้องล็อกอินเข้าใช้งานให้สำเร็จ

1.1.4 ส่งข้อความเตือนไปยังผู้ดูแลระบบให้ทราบว่ามีผู้ใช้งานพยายามล็อกอินแต่ผิดพลาดหลายครั้ง

1.1.5 กำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบได้ ภายหลังจากที่ใส่ข้อมูล การล็อกอินผิดเกินกว่าจำนวนครั้งที่กำหนด

1.1.6 ตรวจสอบข้อมูลการล็อกอิน หลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว

1.1.7 บันทึกข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ

1.1.8 แสดงวันเวลาของการล็อกอินครั้งที่แล้วทั้งที่สำเร็จและไม่สำเร็จ

1.1.9 แสดงรายละเอียดของระบบเท่าที่จำเป็น หลังจากที่ได้ล็อกอินแล้ว

1.1.10 แสดงข้อมูลพื้นฐานเท่าที่จำเป็น เพื่อให้ผู้ใช้งานได้รับทราบข้อมูล

1.1.11 ใช้เมนูเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของระบบ

1.1.12 จำกัดสิทธิ์การเข้าถึงจากอีกระบบหนึ่ง โดยให้สามารถเข้าถึงได้เฉพาะข้อมูลและฟังก์ชันที่จำเป็นต้องใช้งานเท่านั้น

1.1.13 จำกัดการนำข้อมูลออกจากระบบ เพื่อให้เข้าถึงได้เฉพาะข้อมูลที่เกี่ยวข้องและจำเป็นในการนำไปใช้งานเท่านั้น

1.1.14 ไม่แสดงความช่วยเหลือใดๆ ในกรณีเกิดเหตุการณ์ไม่พึงประสงค์ขึ้นกับระบบ

1.1.15 จำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อทันทีเมื่อพ้นช่วงเวลาที่กำหนด

1.1.16 เปลี่ยนรหัสผ่านของระบบตามระยะเวลาที่กำหนด

1.2 กำหนดขั้นตอนและแบบฟอร์มในการเข้าถึงและใช้งานระบบ เพื่อกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงข้อมูล และฟังก์ชันต่างๆ ของระบบ และใช้ในการตรวจสอบและยืนยันตัวตนของผู้ใช้งาน เช่น สิทธิ์ในการอ่าน เขียน ลบ หรือสั่งให้โปรแกรมทำงาน โดยแบบฟอร์มต้องระบุข้อมูลอย่างน้อย ดังนี้ชื่อและนามสกุล ตำแหน่ง หน่วยงาน เหตุผล และระยะเวลาที่ขอเข้าถึงและใช้งานระบบ

1.3 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ตามมาตรฐานสากล

2. ระบบที่ไวต่อการรบกวน

2.1 กำหนดคุณลักษณะของระบบ โดยมีรายละเอียดอย่างน้อย ดังนี้ประเภทของระบบ ลำดับความสำคัญ ลำดับชั้นความลับ ระดับชั้นการเข้าถึง เวลาในการเข้าถึง และช่องทางการเข้าถึง

2.2 ระบุระบบที่ไวต่อการรบกวนและมีผลกระทบสูงต่อ กรมกิจการผู้สูงอายุ โดยเป็นระบบที่มีลำดับชั้นความลับ และมีลำดับความสำคัญมากที่สุด

2.3 ประเมินความเสี่ยงในการใช้ทรัพยากรร่วมกัน ระหว่างระบบที่ไวต่อการรบกวนกับระบบอื่นๆ เช่น ความเสี่ยงในการใช้เครื่องคอมพิวเตอร์เดียวกันในการให้บริการ

2.4 ติดตั้งระบบที่ไวต่อการรบกวนแยกไว้ในเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งต่างหาก

2.5 ควบคุมสภาพแวดล้อม อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอก กรมกิจการผู้สูงอายุ ที่เกี่ยวข้องกับระบบที่ไวต่อการรบกวนโดยเฉพาะ

2.6 ควบคุมการเข้าใช้งานระบบที่ไวต่อการรบกวนจากเครือข่ายภายในและเครือข่ายภายนอกตามที่ตั้งค่า ไว้ในไฟร์วอลล์

3. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

3.1 ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์หรือไม่

3.2 ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้เว้นแต่ข้อมูลที่ได้มีการเผยแพร่ เป็นการทั่วไป

3.3 เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ ที่รับผิดชอบทันที

3.4 เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืน ให้อยู่ในสภาพพร้อมใช้งาน

3.5 หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบ ต่อความเสียหายที่เกิดขึ้น

4. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

4.1 จัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับ ผู้ใช้งานจากระยะไกล

4.2 ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมกิจการผู้สูงอายุ จากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามข้อปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ

4.3 ตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของ กรมกิจการผู้สูงอายุ จากระยะไกล มีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนดหรือไม่

4.4 ผู้ใช้งานจากระยะไกลทุกคน ต้องทำการพิสูจน์ตัวตน (Authentication) ก่อนเข้าใช้งานระบบเทคโนโลยี สารสนเทศและการสื่อสารของ กรมกิจการผู้สูงอายุ

4.5 กำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่างๆ ของหน่วยงาน ที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

4.6 กำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

4.7 สำรองข้อมูลสำหรับการปฏิบัติงานจากระยะไกลอย่างสม่ำเสมอ

เรื่องที่ 9

ข้อปฏิบัติในการควบคุมการเข้าถึงของหน่วยงานภายนอก (outsource control)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมการเข้าถึงของหน่วยงานภายนอก (outsource control) สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของ กรมกิจการผู้สูงอายุ ได้อย่างเหมาะสม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ

1.1 ผู้ใช้งานต้องขออนุญาตล่วงหน้าก่อนวันที่จะเข้าออกพื้นที่ โดยต้องกรอกข้อมูลความต้องการและรายละเอียด ตามแบบกำหนดสิทธิ์การเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ ที่ทาง (ทนส. กยผ. ผส.) กำหนด

1.2 ผู้ใช้งานต้องได้รับอนุมัติสิทธิ์ในการเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุจากผู้อำนวยการกองยุทธศาสตร์และแผนงาน หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อน จึงจะเข้าออกพื้นที่ได้

1.3 ผู้ใช้งานจะถูกบันทึกรายละเอียดข้อมูลลงในทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่าย และเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ

1.4 ผู้ใช้งานต้องแลกบัตรที่ใช้ระบุตัวตนของแต่ละบุคคล เช่น บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ หรือบัตรอนุญาตเข้าออกภายในอาคารที่ได้แลกมาก่อนหน้า เป็นต้น เพื่อรับบัตรผู้มาติดต่อ (Visitor)และบันทึกข้อมูล ลงในแบบบันทึกการเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ ทุกครั้งที่มีการเข้าออก

1.5 ผู้ใช้งานต้องติดบัตรผู้มาติดต่อ (Visitor) ตรงจุดที่สามารถมองเห็นได้ชัดเจน ตลอดเวลาที่อยู่ภายในพื้นที่ ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ

1.6 กรณีที่ต้องการนำอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่าย เข้ามาภายในบริเวณพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ จะต้องบันทึกรายการ อุปกรณ์ที่นำเข้ามา ลงในแบบบันทึกการเข้าออกพื้นที่ศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ ให้ถูกต้อง และจะต้องได้รับอนุญาตจากผู้ดูแลระบบเป็นลายลักษณ์อักษร

1.7 ผู้ใช้งานต้องคืนบัตรผู้มาติดต่อ (Visitor) กับผู้ดูแลระบบ โดยผู้ดูแลระบบจะตรวจสอบแต่ละบุคคล และอุปกรณ์พร้อมลงบันทึกเวลาออกและรายการอุปกรณ์ในแบบบันทึกการเข้าออกพื้นที่ศูนย์ปฏิบัติการ ระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ ทุกครั้งที่มีการเข้าออก

1.8 กรณีที่จะเข้ามาปฏิบัติงานในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ กรมกิจการผู้สูงอายุ ในวันหยุด หรือนอกเวลาราชการ จะต้องขออนุญาตจากผู้ดูแลระบบล่วงหน้าก่อนทุกครั้ง และการดำเนินงานจะต้องอยู่ในการ กำกับดูแลของผู้ดูแลระบบเท่านั้น

2. การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ กรมกิจการผู้สูงอายุ

2.1 ผู้ใช้งานต้องขออนุญาตไว้ล่วงหน้าเป็นลายลักษณ์อักษรก่อนเข้าถึงระบบทุกครั้ง พร้อมทั้งแจ้งให้ผู้ดูแล ระบบทราบ โดยต้องระบุข้อมูลอย่างน้อย ดังนี้ชื่อและนามสกุล ตำแหน่ง หน่วยงาน เหตุผล โครงการที่รับจ้าง และระยะเวลาที่ขอเข้าถึงและใช้งานระบบ

