นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมที่ดิน

๑. คำนำ

ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน เป็นระบบที่มีความสำคัญต่อการให้บริการประชาชน หน่วยงานภาครัฐ และเอกชน รวมทั้งการใช้งานภายในกรมที่ดินส่วนกลาง และสำนักงานที่ดินทั่วประเทศ ดังนั้น เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์ การปฏิบัติงานและบริหารราชการได้อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยเชื่อถือได้ และสามารถดำเนินงานได้อย่างต่อเนื่อง ประกอบกับพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยให้ผ่านความเห็นชอบของคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ก่อน จึงมีผลบังคับใช้ กรมที่ดินจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมที่ดิน

๒. วัตถุประสงค์

๒.๑ เพื่อให้การดำเนินงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดินมีความมั่นคงปลอดภัย สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพอันจะทำให้การดำเนินธุรกรรมมีความถูกต้องเชื่อถือได้ตามมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

๒.๒ เพื่อกำหนดแนวทางปฏิบัติให้ผู้บริหาร ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ใช้งานระบบ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน

๒.๓ เพื่อป้องกันเจ้าหน้าที่ผู้ใช้งานและผู้เกี่ยวข้องไม่ให้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๓. กำหนดคำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

“ผู้ใช้งาน” หมายถึง บุคคลที่ได้รับอนุญาต ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาทซึ่งกรมที่ดินกำหนด ได้แก่บุคคล ดังนี้

- “ผู้บริหาร” หมายถึง อธิบดีหรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน
- “ผู้ดูแลระบบ” หมายถึง ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือผู้ได้รับมอบหมายให้ควบคุมดูแลบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน
- “เจ้าหน้าที่” หมายถึง บุคลากรในสังกัดกรมที่ดิน และรวมถึงบุคคลภายนอกซึ่งได้รับอนุญาตให้เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน

“สิทธิของผู้ใช้งาน” หมายถึง อำนาจอันชอบธรรมที่ผู้ใช้งานได้รับมอบหมายในการเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน

“สินทรัพย์” หมายถึง ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การควบคุมและจำกัดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน ที่เกี่ยวกับการให้บริการและข้อมูลตามความจำเป็น ในการใช้งาน มีการป้องกันการลักลอบการเข้าถึงระบบโดยผู้ที่ไม่มีสิทธิทั้งจากภายในและภายนอกกรมที่ดิน

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การคงไว้ซึ่งความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งานของข้อมูลในระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน

“เหตุการณ์ด้านความมั่นคงปลอดภัย” (Security incidents) หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดินหรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อนหรือสร้างความเสียหายได้ในที่สุด ซึ่งส่งผลให้เป็นการละเมิดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมที่ดิน เช่น การอนุญาตให้ผู้อื่นเข้าใช้งานระบบ การไม่กำหนดรหัสผ่านในการเข้าใช้งานระบบ การเปิดเผยเอกสารสำคัญให้บุคคลภายนอกล่วงรู้ โปรแกรมไม่พึงประสงค์ ระบบถูกบุกรุกทางเครือข่าย หรือการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” ได้แก่ สถานการณ์ที่ผู้ดูแลระบบไม่ต้องการให้เกิดขึ้นหรือสร้างความเสียหายกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน โดยผู้ดูแลระบบไม่ได้คาดการณ์ไว้ว่าจะเกิดขึ้น เช่นโปรแกรมไม่พึงประสงค์ โปรแกรมทำงานผิดพลาดหรือไม่ถูกต้อง ระบบถูกบุกรุกทางเครือข่าย ข้อมูลสำคัญถูกเปลี่ยนแปลงหรือสูญหาย หน้าเว็บไซต์ถูกเปลี่ยนแปลง การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต ระบบถูกโจมตีจนไม่สามารถให้บริการได้ การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย หรือเหตุการณ์อื่น ๆ ที่เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของกรมที่ดิน

“สำนักเทคโนโลยีสารสนเทศ” หมายถึง หน่วยงานที่ดำเนินการเกี่ยวกับระบบสารสนเทศและระบบงานคอมพิวเตอร์และเป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศของกรมที่ดิน โดยมีหน้าที่ศึกษาวิเคราะห์เพื่อพัฒนาระบบสารสนเทศและระบบงานคอมพิวเตอร์ของกรมที่ดิน และปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่ายสื่อสาร” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการเชื่อมโยง หรือการส่งข้อมูลสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของกรมที่ดิน ซึ่งการเชื่อมโยงเป็นได้ทั้งในรูปแบบใช้สายและแบบไร้สาย โดยระบบเครือข่ายสื่อสาร ได้แก่ ระบบเครือข่ายระยะใกล้ (Local Area Network: LAN) ระบบเครือข่ายระยะไกล (Wide Area Network: WAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet)

“ระบบเครือข่ายสื่อสารระยะใกล้” หมายถึง เครือข่ายที่เชื่อมโยงกันในพื้นที่ใกล้เคียงกัน

“ระบบเครือข่ายสื่อสารระยะไกล” หมายถึง เครือข่ายเชื่อมโยงกันในระยะทางที่ห่างไกล

“ระบบอินทราเน็ต” หมายถึง ระบบเครือข่ายสื่อสารภายในที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในกรมที่ดิน

“ระบบอินเทอร์เน็ต” หมายถึง ระบบเครือข่ายสื่อสารที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ของกรมที่ดินเข้ากับระบบเครือข่ายสื่อสารอินเทอร์เน็ตทั่วโลก

“สารสนเทศ” หมายถึง ข้อมูลที่ผ่านการประมวลผล การจัดระเบียบ ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

“ระบบเทคโนโลยีสารสนเทศและการสื่อสาร” หมายถึง ระบบงานของกรมที่ดินที่ประกอบด้วยระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร เจ้าหน้าที่ผู้ใช้ระบบ เจ้าหน้าที่ผู้พัฒนาระบบ เจ้าหน้าที่ผู้จัดการดูแลระบบ และผู้บริหารของกรมที่ดิน นำมาทำงานร่วมกันเพื่อกำหนดวัตถุประสงค์ รวบรวมจัดเก็บข้อมูล ประมวลผลข้อมูล และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้ระบบและผู้บริหารของกรมที่ดินสามารถนำมาใช้ประโยชน์ในการวางแผนเพื่อช่วยสนับสนุนการปฏิบัติงาน การตัดสินใจ การบริหาร การวิเคราะห์และติดตามผลการดำเนินงานของหน่วยงานระดับต่าง ๆ ของกรมที่ดิน

“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” หมายถึง พื้นที่ที่กรมที่ดินอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

(๑) พื้นที่ทำงานทั่วไป หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์แบบพกพา ที่ใช้งานประจำโต๊ะทำงาน

(๒) พื้นที่ทำงานของผู้ดูแลระบบ

(๓) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่ายสื่อสาร

(๔) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

(๕) พื้นที่ใช้งานระบบเครือข่ายไร้สาย

“รหัสผ่าน (Password)” หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศและการสื่อสาร

“การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การดำเนินการรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน ประกอบด้วยคุณสมบัติพื้นฐาน ๓ ประการ ดังนี้

(๑) การรักษาความลับ (Confidentiality) คือ การเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