2.2 ผู้ใช้งานต้องได้รับอนุญาตจากผู้ดูแลระบบแล้วเท่านั้น จึงจะสามารถดำเนินการบำรุงรักษาบริหารจัดการ พอร์ตของอุปกรณ์เครือข่าย บริหารจัดการผ่านระบบเครือข่าย และการเข้าถึงระบบเทคโนโลยีสารสนเทศ และการสื่อสารของ กรมกิจการผู้สูงอายุ ได้และจะดำเนินการได้เฉพาะรายการที่ได้รับอนุญาตเท่านั้น

2.3 ผู้ใช้งานต้องทำการสำรองค่า Config ของอุปกรณ์ทุกชนิดภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่าย คอมพิวเตอร์ กรมกิจการผู้สูงอายุ โปรแกรม/โมดูลของระบบงานสารสนเทศ และโครงสร้างฐานข้อมูล ทุกครั้งก่อนแก้ไข หรือเปลี่ยนแปลงค่า รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไข หากการแก้ไขมีปัญหาเกิดขึ้นทำให้ไม่สามารถ ใช้งานระบบได้ผู้ใช้งานจะต้องเรียกคืนข้อมูลที่ได้สำรองไว้กลับมา เพื่อให้ระบบสามารถใช้งานได้ตามสภาพเดิม

2.4 การเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายคอมพิวเตอร์ของ กรมกิจการผู้สูงอายุ จะต้องดำเนินการ ดังนี้

2.4.1 ขออนุญาตและได้รับอนุญาตจากผู้ดูแลระบบแล้วเท่านั้น จึงจะสามารถเชื่อมต่อจากภายนอกได้ โดยจะต้องระบุ บริการที่ขออนุญาต วัน เวลา และระยะเวลาในการเชื่อมต่อให้ชัดเจน

2.4.2 จะต้องเชื่อมต่อด้วยวิธีการ Remote Access VPN

2.4.3 จะต้องทำการพิสูจน์ตัวตน (Authentication) ด้วยบัญชีผู้ใช้งาน (Account) ของตนเองเพื่อยืนยันตัวตน ทุกครั้งที่เชื่อมต่อจากภายนอก

2.5 กรณีจำเป็นต้องสำเนาฐานข้อมูลทุกประเภทออกจาก กรมกิจการผู้สูงอายุ จะต้องทำหนังสือขอความเห็นชอบ จาก กรมกิจการผู้สูงอายุ ล่วงหน้าก่อนทุกครั้ง โดยจะต้องระบุเหตุผลในการนำไปใช้งานอย่างชัดเจน และต้องรับผิดชอบ ต่อความเสียหายที่อาจจะเกิดขึ้นด้วย

2.6 กรณีที่ผู้ใช้งานประมาทำทำให้อุปกรณ์และระบบสารสนเทศของกรมกิจการผู้สูงอายุ ได้รับความเสียหายหรือสูญหาย ผู้ใช้งานจะต้องรับผิดชอบในการซ่อมแซมแก้ไขหรือเปลี่ยนใหม่ให้อยู่ในสภาพที่สามารถใช้งานได้ดังเดิม

2.7 หากมีการเปลี่ยนแปลงรายชื่อผู้ใช้งาน จะต้องแจ้งให้ผู้ดูแลระบบทราบล่วงหน้าเป็นลายลักษณ์อักษร ก่อนมีการเปลี่ยนแปลงทุกครั้ง

2.8 ผู้ใช้งานต้องปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการผู้สูงอายุ ที่กำหนดไว้ โดยไม่มีข้อยกเว้น หากมีการฝ่าฝืน กรมกิจการผู้สูงอายุ จะทำหนังสือแจ้งไปยังหน่วยงานของผู้ใช้งาน และจะไม่อนุญาต ให้ดำเนินการใดๆ ภายใน กรมกิจการผู้สูงอายุ

เรื่องที่10

ข้อปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศวัตถุประสงค์

เพื่อให้หน่วยงานมีระบบสำรองข้อมูลและสารสนเทศที่เหมาะสม และมีการเตรียมความพร้อมกรณีฉุกเฉินหากไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้เพื่อให้หน่วยงานสามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.) 2. คณะทำงาน หมายถึง คณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศว่าด้วยการ จัดทำระบบสำรองข้อมูลและสารสนเทศ และการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ กรมกิจการผู้สูงอายุ 3. เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมาย

ข้อปฏิบัติ

1. การดำเนินงาน

1.1 แต่งตั้งคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศว่าด้วยการจัดทำ ระบบสำรองข้อมูลและสารสนเทศ และการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ กรมกิจการผู้สูงอายุ ประกอบด้วย กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร กลุ่มการพัฒนาระบบสารสนเทศ และกลุ่มการวิเคราะห์ข้อมูล โดยมีผู้อำนวยการกองยุทธศาสตร์และแผนงาน เป็นประธาน

1.2 ประชุมคณะทำงานฯ เพื่อจัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉินของ กรมกิจการผู้สูงอายุ

1.3 นำเสนอร่างแผนฯ ต่ออธิบดีกรมกิจการผู้สูงอายุ เพื่อขอความเห็นชอบ

1.4 มอบหมายเจ้าหน้าที่ดำเนินงานตามแผน

1.5 กำกับ ติดตาม และประเมินผลการดำเนินงานตามแผน

1.6 ทบทวน/ปรับปรุงแผน ปีละ 1 ครั้ง

2. การสำรองและทดสอบกู้คืนข้อมูล

2.1 จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับระบบสารสนเทศ ของกรมกิจการผู้สูงอายุ

2.2 พิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นตามลำดับความสำคัญ เพื่อจัดทำระบบสำรอง

2.3 กำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ และความถี่ในการสำรอง

2.4 กำหนดสื่อที่ใช้ในการเก็บข้อมูล และรูปแบบของการสำรองข้อมูล ซึ่งมี 2 ชนิด คือ การสำรองข้อมูล แบบเต็ม (Full Back up) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

2.5 รายการที่ต้องสำรองข้อมูลและความถี่อย่างน้อย ดังนี้

เว็บไซต์หน่วยงาน : สำรองข้อมูลที่เผยแพร่บนเว็บไซต์ 1 ครั้ง/สัปดาห์

Web Application Servers: สำรองข้อมูลที่เผยแพร่บนเว็บไซต์ 1 ครั้ง/เดือน

Database Servers : สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ ทุกวัน

Firewall Server: สำรองข้อมูล Rule ของ Firewall 1 ครั้ง/สัปดาห์

Server อื่นๆ: สำรองข้อมูลบนเซิร์ฟเวอร์อื่นๆ เช่น ระบบงานต่างๆ 1 ครั้ง/เดือน

2.6 มีการสำรองข้อมูลเครื่องแม่ข่ายทั้งระบบ (Full System Backup) อย่างน้อยปีละ 1 ครั้ง

2.7 กำหนดขั้นตอนปฏิบัติและโปรแกรมในการสำรองข้อมูลและทดสอบกู้คืนข้อมูล แยกตามระบบสารสนเทศ แต่ละระบบอย่างถูกต้อง

2.8 กำหนดการเข้ารหัสข้อมูลในการสำรองข้อมูลที่สำคัญ โดยใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

2.9 จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูลที่เหมาะสมกับความสำคัญของแต่ละระบบสารสนเทศ

2.10 รายละเอียดที่ปรากฏในแผนการสำรองและทดสอบกู้คืนข้อมูล ต้องมีหัวข้อสำคัญอย่างน้อย ดังนี้

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

2.11 มอบหมายเจ้าหน้าที่หลักเพื่อดำเนินงานตามแผนการสำรองและทดสอบกู้คืนข้อมูลและเจ้าหน้าที่สำรอง เพื่อทำหน้าที่สำรองข้อมูลในกรณีที่เจ้าหน้าที่หลักไม่สามารถปฏิบัติงานได้โดยเจ้าหน้าที่มีหน้าที่ ดังนี้

2.11.1 จัดทำคู่มือการสำรองและทดสอบกู้คืนข้อมูล

2.11.2 ดำเนินการตามปฏิทินการสำรองและทดสอบกู้คืนข้อมูล

2.11.3 บันทึกการสำรองข้อมูล (Operator Logs) และจัดทำรายงานผลการสำรองข้อมูลประจำเดือน โดยมีรายละเอียดอย่างน้อย ดังนี้ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก

2.11.4 กรณีพบปัญหาในการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหา และรายงานให้ผู้บังคับบัญชาทราบ

2.11.5 ตรวจสอบผลการสำรองข้อมูลว่าถูกต้องและสมบูรณ์พร้อมทั้งบันทึกผลการตรวจสอบ

2.11.6 จัดเก็บสื่อบันทึกข้อมูลไว้ในที่ที่ปลอดภัย

2.11.7 มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูล

2.11.8 มีการทดสอบกู้คืนข้อมูลจากข้อมูลที่สำรองเก็บไว้อย่างน้อยปีละ 1 ครั้ง

2.11.9 กรณีพบปัญหาที่สร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย จนทำให้ต้องกู้คืนระบบ เจ้าหน้าที่จะต้องดำเนินการแก้ไขปัญหา พร้อมทั้งสรุปรายงานการปฏิบัติงานและการแก้ไขปัญหา ให้ผู้บังคับบัญชาทราบ

2.11.10 การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด(Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

2.11.11 หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้ระบบทราบทันทีพร้อมทั้งรายงานความก้าวหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

2.11.12 สรุปผลการดำเนินงานรายปีให้ผู้บังคับบัญชารับทราบ โดยการวิเคราะห์ผลการปฏิบัติงานและรายงานตามประเด็นสำคัญอย่างน้อย ดังนี้สรุปผลการดำเนินงาน ปัญหาอุปสรรค วิธีการแก้ไขและข้อเสนอแนะ

2.12 ติดตามประเมินผล และทบทวน/ปรับปรุงแผนการสำรองและทดสอบกู้คืนข้อมูล ปีละ 1 ครั้ง

3. การเตรียมความพร้อมกรณีฉุกเฉิน

3.1 จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อรองรับสถานการณ์ฉุกเฉินหรือภัยพิบัติที่มีผลกระทบ ต่อระบบสารสนเทศของ กรมกิจการผู้สูงอายุ

3.2 พิจารณาคัดเลือกสถานการณ์ฉุกเฉินหรือภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศของกรมกิจการผู้สูงอายุ โดยมีสถานการณ์อย่างน้อย ดังนี้ อัคคีภัย ระบบไฟฟ้าขัดข้อง และระบบปรับอากาศผิดปกติ

3.3 รายละเอียดที่ปรากฏในแผนเตรียมความพร้อมกรณีฉุกเฉิน ต้องมีหัวข้อสำคัญอย่างน้อย ดังนี้ - ประเภทของสถานการณ์ฉุกเฉินหรือภัยพิบัติ

- การเตรียมความพร้อม
- การแก้ปัญหา
- ขั้นตอนการปฏิบัติ
- ผู้รับผิดชอบ
- การติดตามประเมินผล

3.4 พิจารณาคัดเลือกสถานการณ์ฉุกเฉินหรือภัยพิบัติเพื่อซักซ้อมแผนรับสถานการณ์อย่างน้อยปีละ 1 กรณี

3.5 มอบหมายเจ้าหน้าที่ผู้รับผิดชอบเพื่อดำเนินงานตามแผนเตรียมความพร้อมกรณีฉุกเฉิน โดยเจ้าหน้าที่ มีหน้าที่ ดังนี้

3.5.1 จัดเตรียมอุปกรณ์ที่จำเป็น เพื่อรองรับสถานการณ์ฉุกเฉินหรือภัยพิบัติที่อาจจะเกิดขึ้น

3.5.2 ตรวจสอบและบันทึกผลการตรวจสอบความพร้อมของระบบและอุปกรณ์ตามระยะเวลาพร้อมทั้งจัดทำรายงานผลการดำเนินงาน โดยมีรายละเอียดอย่างน้อย ดังนี้วันที่ทำการตรวจสอบ เอกสารหลักฐาน/ ซอฟต์แวร์ที่ควรจัดเตรียม เป็นต้น

3.5.3 กรณีซักซ้อมแผน/เกิดปัญหา เจ้าหน้าที่จะต้องรายงานข้อเท็จจริงและการแก้ไขปัญหาพร้อมทั้งสรุปผลการปฏิบัติงานและการแก้ไขปัญหาให้ผู้บังคับบัญชาทราบ

3.5.4 บันทึกเหตุการณ์/สถานการณ์ฉุกเฉินที่เกิดขึ้น โดยพิจารณาถึง ประเภทำปริมาณและหลักฐาน สำหรับอ้างอิง เพื่อใช้ในกรณีที่เหตุการณ์มีความเกี่ยวข้องทางกฎหมาย

3.5.5 สรุปผลการดำเนินงานรายปีให้ผู้บังคับบัญชารับทราบ โดยการวิเคราะห์ผลการปฏิบัติงานและรายงานตามประเด็นสำคัญอย่างน้อย ดังนี้สรุปผลการดำเนินงาน ปัญหาอุปสรรควิธีการแก้ไขและข้อเสนอแนะ

3.6 ติดตามประเมินผล และทบทวน/ปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน ปีละ 1 ครั้ง

เรื่องที่ 11

ข้อปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้หน่วยงานมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจจะเกิดขึ้น ทำให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน โดยการตรวจสอบและประเมิน ความเสี่ยงนั้น จะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือผู้ตรวจสอบอิสระ ด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. คณะทำงาน หมายถึง คณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศว่าด้วยการ จัดทำระบบสำรองข้อมูลและสารสนเทศ และการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ กรมกิจการผู้สูงอายุ

3. คณะตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ หมายถึง คณะทำงานเทคโนโลยีสารสนเทศ กรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การดำเนินงาน

1.1 แต่งตั้งคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศว่าด้วยการจัดทำ ระบบสำรองข้อมูลและสารสนเทศ และการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ กรมกิจการผู้สูงอายุ ประกอบด้วย กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร กลุ่มการพัฒนาระบบสารสนเทศ และกลุ่มการวิเคราะห์ข้อมูล โดยมีผู้อำนวยการกองยุทธศาสตร์และแผนงาน เป็นประธาน

1.2 ประชุมคณะทำงานฯ เพื่อจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมกิจการผู้สูงอายุ

1.3 นำเสนอร่างแผนฯ ต่ออธิบดีกรมกิจการผู้สูงอายุ เพื่อขอความเห็นชอบ

1.4 มอบหมายเจ้าหน้าที่ดำเนินงานตามแผน และเตรียมความพร้อมเพื่อรับการตรวจสอบและประเมินความเสี่ยง ด้านสารสนเทศของ กรมกิจการผู้สูงอายุ

1.5 กำกับ ติดตาม และประเมินผลการดำเนินงานตามแผน

1.6 ทบทวน/ปรับปรุงแผน ปีละ 1 ครั้ง

2. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

2.1 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของกรมกิจการผู้สูงอายุ โดยดำเนินการ ให้สอดคล้องตามแผนและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล กรมกิจการผู้สูงอายุ

2.2 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของกรมกิจการผู้สูงอายุ ให้ดำเนินการโดยคณะเทคโนโลยีสารสนเทศ กรมกิจการผู้สูงอายุ

2.3 กำหนดขอบเขตและขั้นตอนปฏิบัติสำหรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของกรมกิจการผู้สูงอายุ

2.4 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของ กรมกิจการผู้สูงอายุ ที่มีความสำคัญหรือเป็นข้อมูลส่วนบุคคล มีข้อจำกัด ดังนี้

2.4.1 สามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบในลักษณะที่อ่าน ได้เพียงอย่างเดียว

2.4.2 ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลชนิดที่สามารถเขียน หรือบันทึก ข้อมูลได้ จะต้องดำเนินการด้วยวิธีการที่ปลอดภัย

2.4.3 มีการสร้างสำเนาข้อมูลเพื่อให้ทำงานบนข้อมูลสำเนา

2.4.5 มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ

2.4.4 มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

2.5 เป็นสรุปรายงานผลตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของ กรมกิจการผู้สูงอายุ เสนอต่อ ผู้บริหารกรมกิจการผู้สูงอายุ

2.6 ทบทวน/ปรับปรุงการดำเนินงานตามที่ผู้ตรวจสอบภายในหน่วยงานของรัฐให้ข้อเสนอแนะต่อไป