(๒) บูรณภาพ (Integrity) คือ การรับรองว่าข้อมูลจะไม่ถูกกระทำการใด ๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

(๓) ความพร้อมใช้งาน (Availability) คือ การรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศและการสื่อสารทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

“วิธีการปฏิบัติ” หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวปฏิบัติ” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

“ชุดคำสั่งไม่พึงประสงค์” (Malware) หมายถึง ชุดคำสั่งที่มีผลทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

“จดหมายอิเล็กทรอนิกส์ (e-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายสื่อสารที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP, POP3 หรือ IMAP

๔. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมที่ดิน

ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) เป็นผู้ควบคุม ดูแล และรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่อาจเกิดขึ้นกรณีระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือข้อมูลสารสนเทศ เกิดความเสียหายหรืออันตรายใด ๆ แก่กรมที่ดินหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมที่ดิน และให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการควบคุม ดูแลให้การปฏิบัติงานเป็นไปตามนโยบายและแนวปฏิบัติฯ

๔.๑ การรักษาความมั่นคงปลอดภัยของการเข้าถึงและการควบคุมการใช้งานสารสนเทศ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เป็นการกำหนดชื่อผู้ใช้งาน และรหัสผ่านตามสิทธิในการเข้าถึงข้อมูล เครือข่าย ระบบปฏิบัติการ รวมถึงโปรแกรมประยุกต์หรือแอพลิเคชั่น และสารสนเทศต่าง ๆ และมีการควบคุมการเข้าถึงระบบเครือข่ายสื่อสารเพื่อป้องกันการบุกรุกผ่านระบบเครือข่ายสื่อสารจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก รวมทั้งมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดินได้

๔.๒ การรักษาความมั่นคงปลอดภัยการควบคุมการเข้าออกศูนย์สารสนเทศ

เป็นการควบคุมการเข้าออกศูนย์สารสนเทศที่ดิน และควบคุมความเป็นระเบียบเรียบร้อยของอุปกรณ์และสถานที่ภายในศูนย์สารสนเทศที่ดิน

๔.๓ การรักษาความมั่นคงปลอดภัยการใช้งานเครื่องคอมพิวเตอร์

เป็นการกำหนดแนวทางการใช้งานของผู้ใช้งานระบบให้สามารถใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ได้อย่างปลอดภัยและมีประสิทธิภาพ

๔.๔ การรักษาความมั่นคงปลอดภัยการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

เป็นการกำหนดแนวทางให้ผู้ใช้งานสามารถใช้งานอินเทอร์เน็ต และจดหมายอิเล็กทรอนิกส์ได้อย่างถูกต้อง ปลอดภัยและไม่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้อง

๔.๕ การรักษาความมั่นคงปลอดภัยการบริหารจัดการสินทรัพย์และเครือข่ายสื่อสาร

เป็นการกำหนดการควบคุมและบริหารจัดการสินทรัพย์และเครือข่ายสื่อสาร ให้มีความมั่นคงปลอดภัยและพร้อมใช้งานอยู่เสมอ

๔.๖ การรักษาความมั่นคงปลอดภัยการสำรองและกู้คืนข้อมูล

เป็นการกำหนดแนวทางการสำรองและกู้คืนข้อมูลทุกระบบ และจัดทำแผนฉุกเฉินในกรณีที่ระบบไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ได้

๔.๗ การรักษาความมั่นคงปลอดภัยด้านการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

เป็นการกำหนดแนวทางการจัดทำแผนประเมินความเสี่ยง และแผนฉุกเฉินกรณีเกิดภัยพิบัติ

๔.๘ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เป็นการส่งเสริมให้บุคลากรของกรมที่ดินตระหนักถึงเรื่องของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรมที่ดิน ตามนโยบายและแนวทางปฏิบัติที่กำหนด

๕. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมที่ดิน

๕.๑ การรักษาความมั่นคงปลอดภัยของการเข้าถึงและการควบคุมการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๕.๑.๑ การควบคุมการเข้าถึงสิทธิของผู้ใช้งาน

(๑) มีการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบ โดยพิจารณาจากหน้าที่ความรับผิดชอบในข้อมูลของผู้ใช้งานแต่ละกลุ่มงาน

(๒) ผู้ใช้งานต้องทำหนังสือขอมีสิทธิเป็นลายลักษณ์อักษร ให้กับสำนักเทคโนโลยีสารสนเทศ หรือหน่วยงานที่ได้รับมอบหมาย

(๓) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย เป็นผู้พิจารณาอนุญาต

๕.๑.๒ การบริหารจัดการสิทธิผู้ใช้งาน

(๑) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ได้กำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารนั้น ๆ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งาน และหน้าที่ความรับผิดชอบของผู้ใช้งานเป็นไปตามระเบียบที่กรมที่ดินกำหนด รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานเมื่อผู้ใช้มีการย้าย/เปลี่ยนตำแหน่งงานใหม่/ลาออก/เกษียณ ภายในกรมที่ดินอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง

(๒) ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๓) เมื่อเจ้าหน้าที่ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้สำนัก/กอง/สำนักงานที่ดิน แจ้งสำนักเทคโนโลยีสารสนเทศทันที เพื่อถอดถอนสิทธิของผู้ที่ลาออกหรือเปลี่ยนสิทธิในระบบทันทีที่ได้รับแจ้ง

(๔) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยควบคุมการใช้งานอย่างเข้มงวด เช่นกำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว และมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน และต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมาย

(๕) ห้ามผู้ใช้งานซึ่งไม่ได้รับสิทธิให้เข้าใช้งานบุกรุกเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ไม่ว่าด้วยวิธีการใด ๆ

๕.๑.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

(๑) ผู้ดูแลระบบมีการกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ และระบบต้องไม่แสดงรหัสผ่านให้เห็นบนหน้าจอ

(๒) ระบบต้องกำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเมื่อเข้าระบบครั้งแรก

(๓) ระบบมีการกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๓ ครั้ง

(๔) ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยพิจารณาจากลำดับชั้นความลับของข้อมูล หรือความสำคัญตามภารกิจ โดยกำหนดให้ระบบมีการบันทึกประวัติการเปลี่ยนรหัสผ่าน เพื่อป้องกันการใช้รหัสซ้ำ เช่น ระบบสารบรรณอิเล็กทรอนิกส์ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๖ เดือน ระบบงานให้บริการในสำนักงานที่ดินต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๓ เดือน

(๕) การแจ้งปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ผู้ใช้งานติดต่อผู้ดูแลระบบ เช่น ลืมชื่อผู้ใช้งานหรือรหัสผ่าน

(๖) การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย โดยใส่ซองปิดผนึก และประทับตรา “ลับ” และส่งไปยังผู้ใช้งานพร้อม “แนวปฏิบัติสำหรับการใช้งานรหัสผ่าน” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามแนวปฏิบัติโดยเคร่งครัด

(๗) ผู้ใช้งานต้องตอบยืนยันการได้รับรหัสผู้ใช้งานและรหัสผ่านเป็นลายลักษณ์อักษรด้วยตนเอง

๕.๑.๔ การใช้งานรหัสผ่านสำหรับผู้ใช้งาน

(๑) ผู้ใช้ต้องใช้ชื่อผู้ใช้งาน และรหัสผ่านของตนเองในการใช้งานระบบ เพื่อป้องกันการปฏิเสธความรับผิดชอบ

(๒) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ต้องเปลี่ยนรหัสผ่านที่ได้รับโดยทันที

(๓) ผู้ใช้งานต้องกำหนดรหัสผ่าน และเปลี่ยนรหัสผ่านของตนเองในการใช้งานอย่างสม่ำเสมอ อย่างน้อยทุก ๆ ๓ เดือน หรือตามหลักเกณฑ์ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๔) ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ และระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใด ๆ ทั้งสิ้น เว้นแต่กรณีผู้ใช้งานที่มีอำนาจอนุมัติใด ๆ ในระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถปฏิบัติราชการอันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าว เพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้ว ให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

(๕) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๖) ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “๑๒๓๔๕”

(๗) ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่นชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

(๘) ไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

(๙) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์

(๑๐) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

(๑๑) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๑๒) ผู้ใช้งานต้องไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงาน และในกรณีใช้งานส่วนตัว

(๑๓) ผู้ใช้งานต้องออกจากระบบ (Log off) ทันที เมื่อไม่ใช้งาน เพื่อป้องกันผู้ใช้งานอื่นลักลอบใช้สิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๑๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหากสงสัยว่ารหัสผ่านเกิดการรั่วไหล

๕.๑.๕ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

(๑) ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงาน

(๒) เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่เหมาะสมกับหน้าที่และความรับผิดชอบ

(๓) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติ และกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งาน ในการขออนุญาตเข้าระบบงานนั้น ต้องทำบันทึกและกรอกแบบฟอร์มตามที่สำนักเทคโนโลยีสารสนเทศกำหนด และให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้มีอำนาจที่เป็นเจ้าของข้อมูลและ/หรือเจ้าของระบบงาน เพื่อเก็บไว้เป็นหลักฐาน

(๔) การลงทะเบียนเจ้าหน้าที่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ หรือเมื่อย้าย/เปลี่ยนตำแหน่งงานใหม่/ลาออก/เกษียณ ภายในกรมที่ดิน หน่วยงาน/ผู้ใช้งานต้องทำบันทึก และกรอกแบบฟอร์มตามที่สำนักเทคโนโลยีสารสนเทศกำหนด เพื่อให้มีสิทธิหรือยกเลิกสิทธิต่าง ๆ ในการใช้งาน

๑) ผู้ใช้งานรายใหม่ ต้องทำการกรอกข้อมูลเพื่อขอลงทะเบียนในแบบ “คำขออนุญาตเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร”

๒) ผู้ใช้งานรายใหม่ลงนามในแบบคำขอเพื่อรับทราบแนวทางปฏิบัติ และได้รับอนุมัติจากผู้บังคับบัญชาของผู้ขอ

๓) ยื่นคำขอต่อสำนักเทคโนโลยีสารสนเทศ

๔) ผู้ใช้งานตอบยืนยันการได้รับรหัสผู้ใช้และรหัสผ่านด้วยตนเอง

๕) ผู้ดูแลระบบจะกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เหมาะสมกับการใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน โดยได้รับความเห็นชอบจากผู้มีอำนาจเป็นลายลักษณ์อักษร และจะมีการทบทวนสิทธิอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง หรือในกรณีกองการเจ้าหน้าที่มีคำสั่งย้าย/เปลี่ยนตำแหน่งงานใหม่/ลาออก/เกษียณ หรือในกรณีที่หน่วยงานต้นสังกัดมีบันทึกถึงผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ เพื่อให้มีสิทธิหรือยกเลิกสิทธิต่าง ๆ ในการใช้งาน

(๕) กรณีผู้ใช้ไม่เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระบบ ผู้ดูแลระบบทุกระบบ จะต้องมีกลไกยกเลิกสิทธิเพื่อให้รหัสผ่านของผู้ใช้หมดสิทธิการใช้ระบบทันทีเมื่อครบกำหนดที่ระบุไว้ในแต่ละระบบ

๕.๑.๖ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

(๑) ผู้ดูแลระบบ มีการกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับรวมทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

(๒) เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๓) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบมีการกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

(๔) การรับส่งข้อมูลระดับชั้นความลับ ตั้งแต่ชั้น “ลับ” ขึ้นไปผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN

(๕) มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของสำนักงาน หรือกรณีส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องสำรองข้อมูลไว้ในสื่อบันทึกข้อมูล และลบข้อมูลสำคัญที่เก็บอยู่ในเครื่องคอมพิวเตอร์ออกก่อน

๕.๑.๗ การควบคุมการเข้าถึงระบบเครือข่ายสื่อสาร

เป็นการควบคุมบุคคลที่เข้าสู่ระบบเครือข่ายสื่อสาร รวมถึงการควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ และให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น โดยผู้ดูแลระบบจะต้องทำการออกแบบระบบเครือข่ายสื่อสารตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ ได้แก่ Internal Zone, External Zone และ DMZ Zone เป็นต้น จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย ดังนี้

(๑) ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายสื่อสาร จะต้องขอใช้งานกับผู้ดูแลระบบโดยกรอกข้อมูลลงใน “แบบคำขออนุญาตเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร” และต้องได้รับพิจารณาอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษร

(๓) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายสื่อสารให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างน้อยเดือนละครั้ง

(๔) ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายสื่อสารจากแบบคำขอขึ้นทะเบียนครุภัณฑ์คอมพิวเตอร์และเครือข่ายสื่อสาร

(๕) ผู้ดูแลระบบ จัดให้มีซอฟท์แวร์สำหรับบริหารจัดการและควบคุมระบบเครือข่าย (Network Management System) ซึ่งสามารถระบุอุปกรณ์บนเครือข่าย (Equipment Identification) ถึงระดับ IP address, Computer name, MAC address และสามารถสร้างผังการเชื่อมโยงเครือข่าย (Network Diagram)

(๖) มีการจัดทำผังการเชื่อมโยงเครือข่าย และมีการปรับปรุงให้เป็นปัจจุบันเสมอ

(๗) ผู้ดูแลระบบ มีการบริหารจัดการเครือข่ายสื่อสาร ดังนี้

- มีการแบ่งแยกเครือข่ายสื่อสารเป็นเครือข่ายสื่อสารภายใน เครือข่ายสื่อสารภายนอก และเครือข่ายสื่อสารแบบไร้สาย

- มีการจัดแบ่งแยกส่วนเครือข่ายสื่อสาร /กลุ่ม เพื่อป้องกันและควบคุมการเข้าถึง ได้แก่ ส่วนที่เป็นสาธารณะ ส่วนที่เชื่อมต่อภายใน ส่วนที่เกี่ยวข้องกับสินทรัพย์สำคัญหรือที่เป็นอันตราย กลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

- มีการใช้ VLAN ในแต่ละส่วนเครือข่ายสื่อสาร /กลุ่ม เช่น กลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

- มีการติดตั้งอุปกรณ์ Gateway กั้นไว้ระหว่างเครือข่ายสื่อสาร เพื่อเป็นตัวควบคุมข้อมูลที่สื่อสารกันระหว่างเครือข่ายสื่อสาร

- อุปกรณ์ในเครือข่ายสื่อสารมีการปรับแต่งให้สามารถควบคุมหรือกรองข้อมูลที่สื่อสารกันระหว่างเครือข่าย