เรื่องที่ 12
ข้อปฏิบัติในการใช้งานอินเทอร์เน็ต

วัตถุประสงค์

เพื่อเป็นมาตรการควบคุมการใช้งานอินเทอร์เน็ตของ กรมกิจการผู้สูงอายุ ให้มีความมั่นคงปลอดภัย และลดความเสี่ยง หรือผลกระทบที่อาจจะเกิดจากการใช้งานอินเทอร์เน็ตของผู้ใช้งาน ตลอดจนป้องกันมิให้ผู้ใช้งานละเมิด ต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งาน อินเทอร์เน็ตของ กรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การลงทะเบียนผู้ใช้งาน

1.1ผู้ขอใช้งานอินเทอร์เน็ต กรมกิจการผู้สูงอายุ จะต้องลงทะเบียนเพื่อขอใช้งานจากผู้ดูแลระบบก่อน โดยการกรอกข้อมูล ส่วนบุคคลในแบบฟอร์มลงทะเบียนผู้ใช้งานที่ กรมกิจการผู้สูงอายุ จัดเตรียมไว้

1.2 ผู้ขอใช้งานต้องยอมรับและปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของ กรมกิจการผู้สูงอายุ อย่างเคร่งครัด

1.3 ผู้ขอใช้งานที่ได้รับสิทธิ์ให้เข้าใช้งานอินเทอร์เน็ต กรมกิจการผู้สูงอายุ จะได้รับบัญชีผู้ใช้งานอินเทอร์เน็ต (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 ทุกๆ 3 เดือน หรือตามที่ผู้ดูแลระบบกำหนด

2.4 ผู้ใช้งานควรเปลี่ยน Password ใหม่ทันทีหากถูกเปิดเผยหรือสงสัยว่าถูกผู้อื่นนำ Password ไปใช้

2.5 ผู้ใช้งานต้องใช้ Account ของตนเองเท่านั้น ในการเข้าใช้งานอินเทอร์เน็ต กรมกิจการผู้สูงอายุ

2.6 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้ Account ในนามของตนเองไม่ว่ากรณีใดๆ

2.7 ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดจากการใช้งาน Account ในนามของตนเอง

2.8 ผู้ใช้งานต้องทำการ Logout ออกจากคอมพิวเตอร์ทันทีเมื่อเลิกใช้งานอินเทอร์เน็ต หรือเมื่อไม่อยู่ที่ หน้าจอคอมพิวเตอร์นานเกิน 15 นาที

3. การเข้าใช้งานอินเทอร์เน็ต กรมกิจการผู้สูงอายุ

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. การใช้งานอินเทอร์เน็ต กรมกิจการผู้สูงอายุ อย่างปลอดภัย

4.1 การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเทอร์เน็ต ควรเชื่อมต่อผ่านระบบรักษาความมั่นคงปลอดภัย ที่กรมกิจการผู้สูงอายุ จัดสรรไว้เท่านั้น

4.2 ผู้ใช้งานต้องไม่ใช้อินเทอร์เน็ต กรมกิจการผู้สูงอายุ ในการเผยแพร่ หรือใช้งานโดยมีวัตถุประสงค์ดังนี้

4.2.1 ก่อให้เกิดความเสียหายต่อ กรมกิจการผู้สูงอายุ และบุคคลอื่น หรือละเมิดสิทธิ์หรือสร้างความรำคาญต่อผู้อื่น เช่น การตัดต่อภาพของผู้อื่นแล้วนำมาเผยแพร่ทำให้เกิดความอับอาย ลักลอบแก้ไขข้อมูลส่วนบุคคลของผู้อื่น การแสดงความเห็นดูหมิ่นผู้อื่นบนเว็บไซต์ เป็นต้น

4.2.2 หาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือการพาณิชย์เช่น การจำลอง Mail Server เพื่อส่ง mail จำนวนมาก และการจำลอง Web Server เพื่อจัดทำเว็บไซต์สำหรับค้าขาย เป็นต้น

4.2.3 การกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การเข้าสู่เว็บไซต์ ที่ไม่เหมาะสม การใช้ข้อความที่สร้างความตื่นตระหนกกับสังคมโดยรวม เป็นต้น

4.2.4 เปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาต ซึ่งได้มาจาก กรมกิจการผู้สูงอายุ หรือผู้ที่มีสิทธิ์ ในข้อมูลดังกล่าว

4.3 ผู้ใช้งานไม่ควรดาวน์โหลดหรือใช้งานข้อมูลมัลติมีเดีย ที่มีลักษณะยึดครองช่องสัญญาณการสื่อสารข้อมูล ตลอดเวลา (Consume Bandwidth) ผ่านอินเทอร์เน็ต กรมกิจการผู้สูงอายุ ในเวลาราชการ เช่น เล่นเกม/ดูหนัง/ฟังเพลง ออนไลน์ดูคลิปวิดีโอผ่านเว็บไซต์ดาวน์โหลดซอฟต์แวร์ที่มีขนาดใหญ่ผ่านเว็บไซต์ เป็นต้น

4.4 ผู้ใช้งานไม่ควรดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือหรือไม่มั่นใจว่าปลอดภัย เช่น Freeware โปรแกรมรักษาจอภาพ เกมส์และโปรแกรมที่ลงท้ายด้วย exe หรือ com หากมีความจำเป็น ต้องดาวน์โหลด ต้องมีการตรวจสอบด้วยโปรแกรมป้องกันไวรัส ก่อนการนำไปใช้ทุกครั้ง

4.5 หากผู้ใช้งานมีความจำเป็นต้องส่งข้อมูลที่มีขนาดใหญ่ ให้ติดต่อผู้ดูแลระบบดำเนินการเท่านั้น

4.6 ผู้ใช้งานที่มีความจำเป็นต้องนำคอมพิวเตอร์โน้ตบุ๊กไปเชื่อมต่อเข้ากับอินเทอร์เน็ตอื่นที่มิใช่กรมกิจการผู้สูงอายุ จะต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่คอมพิวเตอร์โน้ตบุ๊กดังกล่าว และต้อง Update ไวรัสให้เป็นปัจจุบันอยู่เสมอ

4.7 ผู้ใช้งานควรแจ้งข้อเท็จจริงต่อผู้ดูแลระบบ หากพบเห็นการใช้งานอินเทอร์เน็ต กรมกิจการผู้สูงอายุ ไปในทาง ที่ไม่เหมาะสม หรือพบเห็นการบุกรุกหรือการละเมิดสิทธิ์ของกรมกิจการผู้สูงอายุ

5. การใช้งานเครือข่ายสังคมออนไลน์

5.1 ผู้ใช้งานต้องตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานอันเกิดจากการใช้งานเครือข่ายสังคมออนไลน์

5.2 ผู้ใช้งานต้องรับผิดชอบทั้งด้านสังคมและกฎหมาย เนื่องจากการโพสต์ข้อความ หรือแสดงความคิดเห็น เพื่อให้เผยแพร่บนเครือข่ายสังคมออนไลน์ เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ

5.3 ผู้ใช้งานไม่ควรเปิดเผยข้อมูลส่วนตัวมากเกินไป รวมถึงข้อมูลทางการเงิน

5.4 ผู้ใช้งานไม่ควรโพสต์ข้อความที่บอกสถานะความเคลื่อนไหวของตนเอง เพราะจะทำให้ผู้ไม่หวังดีวางแผนมาทำร้ายหรือขโมยทรัพย์สินได้

5.5 ผู้ใช้งานต้องระมัดระวังอย่างยิ่งในการโพสต์หรือเผยแพร่ ส่งต่อข้อความ รูปภาพ วิดีโอ ที่อาจทำให้ ผู้อื่นเสียหาย เช่น ภาพหลุด คลิปหลุด หรือโพสต์รูปภาพที่สื่อถึงอบายมุขต่างๆ และไม่ควรใช้ถ้อยคำหยาบคาย ถ้อยคำลามก อนาจาร ดูหมิ่น ส่อเสียด เสียดสีให้ร้ายผู้อื่นในทางเสียหาย หรือสร้างความแตกแยกในสังคม

5.6 ผู้ใช้งานต้องระมัดระวังอย่างยิ่งที่จะไว้ใจหรือเชื่อใจคนที่รู้จักผ่านอินเทอร์เน็ต ในการแลกเปลี่ยนข้อมูลส่วนตัว เช่น ชื่อ อีเมล หมายเลขโทรศัพท์ ที่อยู่ เพราะอาจถูกหลอกลวงหรือล่อลวงไปทำอันตรายได้

5.7 ผู้ใช้งานต้องระมัดระวังการเช็คอิน (Check-in) โดยใช้กล้องโทรศัพท์ถ่ายภาพ ระบุพิกัดและเวลา เพราะภาพทุกภาพ การโพสต์ทุกอย่างจะอยู่บนอินเทอร์เน็ตอย่างถาวร ไม่สามารถถูกลบได้อย่างแท้จริง