(๘) มีการควบคุมและป้องกันให้ปลอดภัย เช่น การใช้การตรวจสอบตัวตน การเข้ารหัสผ่าน การเลือกกำหนดความถี่ช่องสัญญาณเอง

(๙) มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๑๐) มีการตรวจสอบการทำงานของระบบเครือข่ายสื่อสารและอุปกรณ์เครือข่ายสื่อสารอย่างสม่ำเสมอเป็นประจำทุกวัน

(๑๑) มีการตั้งค่า และการปรับแต่งค่า (Configuration) ที่ถูกต้องเหมาะสม และเป็นปัจจุบัน

(๑๒) มีการเฝ้าระวังระบบเครือข่ายสื่อสาร

(๑๓) มีการสำรองข้อมูลการตั้งค่าของอุปกรณ์เครือข่ายสื่อสาร

(๑๔) มีการ Update patch หรือ Release ของซอฟต์แวร์ระบบหรือ Firmware

(๑๕) มีการตรวจสอบช่องโหว่ของอุปกรณ์และเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการในระบบเครือข่ายสื่อสารของกรมที่ดิน

(๑๖) มีการทดสอบการบุกรุกเครือข่ายสื่อสาร

๕.๑.๗.๑ การควบคุมการเข้าถึงระบบเครือข่ายสื่อสารจากภายใน

(๑) การควบคุมการเชื่อมต่อทางเครือข่าย

- การขอติดตั้งจุดเพื่อเชื่อมต่อเข้าเครือข่ายของศูนย์สารสนเทศที่ดินต้องทำเป็นหนังสือและได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมาย
- ดูแลและปรับปรุงสิทธิการเข้าถึงและใช้งานเครือข่ายของผู้ใช้งานอยู่เสมอ
- มีอุปกรณ์ในการกรองการรับส่งข้อมูล เช่น อีเมล์ การรับส่งแฟ้มข้อมูล การเข้าถึงแบบโต้ตอบหรือการแช็ท การเข้าถึงโปรแกรมประยุกต์
- จำกัดช่วงวันหรือช่วงเวลาในการอนุญาตให้เชื่อมต่อตามความจำเป็น
- จำกัดระยะเวลาการใช้งานเครือข่ายที่เชื่อมต่อ เช่น ตัดการเชื่อมต่อเมื่อใช้งานได้ระยะหนึ่งซึ่งได้กำหนดไว้ล่วงหน้า จำกัดการเชื่อมต่อเครือข่ายให้เป็นเฉพาะภายในระยะเวลาทำการ ให้ตรวจสอบยืนยันตัวตนใหม่ทุกช่วงเวลาที่กำหนด
- กำหนดการหมดเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ โดยมีกลไกในการยกเลิกเมื่อไม่ได้ใช้งานตามระยะเวลาที่กำหนด

(๒) การควบคุมการกำหนดเส้นทางบนเครือข่าย

- มีการควบคุมการกำหนดเส้นทางบนเครือข่ายบนอุปกรณ์เครือข่าย ได้แก่ Core switch, Edge Switch, Router เป็นต้น
- มีอุปกรณ์ Gateway ในการตรวจสอบต้นทางและปลายทาง ณ จุดควบคุมที่อยู่ระหว่างเครือข่ายภายใน โดยการใช้ Proxy Server หรือ Network Access Controler (NAC)
- มีการกำหนดโปรโตคอล สิทธิ IP Address ในการเชื่อมโยงเครือข่ายของอุปกรณ์และผู้ใช้งานเครือข่ายให้เหมาะสม
- มีการกำหนดโปรโตคอล และพอร์ตการใช้งานของแต่ละกลุ่มผู้ใช้งาน เช่น HTTP, FTP, SMTP, TELNET
- มีการกำหนด VLAN เพื่อควบคุมและกำหนดสิทธิการใช้งาน

(๓) การระบุและพิสูจน์ตัวตนของผู้ใช้งาน

- มีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน โดยต้องแสดงตัวตนด้วยชื่อผู้ใช้งาน พิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านในการเข้าสู่เครือข่าย
- มีการยืนยันตัวตนอย่างเข้มข้นแทนการใช้รหัสผ่าน เช่นวิธีการใช้การเข้ารหัสเพื่อรักษาความลับ Smart Card หรือวิธีการทาง Bio Metric

(๔) การติดตั้งอุปกรณ์ Firewall เพื่อรักษาความปลอดภัยของระบบเครือข่าย

- ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของ Firewall ทั้งหมด การเปลี่ยนแปลงค่าต่าง ๆ ของอุปกรณ์ Firewall ในแต่ละครั้ง ได้แก่ ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการกำหนดระบบเครือข่ายสื่อสารต่าง ๆ ให้สามารถเชื่อมต่อกับระบบเครือข่ายสื่อสารของกรมที่ดิน โดยได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมาย

- การกำหนดค่าเริ่มต้นพื้นฐานของทุกระบบเครือข่ายสื่อสาร จะต้องเป็นการปฏิเสธทั้งหมด

- การเชื่อมต่อระบบอินเทอร์เน็ตและบริการระบบอินเทอร์เน็ตที่ไม่ได้รับการอนุญาตตามนโยบาย ทุกเส้นทางจะต้องถูกบล็อก (Block) โดย Firewall

- การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

- ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้องจัดเก็บไว้ที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่น่าเชื่อถือและมีการเข้ารหัสข้อมูลเพื่อป้องกันการแก้ไขหรือเปลี่ยนแปลง และต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า ๙๐ วัน

- ผู้ดูแลระบบต้องตรวจสอบเหตุการณ์ ข้อมูลจราจรทางคอมพิวเตอร์ พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลการเข้าใช้งานระบบเครือข่ายเป็นประจำทุกวัน

- การกำหนดการให้บริการระบบอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตใน Firewall สำหรับการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานนอกเหนือจากที่กำหนดไว้จะต้องมีการเปิดพอร์ตให้เป็นกรณีพิเศษ ต้องทำหนังสือและได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมาย

- การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของระบบเครือข่ายสื่อสาร จะต้องกำหนดค่าอนุญาตใน Firewall เฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

- เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานระบบอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

- การสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ Firewall จะต้องสำรองข้อมูลเป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงการกำหนดค่าในอุปกรณ์ Firewall

- ผู้ดูแลระบบมีสิทธิที่จะระงับการใช้งานของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

- การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกผ่านระบบเครือข่ายสื่อสารมายังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์ระบบเครือข่ายสื่อสารภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบคำขออนุญาตเปิดบริการใน Firewall และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน

- ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานระบบอินเทอร์เน็ตหรือการเชื่อมต่อระบบเครือข่ายสื่อสารภายในโดยทันที

(๕) การติดตั้งอุปกรณ์ตรวจจับและป้องกันการบุกรุก (IDS/IPS)

- การติดตั้งระบบ IDS/IPS เพื่อตรวจสอบหรือเฝ้าระวัง หรือมอนิเตอร์เหตุการณ์ต่าง ๆ ที่เกิดขึ้นจากการใช้งานของบุคคลที่เข้าใช้งานระบบคอมพิวเตอร์หรือระบบเครือข่ายสื่อสารของหน่วยงานในลักษณะที่ผิดปกติ เช่นการพยายามที่จะทำลายความลับ (Confidentiality) ความคงสภาพ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล หรือการหลีกเลี่ยงระบบการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยการบุกรุกดังกล่าวเกิดจากการที่ผู้บุกรุกเข้าถึงระบบจากอินเทอร์เน็ต หรือการที่ผู้ใช้ภายในพยายามเข้าถึงหรือกระทำในสิ่งที่ไม่ได้รับอนุญาต หรือการที่ผู้ใช้พยายามใช้สิทธิพิเศษของตนในทางที่ผิด

- การติดตั้งระบบ IDS/IPS ให้ครอบคลุมระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารของกรมที่ดินทั้งหมด รวมถึงเส้นทางข้อมูลจราจร ทั้งที่เชื่อมต่อสู่ระบบเครือข่ายสื่อสารภายนอกและภายในทุกเส้นทาง

- ระบบคอมพิวเตอร์ทั้งหมดที่สามารถเข้าถึงได้จากระบบเครือข่ายสื่อสารภายนอกหรือเครือข่ายอินเทอร์เน็ต จะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

- ระบบคอมพิวเตอร์ทั้งหมดใน Demilitarized Zone (DMZ) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการจากระบบ IDS/IPS ก่อนการติดตั้งและเปิดให้บริการ

- ข้อมูลจราจรทางคอมพิวเตอร์ที่ผ่านเข้าออกระบบ IDS/IPS จะต้องมีการบันทึกไม่น้อยกว่า ๙๐ วัน

- ผู้ดูแลระบบต้องตรวจสอบ และ Update Patch / Signature ของระบบ IDS /IPS เป็นประจำอย่างน้อยเดือนละหนึ่งครั้ง

- ผู้ดูแลระบบต้องตรวจสอบเหตุการณ์ ข้อมูลจราจรทางคอมพิวเตอร์ พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลการเข้าใช้งานระบบเครือข่ายเป็นประจำทุกวัน

- ระบบ IDS/IPS ทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ต้องรายงานให้ผู้บังคับบัญชาทราบตามลำดับชั้นทันทีที่ตรวจพบ

- ผู้ดูแลระบบมีสิทธิในการยุติการเชื่อมต่อระบบเครือข่ายสื่อสารของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า และรายงานให้ผู้บังคับบัญชาทราบ

๕.๑.๗.๒ การควบคุมการเข้าถึงระบบเครือข่ายสื่อสารจากภายนอก

(๑) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือระบบคอมพิวเตอร์ระยะไกลจากภายนอก (Remote) ผ่านเครือข่ายสื่อสาร ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดพอร์ตใน Firewall หรือโมเด็มหรืออุปกรณ์สื่อสารที่ใช้ตลอดเวลาโดยไม่จำเป็น และตัดช่องทางการเชื่อมต่อเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารจากภายนอกทันทีเมื่อไม่ได้ใช้งานแล้ว

(๒) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบคอมพิวเตอร์ระยะไกลจากภายนอก ต้องได้รับการอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายก่อน ตามแบบคำขออนุญาตเปิดบริการใน Firewall และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบ และข้อมูลอย่างเคร่งครัด

(๓) การให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบคอมพิวเตอร์ระยะไกลจากภายนอก ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการปฏิบัติงาน และต้องได้รับอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย

(๔) การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบคอมพิวเตอร์ระยะไกลจากภายนอก โดยเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แบบพกพา อุปกรณ์คอมพิวเตอร์แบบพกพา รวมถึงอุปกรณ์สื่อสารเคลื่อนที่ ต้องมีการควบคุมพอร์ตใน Firewall ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการแบ่งช่องสัญญาณอย่างชัดเจน

(๕) มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก โดยต้องแสดงตัวตนด้วยชื่อผู้ใช้ การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน และการเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบคอมพิวเตอร์จากอินเทอร์เน็ตนั้น จะมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานด้วย

(๖) มีการใช้อุปกรณ์พิเศษเพื่อยืนยันตัวตนอย่างเข้มข้นในการเข้าสู่ระบบสารสนเทศที่เกี่ยวกับข้อมูลที่เป็นชั้นข้อมูลที่ใช้ภายในกรมที่ดิน และชั้นข้อมูลตั้งแต่ชั้น “ลับ” แทนการใช้รหัสผ่าน เช่นการใช้อุปกรณ์ Token เมื่อต้องปฏิบัติงานภายนอกองค์กร

๕.๑.๗.๓ การควบคุมการเข้าถึงระบบเครือข่ายสื่อสารแบบไร้สาย

(๑) ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๒) ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และทำการสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่

(๓) ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ชื่อผู้ใช้งานและรหัสผ่าน ที่ถูกกำหนดเป็นค่าตั้งต้นจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

(๔) ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่างอุปกรณ์รับและอุปกรณ์กระจายสัญญาณเพื่อให้ยากต่อการดักจับและปลอดภัย

(๕) ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุม MAC Address หรือชื่อผู้ใช้และรหัสผ่านของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายสื่อสารแบบไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้ และรหัสผ่านตามที่กำหนดไว้เท่านั้น

(๖) ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างระบบเครือข่ายสื่อสารแบบไร้สาย กับเครือข่ายสื่อสารภายในองค์กร

(๗) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้ในระบบเครือข่ายสื่อสารแบบไร้สายติดต่อสื่อสารได้เฉพาะกับระบบ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

(๘) ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ / อุปกรณ์ที่อนุญาตให้เชื่อมต่อเครือข่ายสื่อสารแบบไร้สายได้ และบันทึกข้อมูลจราจรทางคอมพิวเตอร์ที่ใช้งานระบบเครือข่ายไร้สายไว้ไม่น้อยกว่า ๙๐ วัน

๕.๑.๘ การควบคุมการเข้าถึงระบบปฏิบัติการ

เป็นการควบคุมบุคคลเข้าสู่ระบบปฏิบัติการที่อยู่ภายใต้ระบบเครือข่ายสื่อสารของกรมที่ดิน เพื่อรักษาความปลอดภัยของข้อมูล และทรัพยากร จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย

(๑) มีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน

- โดยต้องแสดงตัวตนด้วยชื่อผู้ใช้งาน
- พิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน
- การเข้าสู่ระบบปฏิบัติการจะมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานโดยอัตโนมัติจากระบบ Active Directory (AD) หรือ Radius Server

(๒) การติดตั้งโปรแกรมอรรถประโยชน์เพื่อใช้งานร่วมกับระบบปฏิบัติการ

- ต้องไม่ติดตั้งโปรแกรมซอฟแวร์ที่ละเมิดลิขสิทธิ์
- ต้องติดตั้งโปรแกรมตามภารกิจและไม่ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

(๓) สำนักเทคโนโลยีสารสนเทศ กำหนดมาตรการการควบคุมการหมดเวลาใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Session time-out) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง เพื่อยุติการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารนั้น ดังนี้

- กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร มีการยุติการใช้งาน รวมถึงปิดการใช้งานในกรณีที่ไม่มีกิจกรรมการใช้งานภายในช่วงระยะเวลา ๑๐ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- มีกลไกในการยกเลิกการใช้โปรแกรมประยุกต์ และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ เมื่อไม่มีการใช้งานตามระยะเวลาที่กำหนด