6. การระงับ/เพิกถอน บัญชีผู้ใช้งานอินเทอร์เน็ต (Account)

6.1 ผู้ดูแลระบบมีสิทธิ์ระงับ Account ของผู้ใช้งานได้ทันที หากได้รับแจ้งหรือตรวจพบการกระทำใดที่อาจ ก่อให้เกิดปัญหาความมั่นคงปลอดภัย หรือการกระทำที่ละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง

6.2 ผู้ดูแลระบบมีสิทธิ์เพิกถอน Account ของผู้ใช้งานออกจากระบบได้ทันที หากไม่มีการติดต่อภายใน ระยะเวลา 90 วันนับจากวันที่ถูกระงับ Account หรือไม่มีการร้องขอขยายสิทธิ์การใช้งาน

6.3 ผู้ดูแลระบบมีสิทธิ์เพิกถอน Account ของผู้ใช้งานออกจากระบบได้ ดังนี้

6.3.1 กรณีเป็นเจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ ให้เพิกถอนเมื่อผู้ใช้งานนั้นลาออกหรือพ้นสภาพจากการเป็น เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือเมื่อไม่มีการเข้าใช้งานอินเทอร์เน็ต กรมกิจการผู้สูงอายุ เป็นระยะเวลาติดต่อกันเกิน 90 วัน

6.3.2 กรณีเป็นบุคคลจากหน่วยงานภายนอก ให้เพิกถอนตามวันที่ระบุในแบบฟอร์มลงทะเบียนผู้ใช้งาน หรือเมื่อไม่มีการเข้าใช้งานอินเทอร์เน็ต กรมกิจการผู้สูงอายุ เป็นระยะเวลาติดต่อกันเกิน 30 วัน

6.4 ผู้ใช้งานสามารถร้องขอขยายสิทธิ์การใช้งาน Account ได้ เพื่อคงสิทธิ์เดิมไว้เมื่อต้องพ้นสภาพจากการ เป็นเจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ โดยยื่นคำร้องส่งถึงกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ กรมกิจการผู้สูงอายุ ทั้งนี้ การอนุญาต และระยะเวลาการขยายสิทธิ์ให้เป็นอำนาจของผู้อำนวยการกองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

เรื่องที่ 13

ข้อปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail)

วัตถุประสงค์

ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) ภายใต้ชื่อโดเมน @dop.mail.go.th ให้บริการเพื่อสนับสนุนการดำเนินงานของเจ้าหน้าที่ในสังกัดกรมกิจการผู้สูงอายุ สำหรับใช้ ติดต่อสื่อสารงานราชการ ให้มีความปลอดภัยและเชื่อถือได้ รวมถึงมีข้อปฏิบัติที่สอดคล้องตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.)

2. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมาย

3. ผู้ใช้งาน หมายถึง เจ้าหน้าที่หรือหน่วยงานในสังกัด กรมกิจการผู้สูงอายุ และสำนักงานรัฐมนตรี (สร.) ข้อปฏิบัติ

1. การลงทะเบียนผู้ใช้งาน

1.1 ผู้ขอใช้งานจะต้องลงทะเบียนเพื่อขอใช้งาน e-Mail จากผู้ดูแลระบบก่อน โดยการกรอกข้อมูลในแบบฟอร์ม ลงทะเบียนผู้ใช้งานที่ กรมกิจการผู้สูงอายุ จัดเตรียมไว้

1.2 ผู้ขอใช้งานต้องยอมรับและปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

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

1.4 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 และต้องประกอบด้วยตัวอักษรภาษาอังกฤษ พิมพ์ใหญ่ พิมพ์เล็ก และตัวเลข

3.3 ผู้ใช้งานควรเปลี่ยน Password ทุกๆ 3 เดือน หรือตามที่ผู้ดูแลระบบกำหนด

3.4 ผู้ใช้งานควรเปลี่ยน Password ใหม่ทันทีหากถูกเปิดเผยหรือสงสัยว่าถูกผู้อื่นนำ Password ไปใช้

3.5 ผู้ใช้งานต้องใช้ Account ของตนเองหรือที่ได้รับมอบหมายเท่านั้น ในการเข้าใช้งาน e-Mail

3.6 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้ Account ในนามของตนเองไม่ว่ากรณีใดๆ

3.7 ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดจากการใช้งาน Account ในนามของตนเอง

3.8 ผู้ใช้งานต้องทำการ Logout ออกจากการใช้งาน e-Mail ทันทีเมื่อเลิกใช้งาน หรือเมื่อไม่อยู่ที่หน้าจอ คอมพิวเตอร์นานเกิน 15 นาที

4. การรับ - การส่ง e-Mail

4.1 ผู้ใช้งาน e-Mail ต้องตรวจสอบไวรัสกับไฟล์ที่แนบมาพร้อม e-Mail ทุกครั้ง

4.2 หากผู้ใช้งาน e-Mail ต้องการส่ง e-Mail ถึงผู้ใช้งานทุกคนหรือส่งแบบกลุ่ม ควรแจ้งให้ผู้ดูแลระบบทราบ เนื่องจากผู้ดูแลระบบได้สร้างบัญชีผู้ใช้งานแบบกลุ่มไว้แล้ว เพื่ออำนวยความสะดวก และป้องกันการส่ง e-Mail ในลักษณะ Spam mail

4.3 ห้ามผู้ใช้งาน ใช้e-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 นั้นๆ 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 เชื้อชาติหรือเพศ

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 ไปยังผู้รับ ที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

4.3.15 การส่ง e-Mail เพื่อโฆษณาสินค้า ผลิตภัณฑ์หรือส่งข้อความในลักษณะ Spam Mail ไปยังผู้รับ ที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

4.3.16 การส่ง e-Mail ซึ่งส่งผลกระทบทำให้ระบบ e-Mail หรือระบบเครือข่ายลดทอนประสิทธิภาพลง

4.3.17 การส่ง e-Mail เพื่อกระจายไวรัสหรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบ

4.3.18 การส่ง e-Mail ต้องไม่เข้าข่ายการกระทำความผิดหรือขัดต่อกฎหมายอื่นๆ ที่เกี่ยวข้อง

5. การส่ง e-Mail ผ่านบัญชีผู้ใช้งานแบบกลุ่ม

5.1 ผู้ดูแลระบบจัดให้มีระบบบัญชีผู้ใช้งาน e-Mail แบบกลุ่มตามคำร้องขอของหน่วยงาน ทั้งนี้ ผู้ดูแลระบบ ขอสงวนสิทธิ์ในการอนุมัติการขอจดทะเบียนชื่อกลุ่ม ตลอดจนการตั้งชื่อกลุ่ม โดยจะต้องตั้งชื่อกลุ่มตามหลักการ ที่ได้กำหนดไว้ หรือตามความเหมาะสมเป็นกรณีๆ ไป

5.2 ผู้ดูแลระบบใช้เพื่อแจ้งเตือนหรือแจ้งข่าวที่เกี่ยวข้องกับความมั่นคงปลอดภัย หรือการรักษาประสิทธิภาพ ของระบบคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

5.3 ผู้ใช้งานใช้เพื่อส่งข้อมูลหรือเผยแพร่ข่าวสารประชาสัมพันธ์ เพื่อการดำเนินงานตามภารกิจหรือสิทธิประโยชน์ต่างๆ ที่ควรทราบ

6. การระงับ/เพิกถอน บัญชีผู้ใช้งาน e-Mail

6.1 ผู้ดูแลระบบสามารถระงับบัญชีผู้ใช้งาน e-Mail นั้นได้ หากผู้ใช้งานพ้นสภาพจากการสังกัดกรมกิจการผู้สูงอายุ

6.2 ผู้ใช้งานสามารถร้องขอการขยายสิทธิ์การใช้งานบัญชีผู้ใช้ได้ เพื่อคงสิทธิ์เดิมไว้เมื่อต้องพ้นสภาพจาก การสังกัดกรมกิจการผู้สูงอายุ โดยยื่นคำร้องส่งถึงกลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ ทั้งนี้ การอนุญาต และระยะเวลาการขยายสิทธิ์ให้เป็นอำนาจของผู้อำนวยการกองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ

6.3 ผู้ดูแลระบบสามารถเพิกถอนบัญชีผู้ใช้งาน e-Mail ออกจากระบบได้ โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า หากตรวจพบว่าบัญชี e-Mail ของผู้ใช้งานนั้น ไม่มีการใช้งานหรือความเคลื่อนไหวใดๆ เป็นระยะเวลาเกิน 1 ปี

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

เรื่องที่ 14

ข้อปฏิบัติในการใช้สื่อสังคมออนไลน์ (Social Media)

วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแลการเผยแพร่ข้อมูลและการเข้าถึงสื่อเครือข่ายสังคมออนไลน์ของ กรมกิจการผู้สูงอายุ ตลอดจนการแสดงความคิดเห็นของบุคลากรในหน่วยงาน ผ่านสื่อเครือข่ายสังคมออนไลน์ให้เป็นไปอย่างถูกต้อง เหมาะสม เพื่อรักษาภาพลักษณ์ของบุคลากรและการดำเนินงานของหน่วยงานให้มีความเป็นระเบียบเรียบร้อย และเกิดประโยชน์สูงสุด ตลอดจนป้องกันมิให้เกิดการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และที่แก้ไขเพิ่มเติม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. ผู้ใช้งาน หมายถึง เจ้าหน้าที่ของ กรมกิจการผู้สูงอายุ หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งาน อินเทอร์เน็ตของ กรมกิจการผู้สูงอายุ

2. หน่วยงานที่รับผิดชอบ หมายถึง กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน กรมกิจการผู้สูงอายุ (ทนส. กยผ. ผส.) รับผิดชอบในการ ให้บริการอินเทอร์เน็ตของ กรมกิจการผู้สูงอายุ

3. เจ้าหน้าที่/ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ของ (ทนส. กยผ. ผส.) ที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบอินเทอร์เน็ต ของกรมกิจการผู้สูงอายุ

ข้อปฏิบัติ

1. การใช้สื่อสังคมออนไลน์ทั่วไป

1.1 หลักการและแนวปฏิบัติทั่วไป

1.1.1 กรมกิจการผู้สูงอายุ อนุญาตให้ใช้ระบบเครือข่ายสำหรับเข้าถึงสื่อสังคมออนไลน์ประเภทเว็บไซต์ที่ไม่มี เนื้อหาขัดต่อกฎหมาย ศีลธรรม และหลักจรรยาบรรณของหน่วยงาน

1.1.2 หน่วยงานภายใน กรมกิจการผู้สูงอายุ บุคลากร สามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์เพื่อประโยชน์ ในการเผยแพร่ ประชาสัมพันธ์ที่เกี่ยวข้องกับ กรมกิจการผู้สูงอายุ ในการติดต่อสื่อสารระหว่างกันได้ แต่ต้องแยกแยะ ให้ชัดเจนว่าข้อความใดเป็น “ข่าวประชาสัมพันธ์” “ความคิดเห็น” “ความคิดเห็นส่วนบุคคล” “การแลกเปลี่ยน ข่าวสารส่วนตัว” “การเผยแพร่ข่าวสารเรื่องงาน” หรืออื่นๆ และความคิดเห็นดังกล่าวควรคำนึงถึงประโยชน์ สาธารณะด้วย

1.1.3 การเผยแพร่ประชาสัมพันธ์ในนามของหน่วยงาน ผู้เผยแพร่ต้องแสดงตำแหน่งหน้าที่ สังกัดให้ชัดเจน เพื่อความน่าเชื่อถือ และเพื่อให้ผู้ที่ติดตามสามารถใช้ดุลพินิจในการติดตามได้

1.1.4 พึงระมัดระวังการใช้ถ้อยคำและภาษา ที่อาจเป็นการดูหมิ่น หรือหมิ่นประมาทบุคคลอื่น และ ควรใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์

1.1.5 พึงงดเว้นการโต้ตอบด้วยความรุนแรงในกรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง การละเว้นไม่โต้ตอบจะทำให้ความขัดแย้งไม่บานปลายจนหาที่สิ้นสุดไม่ได้

1.1.6 พึงงดเว้นการใช้สื่อสังคมออนไลน์วิพากษ์ วิจารณ์ ตลอดจนแสดงความคิดเห็นในเรื่องที่เป็นข้อมูลภายในหน่วยงาน หรืออาจส่งผลกระทบต่อหน่วยงานได้

1.1.7 พึงใช้รูปแสดงตัวตนที่แท้จริง และพึงงดเว้นการนำรูปบุคคลอื่น รูปบุคคลสาธารณะมาแสดงว่า เป็นรูปของตนเอง

1.1.8 หน่วยงานที่สังกัด อาจใช้รูปสัญลักษณ์ เครื่องหมายแสดงสังกัดได้ แต่ต้องคำนึงถึงความเหมาะสม ในการใช้งาน

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 ละเว้นการส่งข้อมูลที่เป็นข่าวลือ ข่าวไม่ปรากฏที่มา หรือเป็นเพียงการคาดเดา

1.2.3 งดเว้นการส่งต่อข้อความที่เกี่ยวข้องกับหน่วยงานทุกกรณี ยกเว้นข้อความนั้นๆ เป็นที่เผยแพร่ ต่อสาธารณะแล้ว

1.2.4 พึงระลึกเสมอว่า การส่งต่อข้อความที่เป็นเท็จหรือข้อความที่เจ้าของประสงค์จะกระจายข่าวเพื่อสร้างความสับสนวุ่นวายในบ้านเมือง เท่ากับตกเป็นเครื่องมือของบุคคลเหล่านั้น

1.2.5 ควรงดเว้นการส่งต่อข้อความเรื่องบุคคลเสียชีวิต เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้ว

1.2.6 การส่งต่อข้อความเชิญชวนไปร่วมชุมนุมหรือกระทำกิจกรรมทางสังคมใดๆ ต้องตรวจสอบข้อเท็จจริงให้แน่ชัดเสียก่อน

1.3 หลักความรับผิดชอบ

1.3.1 ควรแสดงความรับผิดชอบด้วยการขอโทษ แสดงความเสียใจทันทีเมื่อรู้ว่ามีการเผยแพร่ข้อมูลที่ผิดพลาดหรือกระทบต่อบุคคลอื่น

1.3.2 กรณีการส่งต่อข้อความข่าวลือหรือข่าวเท็จ ต้องแก้ไขข้อความนั้นโดยทันที หากสามารถตรวจสอบข้อเท็จจริงได้ พึงแสดงข้อเท็จจริงให้เป็นที่ประจักษ์

1.3.3 หากพบข้อมูลที่ไม่ถูกต้อง ควรดำเนินการแก้ไขอย่างรวดเร็ว และแสดงให้เห็นอย่างชัดเจนว่าเป็นผู้ดำเนินการดังกล่าว

1.3.4 หากพบข้อมูลใดๆ ที่ไม่เหมาะสม (เช่น สิ่งที่เป็นลิขสิทธิ์ของผู้อื่น หรือการแสดงความคิดเห็นที่เป็นการหมิ่นประมาท) ควรดำเนินการอย่างรวดเร็ว โดยลบข้อความดังกล่าวออกทันที เพื่อลดโอกาสที่จะเกิดข้อขัดแย้งทางกฎหมาย และผลกระทบด้านลบต่อหน่วยงาน

1.4 การพบข้อร้องเรียนและประเด็นขัดแย้ง

หากพบเห็นข้อร้องเรียนหรือการบิดเบือนข้อเท็จจริงเกี่ยวกับบริการอิเล็กทรอนิกส์ของหน่วยงานหรือพบเห็นข้อร้องเรียนอื่นๆ ที่เกี่ยวข้องกับหน่วยงาน ควรหลีกเลี่ยงการถกเถียงหรือโต้ตอบ ซึ่งนำไปสู่การกระตุ้นให้เกิดอารมณ์รุนแรง และพาดพิงไปยังผู้อื่น

1.5 การไม่เปิดเผยข้อมูลที่เป็นความลับ

การพูดคุยแลกเปลี่ยนกับชุมชนออนไลน์ รวมถึงการโพสต์ข้อความที่เกี่ยวข้องกับงานประจำ เป็นสิ่งที่บุคคลสามารถกระทำได้ ถ้าไม่ขัดต่อหลักจรรยาบรรณของหน่วยงาน เว้นแต่ข้อมูลนั้นเป็นข้อมูลที่มีความสำคัญ

หรือเป็นความลับของหน่วยงาน ซึ่งห้ามเปิดเผยโดยเด็ดขาด เช่น รายละเอียดของโครงการงบลงทุน ข้อมูล สำคัญทางการเงิน งานวิจัย เป็นต้น

1.6 ความน่าเชื่อถือของข้อมูล

ไม่โพสต์ข้อความที่เป็นเท็จหรือก่อให้เกิดความเข้าใจผิด และระบุที่มาของข้อมูลนั้นอย่างชัดเจน การโพสต์ข้อความใดๆ ควรพิจารณาเนื้อหาอย่างรอบคอบและระมัดระวัง โดยเฉพาะการเปิดเผยข้อมูลส่วนบุคคล