(๔) สำนักเทคโนโลยีสารสนเทศ กำหนดมาตรการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Limitation of connection time) สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือแอพพลิเคชันที่มีความเสี่ยง หรือมีความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัย ดังนี้

- กำหนดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือแอพพลิเคชันที่มีความเสี่ยง หรือมีความสำคัญสูง เพื่อให้ผู้ใช้งาน สามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้ได้ ๑ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง เฉพาะในช่วงเวลาทำการของหน่วยงานเท่านั้น
- กำหนดระยะเวลาในการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ใช้ในการปฏิบัติงานต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเกินกว่า ๑๐ นาที กำหนดให้ระบบยุติการใช้งานของผู้ใช้งาน
- กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุและพิสูจน์ตัวตน เพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ทุก ๆ ๑ ชั่วโมง

๕.๑.๙ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ โปรแกรมประยุกต์และแอพพลิเคชั่น

เป็นการเข้าสู่ระบบเทคโนโลยีสารสนเทศ โปรแกรมประยุกต์ และแอพพลิเคชั่นของกรมที่ดิน เพื่อความปลอดภัยของข้อมูล จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย

(๑) มีการแบ่งแยกสภาพแวดล้อมการใช้งานโดยกำหนดให้ เครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งระบบงานที่สำคัญกำหนดให้อยู่ใน Server Zone ส่วนเครื่องแม่ข่ายระบบงานที่ให้บริการบุคคลทั่วไป ซึ่งมีความไวต่อการถูกรบกวนและมีความเสี่ยงสูง จำเป็นต้องเฝ้าระวังเป็นพิเศษ กำหนดให้อยู่ใน Demilitarized Zone (DMZ)

(๒) มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานก่อนเข้าใช้งานระบบ เป็นไปตาม “แนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน” และ “แนวปฏิบัติการบริหารจัดการสิทธิผู้ใช้งาน”

(๓) การป้อนรหัสผ่าน ระบบต้องทำการเข้ารหัสเพื่อป้องกันมิให้ผู้อื่น ทราบรหัสผ่าน

(๔) มีการตัดการใช้งานออกจากระบบอัตโนมัติ เมื่อผู้ใช้งานไม่ตอบสนองกับระบบเป็นเวลาเกิน ๑๐ นาที

(๕) มีการจำกัดระยะเวลาใช้งานระบบเทคโนโลยีสารสนเทศ ตามประเภทภารกิจ เช่น ระบบจดทะเบียนสิทธิและนิติกรรมเปิดให้บริการตามวันและเวลาราชการ ระบบจดหมายอิเล็กทรอนิกส์เปิดให้บริการตลอด ๒๔ ชั่วโมง

(๖) มีการเข้ารหัสข้อมูลที่อยู่ในชั้นความลับในระบบฐานข้อมูล

๕.๒ แนวปฏิบัติการบริหารจัดการศูนย์สารสนเทศที่ดิน กรมที่ดิน

๕.๒.๑. การจัดการบริเวณพื้นที่โดยรอบ (Physical security management)

(๑) พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ภายใน (Data Center) ได้ติดตั้งสัญญาณเตือนภัย เพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น โดยมีการแบ่งพื้นที่สำคัญเป็นส่วน ๆ ดังนี้

- ห้องเครื่องแม่ข่าย (Server Room)
- ห้องสำรองข้อมูล (Backup Room)
- ห้องควบคุม (Control Room)
- ห้องเครือข่าย (Network Room)
- ส่วนระบบปรับอากาศ

(๒) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบการใช้งานได้ตามปกติ

๕.๒.๒ การควบคุมการเข้า-ออก (Physical entry controls) ศูนย์สารสนเทศที่ดิน

(๑) มีขั้นตอนการขออนุญาต การกำหนดสิทธิ และควบคุมการเข้าศูนย์ฯ และพื้นที่สำคัญภายในศูนย์ฯ

(๒) มีระบบการบันทึกวันและเวลาการเข้า-ออกพื้นที่ในศูนย์สารสนเทศที่ดินโดยอัตโนมัติเกี่ยวกับตัวบุคคลและเวลาที่ผ่านเข้า-ออก เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๓) มีการควบคุมการเข้าออกศูนย์ฯ และพื้นที่สำคัญภายในศูนย์ฯ ด้วยการใช้บัตรประจำตัวและลายนิ้วมือ หรือใช้บัตรประจำตัวและรหัสผ่าน เพื่อพิสูจน์ตัวตนของผู้มีสิทธิ

(๔) มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในศูนย์ฯ จนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สิน หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๕) บุคคลภายนอกต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในศูนย์ฯ

(๖) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญในศูนย์ฯ

(๗) สร้างความเข้าใจและตระหนักในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในศูนย์ฯ

(๘) จัดให้มีการทบทวนสิทธิอย่างสม่ำเสมอ และยกเลิกสิทธิการเข้าศูนย์ฯ ทันทีในกรณีที่มีการเปลี่ยนแปลงสิทธิ

๕.๒.๓ การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection) ในศูนย์สารสนเทศที่ดิน

(๑) จัดวางอุปกรณ์แต่ละประเภทตามพื้นที่ที่กำหนด

(๒) ห้ามนำอาหาร เครื่องดื่ม เข้าไปในบริเวณศูนย์ฯ

(๓) ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในศูนย์ฯ เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้นให้อยู่ในระดับปกติ

๕.๒.๔ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) ในศูนย์สารสนเทศที่ดิน

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดินที่เพียงพอต่อความต้องการใช้งานโดยมีระบบดังต่อไปนี้ ระบบไฟฟ้าและเครื่องกำเนิดไฟฟ้า ระบบสำรองไฟฟ้า ระบบปรับอากาศแบบควบคุมความชื้น ระบบตรวจจับและแจ้งเตือนการรั่วซึมของน้ำ ระบบควบคุมการเข้า-ออกประตูอัตโนมัติ ระบบดับเพลิงอัตโนมัติ ระบบเฝ้าดูและแจ้งเตือนความผิดปกติของสภาวะแวดล้อมอัตโนมัติ ระบบกล้องโทรทัศน์วงจรปิด ระบบสายสัญญาณและอุปกรณ์เครือข่ายคอมพิวเตอร์ อุปกรณ์ในการสลับใช้งานแป้นพิมพ์ จอภาพและเมาส์ของเครื่องคอมพิวเตอร์แม่ข่าย (KVM: Keyboard Video Mouse) และระบบไฟฟ้าฉุกเฉิน

(๒) มีการตรวจสอบหรือทดสอบระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้ระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงาน

๕.๒.๕ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ ในศูนย์สารสนเทศที่ดิน

(๑) มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๒) มีการเดินสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซง รบกวนของสัญญาณซึ่งกันและกัน

(๓) มีป้ายชื่อสำหรับสายสัญญาณบนอุปกรณ์ เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๔) มีการจัดทำผังสายสัญญาณสื่อสารต่าง ๆ ครบถ้วนถูกต้องและเป็นปัจจุบัน

(๕) ตู้ Rack ที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๕.๒.๖ การบำรุงรักษาอุปกรณ์ (Equipment maintenance) ในศูนย์สารสนเทศที่ดิน