1.7 ไม่ละเมิดกฎหมายลิขสิทธิ์และทรัพย์สินทางปัญญา

ไม่ละเมิดกฎหมายลิขสิทธิ์การใช้งานใดๆ ที่เป็นลิขสิทธิ์ของผู้อื่น รวมทั้งของหน่วยงานเอง ทั้งนี้ การอ้างอิงคำพูดหรือข้อมูลของผู้อื่น ควรใช้ข้อความที่คัดลอกมาสั้นๆ เท่านั้น และควรระบุถึงที่มาของแหล่งข้อมูลหรือเจ้าของผลงานเสมอ การเชื่อมลิงก์ไปยังงานของเจ้าของข้อมูล ถือเป็นการปฏิบัติที่เหมาะสมกว่าการคัดลอกข้อมูลมาใช้งาน

1.8 คำนึงถึงผู้เข้าชมและผู้เกี่ยวข้อง

บุคลากรของหน่วยงานไม่ควรโพสต์ข้อมูลใดๆ ที่ขัดแย้งกับข้อกำหนดของหน่วยงาน รวมถึงละเว้นการแสดงออกถึงความคิดเห็นที่ก้าวร้าว หมิ่นประมาทำดูถูกเป็นการส่วนตัว ลามกอนาจาร และอื่นๆ ที่ไม่ เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วยุหรือขัดต่อจริยธรรม เช่น การเมือง ศาสนา ชนชาติ เป็นต้น การแสดงความคิดเห็นต่างๆ ที่โพสต์โดยบุคลากรของหน่วยงาน โดยที่ไม่ได้รับมอบหมายอย่างเป็นทางการ 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

การใช้สื่อเครือข่ายสังคมออนไลน์จะต้องไม่รบกวนการปฏิบัติงานหรือหน้าที่ความรับผิดชอบที่ได้รับ มอบหมาย

1.12 การฝ่าฝืนและบทลงโทษ

1.12.1 หน่วยงานไม่รับผิดชอบต่อผลของการกระทำที่เกิดจากผู้ใช้งาน และ/หรือบัญชีผู้ใช้งานที่ฝ่าฝืนต่อนโยบายนี้

1.12.2 หากหน่วยงานตรวจสอบแล้วพบว่าบัญชีผู้ใช้งานใดละเมิดต่อนโยบายนี้ หน่วยงานขอสงวนสิทธิ์ ในการระงับ และ/หรือยกเลิกบัญชีผู้ใช้งานอินเทอร์เน็ต และ/หรือหยุดให้บริการแก่ผู้ใช้งานนั้น

1.12.3 หากการกระทำอันฝ่าฝืนต่อนโยบายนี้เป็นความผิดตามกฎหมาย ให้หน่วยงานดำเนินคดีตามกฎหมายโดยลำดับต่อไป

2. การใช้สื่อสังคมออนไลน์ในระดับบุคคล

การนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรในหน่วยงาน มีข้อปฏิบัติดังนี้

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

2.2 กรณีใช้ชื่อบัญชีผู้ใช้งานที่ระบุถึงตัวตนอันอาจทำให้ผู้ติดตาม (followers) หรือเพื่อนในเครือข่าย (friends) เข้าใจได้ว่าเป็นบุคลากรในหน่วยงาน ผู้ใช้งานพึงระมัดระวังการนำเสนอข้อมูลข่าวสารและการแสดงความคิดเห็น ที่อาจนำไปสู่การละเมิดจริยธรรมของผู้อื่น

2.3 ในการรวบรวมข้อมูลข่าวสาร การนำเสนอ และการแสดงความคิดเห็น ผู้ใช้งานพึงระวังการละเมิดสิทธิ ส่วนบุคคล ศักดิ์ศรีความเป็นมนุษย์ สิทธิเด็กและสตรี ภาพอุจาด ลามก อนาจาร

2.4 หากการนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรในหน่วยงาน เกิดความผิดพลาด จนก่อให้เกิดความเสียหายต่อบุคคลหรือหน่วยงานอื่น ผู้ใช้งานต้องดำเนินการแก้ไขข้อความ ที่มีปัญหาโดยทันที พร้อมทั้งแสดงถ้อยคำขอโทษต่อบุคคลหรือหน่วยงานที่ได้รับความเสียหาย ทั้งนี้ ต้องให้ผู้ที่ ได้รับความเสียหายได้มีโอกาสชี้แจงข้อมูลข่าวสารในด้านของตนด้วย

3. การใช้สื่อสังคมออนไลน์ในระดับหน่วยงาน

3.1 การจัดทำสื่อสังคมออนไลน์ในระดับหน่วยงาน ควรที่จะคำนึงถึงหลักการพื้นฐานดังต่อไปนี้

3.1.1 วัตถุประสงค์ของการจัดทำ

3.1.2 แนวทางการใช้งานสื่อสังคมออนไลน์เพื่อช่วยพัฒนาและดำเนินงานของหน่วยงาน

3.2 การตั้งค่าบนสื่อสังคมออนไลน์ของหน่วยงาน

การใช้ชื่อหรือตราสัญลักษณ์ของหน่วยงาน เพื่อเปิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ โดยมีวัตถุประสงค์เพื่อการประชาสัมพันธ์ เผยแพร่ข้อมูลข่าวสาร หรือการสื่อสารภายในหน่วยงาน จะต้องผ่านการรับทราบและเห็นชอบจาก DCIO ของหน่วยงาน หรือผู้อำนวยการกองยุทธศาสตร์และแผนงานก่อน รวมทั้งจะต้องมีการตระหนักถึงหลักการพื้นฐานดังที่กล่าวมาข้างต้น

3.3 การนำเสนอข่าวโดยการใช้สื่อสังคมออนไลน์ของหน่วยงาน ควรมีหลักในการอ้างอิงถึงหน่วยงานดังต่อไปนี้

3.3.1 ชื่อหน่วยงานที่เผยแพร่ข้อมูลข่าวสาร

3.3.2 รายละเอียด สัญลักษณ์ หรือชื่อย่อ ที่แสดงถึงหน่วยงาน

3.3.3 มาตรการทางเทคนิคที่ยืนยันถึงสถานะและความมีตัวตนของหน่วยงาน (ถ้ามี)

3.3.4 ชื่อตัวแทนหน่วยงานที่นำเสนอข่าวสาร (ถ้ามี)

3.4 การปกป้องข้อมูลที่เป็นความลับของหน่วยงาน

ในกรณีที่มีบัญชีผู้ใช้งานของหน่วยงาน ควรมีการตั้งค่าความเป็นส่วนตัว (Privacy) เพื่อป้องกันไม่ให้ บุคคลอื่นโพสต์ข้อความหรือเข้าถึงข้อมูลที่มีความสำคัญหรือเป็นความลับของหน่วยงาน ซึ่งห้ามเปิดเผย โดยเด็ดขาด เช่น รายละเอียดของโครงการงบลงทุน ข้อมูลสำคัญทางการเงิน งานวิจัย เป็นต้น โดยมีการ กำหนดให้อยู่ใน

วงจำกัดเท่านั้น และควรให้ความระมัดระวังในการโพสต์ข้อความเฉพาะกลุ่มหรือส่วนบุคคล ที่ไม่ต้องการเผยแพร่ให้สาธารณะชนรับรู้

3.5 การนำเสนอข้อมูลข่าวสารของหน่วยงานผ่านสื่อสังคมออนไลน์

ควรเป็นไปตามข้อบังคับจริยธรรม หลักเกณฑ์ และข้อปฏิบัติของหน่วยงานตามที่ได้ระบุไว้ และต้องไม่ เป็นการสร้างความเกลียดชังระหว่างคนในชาติ จนอาจนำไปสู่ความขัดแย้งและเสียหายรุนแรงขึ้นในสังคม

3.6 หน่วยงานต้องให้ความเคารพและยอมรับข้อมูลข่าวสารหรือภาพข่าวที่ผลิตโดยบุคคลอื่นผ่านสื่อสังคมออนไลน์

การคัดลอกข้อความใดๆ จากสื่อสังคมออนไลน์ พึงได้รับการอนุญาตจากเจ้าของข้อความนั้นๆ ตามแต่กรณีจำเป็น เพื่อประโยชน์ในการเผยแพร่ข้อมูลข่าวสาร ต้องอ้างอิงถึงแหล่งที่มาของข้อความและข่าวสารนั้น โดยรับรู้ถึงสิทธิ หรือลิขสิทธิ์ของหน่วยงานหรือบุคคลผู้เป็นเจ้าของข้อมูลดังกล่าว