(๑) มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนดทุก ๑ เดือน

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) มีการจัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินผลในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) มีการควบคุมและดูแลการปฏิบัติงานของบริษัทผู้รับจ้างบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๖) มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของบริษัทผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๕.๓ การรักษาความมั่นคงปลอดภัยการใช้งานเครื่องคอมพิวเตอร์

๕.๓.๑ การใช้งานของผู้ใช้งาน

(๑) ให้มีการกำหนดรหัสผ่าน เปลี่ยนรหัสผ่านและเก็บรักษารหัสผ่าน เป็นไปตามข้อ ๕.๑.๔ การใช้งานรหัสผ่านสำหรับผู้ใช้งาน

(๒) ให้ผู้ใช้งานออกจากระบบ (Log off) ทันทีในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันบุคคลอื่นมาใช้ระบบต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหล ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที

(๓) ผู้ไม่ได้รับสิทธิให้เข้าใช้งาน ห้ามบุกรุกเข้าใช้งานระบบเทคโนโลยีสารสนเทศไม่ว่าด้วยวิธีการใด ๆ

(๔) ห้ามติดตั้งซอฟต์แวร์ หรือ โปรแกรมอื่นใดลงบนเครื่องคอมพิวเตอร์ ที่ใช้ปฏิบัติงาน หรือติดตั้งอุปกรณ์เชื่อมโยงเครือข่ายเพิ่มเติม หรือเชื่อมโยงเครือข่ายคอมพิวเตอร์ที่ใช้ปฏิบัติงานกับเครือข่ายอื่นนอกจากเครือข่ายของกรมที่ดิน หรือนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้งานกับระบบเทคโนโลยีสารสนเทศ เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

(๕) ไม่เปิดให้มีการแชร์ไฟล์ในเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน เว้นแต่ในกรณีที่เป็นระบบงานที่กรมที่ดินกำหนดไว้ หากมีความจำเป็นให้กำหนดระยะเวลาเท่าที่ใช้งานและยกเลิกการแชร์ไฟล์ทันทีที่ใช้งานเสร็จเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และข้อมูล

(๖) ไม่ดาวน์โหลด (Download) ข้อมูลหรือโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน หรือ จากเว็บไซต์ซึ่งไม่น่าเชื่อถือ หรือไม่มั่นใจว่าจะปลอดภัย

๕.๓.๒ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

(๑) เครื่องคอมพิวเตอร์ส่วนบุคคลที่อนุญาตให้ใช้ เป็นทรัพย์สินของกรมที่ดิน จึงต้องใช้งานอย่างระมัดระวัง และให้มีประสิทธิภาพ

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องเป็นโปรแกรมที่กรมที่ดินเห็นชอบให้ใช้งาน หรือได้ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอก ติดตั้ง หรือแก้ไขเปลี่ยนแปลงโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคลที่มิใช่ทรัพย์สินของกรมที่ดิน หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่นำสื่อข้อมูล เช่น แผ่นซีดี ดีวีดี แฟลชไดร์ฟ ที่ใช้งานจากเครื่องคอมพิวเตอร์ส่วนบุคคลอื่น ๆ นอกระบบเทคโนโลยีสารสนเทศ หรือมาจากแหล่งข้อมูลที่น่าสงสัย มาใช้งานกับเครื่องคอมพิวเตอร์ ส่วนบุคคลที่ใช้ปฏิบัติงานในระบบเทคโนโลยีสารสนเทศ โดยไม่ได้ตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ก่อน

(๔) ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้ปฏิบัติงานในระบบเทคโนโลยีสารสนเทศ

(๕) ให้ติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุงฐานข้อมูลไวรัสในเครื่องคอมพิวเตอร์ส่วนบุคคลให้เป็นปัจจุบัน อย่างสม่ำเสมอ

(๖) ผู้ใช้งานต้องตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองรับผิดชอบ ให้ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๕ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์ส่วนบุคคล

(๗) ผู้ใช้งานต้องปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองใช้งาน เมื่อปฏิบัติงานเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์ส่วนบุคคลที่ไม่ใช่ทรัพย์สินของกรมที่ดินมาใช้กับระบบเครือข่ายสื่อสาร ของกรมที่ดิน ยกเว้นได้รับการอนุญาตจากผู้ดูแลระบบก่อนการใช้งาน

(๙) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

(๑๐) ผู้ใช้งานต้องตรวจสอบข้อมูลใด ๆ ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูล หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(๑๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ส่วนบุคคลไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๑๒) เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ และสื่อสำรองข้อมูลที่ไม่ใช้งานแล้วต้องทำลายข้อมูลที่สำรองไว้ ไม่ให้สามารถนำไปใช้งานได้อีก

๕.๓.๓ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่อนุญาตให้ใช้เป็นทรัพย์สินของกรมที่ดิน จึงต้องใช้งานอย่างระมัดระวัง และให้มีประสิทธิภาพ

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพา ต้องเป็นโปรแกรมที่กรมที่ดินเห็นชอบให้ใช้งาน หรือได้ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอก ติดตั้ง หรือแก้ไขเปลี่ยนแปลงโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาที่ไม่ใช่ทรัพย์สินของกรมที่ดิน หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์แบบพกพา และรักษาสภาพของเครื่องคอมพิวเตอร์พกพาให้มีสภาพเดิมและพร้อมใช้งาน

(๕) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๖) กรณีที่หน้าจอคอมพิวเตอร์ไม่ใช่แบบ Touch Screen ให้หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปากกากดสัมผัสหน้าจอ เพราะอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้

(๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๘) การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๙) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๑๐) ไม่เก็บหรือใช้งานเครื่องคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

(๑๑) ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(๑๒) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ใน “แนวปฏิบัติการใช้งานรหัสผ่าน”

(๑๓) ผู้ใช้งานต้องตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์แบบพกพาที่ตนเองรับผิดชอบ ให้ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๕ นาที เพื่อป้องกันบุคคลอื่นมาใช้งาน

(๑๔) ปิดเครื่องคอมพิวเตอร์แบบพกพาที่ตนเองใช้งาน เมื่อปฏิบัติงานเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๑๕) ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน “การใช้งานรหัสผ่าน”

(๑๖) ทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk

(๑๗) เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ และสื่อสำรองข้อมูลที่ไม่ใช้งานแล้วควรทำลายข้อมูลที่สำรองไว้ ไม่ให้สามารถนำไปใช้งานได้อีก

๕.๓.๔ การใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

(๑) อุปกรณ์คอมพิวเตอร์แบบพกพา ที่กรมที่ดินอนุญาตให้ใช้งาน เป็นสินทรัพย์ของกรมที่ดิน จึงต้องใช้งานอย่างระมัดระวังและมีประสิทธิภาพ

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนอุปกรณ์คอมพิวเตอร์แบบพกพา ต้องเป็นโปรแกรมที่กรมที่ดินเห็นชอบให้ใช้งาน หรือได้ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอก ติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมต่าง ๆ และนำไปติดตั้งบนอุปกรณ์คอมพิวเตอร์แบบพกพาที่มิใช่สินทรัพย์ของกรมที่ดิน หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๔) ต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของอุปกรณ์คอมพิวเตอร์และรักษาสภาพของอุปกรณ์คอมพิวเตอร์ให้มีสภาพเดิมและพร้อมใช้งาน