3.7 หลีกเลี่ยงการสื่อสาร

ควรหลีกเลี่ยงการสื่อสารข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง และข้อมูลใดๆ ของหน่วยงานหรือที่เกี่ยวข้องกับหน่วยงานที่ก่อให้เกิดความขัดแย้ง หรือโต้แย้งในสังคม ขัดต่อหลักกฎหมายทั้งในประเทศและในระดับสากล หรือการเสนอเรื่องราวตลกไร้สาระ เพ้อฝัน ไร้ศีลธรรม เกินความจริง ไม่ให้เกียรติ ดูถูกเหยียดหยามและลอกเลียนแบบผู้อื่น

3.8 ไม่เผยแพร่ข้อมูลที่เป็นความลับของหน่วยงาน

ไม่นำข้อมูลที่เป็นความลับทุกระดับชั้นของหน่วยงาน มาเผยแพร่ผ่านสื่อสังคมออนไลน์ทุกประเภท

4. การใช้งานเครื่องคอมพิวเตอร์และเครือข่าย

4.1 ห้ามนำข้อมูลส่วนตัวที่ไม่เกี่ยวข้องกับงานของหน่วยงานมาเก็บไว้ในเครื่องคอมพิวเตอร์ของหน่วยงาน

4.2 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขายหรือเผยแพร่สิ่งที่ผิดกฎหมาย การตั้งกระทู้หรือตอบกระทู้บน

กระดานถาม-ตอบ หรือบนเว็บไซต์ประเภท social network หรือบริการบล็อค (Blog) เพื่อเผยแพร่สิ่งที่ผิด กฎหมาย และขัดต่อศีลธรรม เป็นต้น

4.3 ห้ามเข้าใช้เครือข่ายคอมพิวเตอร์ด้วยบัญชีของผู้อื่น ทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของบัญชี

4.4 ห้ามเข้าถึงระบบคอมพิวเตอร์และข้อมูลที่มีมาตรการป้องกันการเข้าถึงของผู้อื่น เพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม เช่น มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นเข้ามาใช้เครื่องคอมพิวเตอร์หรือเข้าดูข้อมูล เป็นต้น

4.5 ห้ามเผยแพร่ข้อมูลของผู้ใช้งานหรือหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้ที่เป็นเจ้าของหรือเป็นผู้จัดทำ ข้อมูลนั้นๆ

4.6 ห้ามก่อกวน ขัดขวาง ชะลอหรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของหน่วยงานและระบบเครือข่ายอื่นเกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ เพื่อให้เกิดผลชะลอการทำงาน

การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) หรือทำให้ เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายทำงานได้ช้าลง เป็นต้น

4.7 ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมประเภทที่ละเมิดลิขสิทธิ์และชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะ โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์หรือเพื่อนำไปใช้เป็นเครื่องมือในการกระทำผิดบนเครือข่ายคอมพิวเตอร์

4.8 ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของหน่วยงานและของผู้อื่นที่อยู่ระหว่างการรับและ ส่งในเครือข่ายคอมพิวเตอร์

4.9 ห้ามส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-Mail) ในรูปแบบภาพนิ่ง ภาพเคลื่อนไหว ภาพที่เกิดจากการสร้างขึ้น ตัดต่อ ดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ และข้อความที่เกี่ยวกับการลามก อนาจาร การละเมิดทรัพย์สินทางปัญหา การหมิ่นพระบรมเดชานุภาพ การสร้างปัญหาความมั่นคงของประเทศ หรือการทำให้บุคคลเสียชื่อเสียงหรือได้รับความอับอาย การปลอมแปลงหรือแอบอ้างชื่อเป็นบุคคลอื่นเพื่อสร้าง ความเข้าใจผิด การส่งอีเมลมากจนล้นระบบเครือข่ายคอมพิวเตอร์ของบุคคลอื่นจนทำให้เกิดความยุ่งยาก ในการใช้งานระบบเครือข่ายคอมพิวเตอร์

4.10 ห้ามเผยแพร่หรือเข้าถึงสื่อที่เกี่ยวกับเรื่องลามกอนาจาร การละเมิดทรัพย์สินทางปัญญา การหมิ่น พระบรมเดชานุภาพ การสร้างปัญหาความมั่นคงของประเทศ หรือการทำให้บุคคลเสียชื่อเสียงหรือได้รับความอับอาย

4.11 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์เพื่อประกอบธุรกิจการค้า หรือเปิดให้บริการใดๆ นอกจาก
จะได้รับอนุญาตจากหน่วยงานหรือผู้รับผิดชอบทรัพยากรและเครือข่ายคอมพิวเตอร์

4.12 ห้ามกระทำการเคลื่อนย้าย หรือทำการใดๆ ต่อทรัพยากรและเครือข่ายคอมพิวเตอร์ของหน่วยงาน โดยพลการ นอกจากได้รับอนุญาตจากหน่วยงานหรือผู้รับผิดชอบทรัพยากรและเครือข่ายคอมพิวเตอร์

4.13 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์อื่นใดที่ขัดต่อนโยบาย ระเบียบ ข้อบังคับ และประกาศ ของหน่วยงาน

5. การใช้งานแบนด์วิดท์เครือข่ายที่เหมาะสม

5.1 รณรงค์ให้ผู้ใช้งานเครือข่ายใช้งานระบบอีเมลที่หน่วยงานจัดให้ เนื่องจากการที่ผู้ใช้งานเครือข่ายใช้ระบบอีเมลจากภายนอก เช่น Hotmail Gmail เป็นต้น ทำให้ผู้ใช้งานนั้นต้องเชื่อมต่อเครื่องลูกข่ายของตนไปยังเครื่องแม่ข่ายภายนอก ส่งผลให้มีการใช้งานแบนด์วิดท์ของเครือข่ายหน่วยงานเป็นจำนวนมาก ทำให้ เหลือแบนด์วิดท์ เพื่อการใช้งานแอปพลิเคชันอื่นน้อยลง

5.2 หลีกเลี่ยงการสำรองข้อมูลขึ้นระบบ Cloud Computing หรือการดาวน์โหลดไฟล์ขนาดใหญ่ในช่วงเวลา ปฏิบัติงาน กรณีตั้งค่าการสำรองข้อมูลขึ้นระบบ Cloud อัตโนมัติ ควรตั้งเวลาที่เหมาะสม เช่น ระหว่างเวลา 23.00 – 03.00 น. เป็นต้น

5.3 ควรใช้พร็อกซี่ (Proxy) ในการเข้าใช้งานเว็บไซต์ เนื่องจากเครื่องลูกข่ายไม่ต้องเชื่อมโยงเข้ากับเครื่องแม่ข่าย ที่อยู่ระยะไกลทุกครั้งที่มีการเรียกใช้เว็บไซต์ ทำให้ลดการใช้งานแบนด์วิดท์ของเครือข่ายลงได้

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

5.5 กรณีที่หน่วยงานตรวจสอบแล้วพบว่าบัญชีผู้ใช้งานใดมีพฤติกรรมสุ่มเสี่ยง เช่น โหลดบิต เป็นต้น หน่วยงานขอสงวนสิทธิ์ในการระงับ และ/หรือยกเลิกบัญชีผู้ใช้งานอินเทอร์เน็ต และ/หรือหยุดให้บริการแก่ผู้ใช้งานนั้น

5.6 รณรงค์ให้ผู้ใช้งานเครือข่ายลดการเข้าถึงเว็บไซต์ประเภทสื่อสังคมออนไลน์ ที่ใช้เผยแพร่ข้อมูล และ แสดงความคิดเห็นบนโลกออนไลน์ เช่น Facebook Twitter เป็นต้น ในช่วงเวลาปฏิบัติงาน และ/หรือ ในช่วง เวลาที่มีการใช้งานแบนด์วิดท์เครือข่ายปริมาณสูง และ/หรือส่งผลรบกวนการปฏิบัติงานหรือหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย เนื่องจากเว็บไซต์ดังกล่าวมีแอปพลิเคชันที่จองช่องทางวงจรอินเทอร์เน็ตอยู่ตลอดเวลา ส่งผลให้แบนด์วิดท์เต็มหรือเหลือน้อยได้

5.7 หน่วยงานขอสงวนสิทธิ์ในการจัดสรรแบนด์วิดท์ (Bandwidth Quota) ของผู้ใช้งานแต่ละคน เพื่อการ จัดการทรัพยากรแบนด์วิดท์ที่เหมาะสม