(๕) ในกรณีที่ต้องการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๖) กรณีที่หน้าจอคอมพิวเตอร์ไม่ใช่แบบ Touch Screen ให้หลีกเลี่ยงการใช้ของแข็ง เช่น ปากกากดสัมผัสหน้าจอ เพราะอาจทำให้เป็นรอยขีดข่วนหรือ แตกเสียหายได้

(๗) ไม่วางของทับบนอุปกรณ์คอมพิวเตอร์แบบพกพา

(๘) การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๙) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๑๐) ไม่เก็บหรือใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

(๑๑) ต้องกำหนดรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของอุปกรณ์คอมพิวเตอร์แบบพกพา

(๑๒) ผู้ใช้งานต้องล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่อุปกรณ์คอมพิวเตอร์แบบพกพา

๕.๔ การรักษาความมั่นคงปลอดภัยการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

๕.๔.๑ การใช้งานอินเทอร์เน็ต

(๑) ผู้ดูแลระบบต้องลงทะเบียนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบอินเทอร์เน็ตของกรมที่ดิน ซึ่งทำให้สามารถพิสูจน์ทราบได้ว่าเป็นเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงานที่ตั้งอยู่ที่หน่วยงานใดของกรมที่ดิน

(๒) ผู้ใช้งานต้องลงทะเบียนเป็นผู้ได้รับสิทธิการใช้ และรหัสผ่าน เพื่อเป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลในการเข้าถึงระบบอินเทอร์เน็ตของกรมที่ดิน ซึ่งผู้ใช้งานแต่ละคนจะต้องดูแลรักษาสิทธิการใช้งานและรหัสผ่านของตนเองไม่ให้ผู้อื่นนำไปใช้งานได้ หากมีการกระทำใดซึ่งเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เจ้าของสิทธิต้องรับผิดชอบผลจากความเสียหายที่เกิดขึ้นโดยไม่อาจปฏิเสธได้

(๓) ผู้ใช้งานต้องไม่ใช้ระบบอินเทอร์เน็ตในการใช้งานข้อมูลมัลติมีเดีย หรือดาวน์โหลดข้อมูลที่ไม่เกี่ยวกับการปฏิบัติงานและยึดครองช่องสัญญาณการสื่อสารข้อมูล

(๔) ให้ผู้ดูแลระบบ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย เช่น Proxy, Firewall, IPS, IDS

(๕) เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์คอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

(๖) ผู้ใช้งานต้องไม่ใช้งานอินเทอร์เน็ตของกรมที่ดิน เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

(๗) ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกรมที่ดิน โดยผ่านความเห็นชอบจากผู้ดูแลระบบ

(๘) ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมที่ดิน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

(๙) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

(๑๐) ให้ออกจากระบบอินเทอร์เน็ตทันทีหลังจากเลิกใช้งาน เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

(๑๑) ผู้ใช้งานต้องปฏิบัติตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

๕.๔.๒ การใช้งานจดหมายอิเล็กทรอนิกส์

(๑) ผู้ใช้งานต้องลงทะเบียนเป็นผู้ได้รับสิทธิการใช้ และรหัสผ่าน เพื่อเป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลในการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมที่ดิน ซึ่งผู้ใช้งานแต่ละคนจะต้องดูแลรักษาสิทธิการใช้งานและรหัสผ่านของตนเองไม่ให้ผู้อื่นนำไปใช้งานได้ หากมีการกระทำใดซึ่งเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เจ้าของสิทธิต้องรับผิดชอบผลจากความเสียหายที่เกิดขึ้นโดยไม่อาจปฏิเสธได้

(๒) ผู้ใช้งานต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมที่ดินในการรับ-ส่งจดหมายอิเล็กทรอนิกส์ซึ่งเกี่ยวกับการปฏิบัติราชการ

(๓) ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อกรมที่ดิน สร้างความน่ารำคาญต่อผู้อื่น หรือขัดต่อศีลธรรม และไม่แสวงหาประโยชน์จากการใช้จดหมายอิเล็กทรอนิกส์ของกรมที่ดิน

(๔) ผู้ใช้งานต้องออกจากระบบจดหมายอิเล็กทรอนิกส์ทันทีหลังจากการเลิกใช้งานเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

(๕) ก่อนเปิดเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องใช้โปรแกรมป้องกันไวรัส ตรวจสอบเอกสารแนบเสมอ

(๖) ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(๗) ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

(๘) ผู้ใช้งานต้องสำรองข้อมูลที่มีความสำคัญในจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ

๕.๕ การรักษาความมั่นคงปลอดภัยการบริหารจัดการสินทรัพย์และเครือข่าย

๕.๕.๑ การบริหารจัดการข้อมูลคอมพิวเตอร์

(๑) กำหนดประเภทของข้อมูล

- ข้อมูลที่เป็นตัวอักขระ คือข้อมูลที่ประกอบด้วยตัวอักษร และตัวเลขที่ไม่ใช้ในการคำนวณ เช่นข้อมูลทางทะเบียนที่ดิน เจ้าของผู้ถือกรรมสิทธิ์ ที่ตั้งที่ดิน

- ข้อมูลที่เป็นตัวเลข คือข้อมูลที่ประกอบด้วยตัวเลข ๐-๙ ที่ใช้ในการคำนวณได้ เช่น เลขที่เอกสารสิทธิ จำนวนเนื้อที่ในเอกสารสิทธิ

- ข้อมูลที่เป็นรูปภาพ คือข้อมูลที่เป็นภาพนิ่ง ภาพเคลื่อนไหว ภาพลายเส้น ภาพถ่าย ภาพจากวิดิทัศน์ เช่นภาพสแกนโฉนดที่ดิน ภาพสแกนสารบบ

- ข้อมูลที่เป็นเสียง คือข้อมูลที่ประสาทสัมผัสทางหูรับรู้ได้ เช่น การให้นโยบายของอธิบดีเนื่องในโอกาสต่าง ๆ

(๒) กำหนดชั้นความลับข้อมูล

ชั้นที่ ๑ ข้อมูลเปิดเผยได้

- ข้อมูลที่บุคคลทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น เป็นข้อมูลที่ไม่มีผลต่อการปฏิบัติงานของกรมที่ดิน สามารถนำเสนอต่อสาธารณชน หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย

- การเปิดเผยข้อมูลทั้งหมดหรือบางส่วน จะไม่เกิดผลเสียหายต่อกรมที่ดิน เช่น ข้อมูลที่เผยแพร่บนเว็บไซต์กรมที่ดิน

ชั้นที่ ๒ ข้อมูลใช้ภายในกรมที่ดิน

- ข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้ผู้ใช้งานภายในกรมที่ดินรับทราบได้ แต่ไม่สมควรเปิดเผยต่อบุคคลภายนอก เพราะอาจจะสร้างความเสียหายให้กับกรมที่ดินได้

- การเปิดเผยข้อมูล เจ้าของข้อมูลต้องใช้ดุลยพินิจในการอนุญาตหรือได้รับความเห็นชอบจากคณะทำงานเพื่อดำเนินการตาม พรบ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ หรือการบังคับตามกฎหมาย เช่น ข้อมูลระบบบุคลากรกรมที่ดิน ข้อมูลระบบจดทะเบียนสิทธิและนิติกรรม ข้อมูลระบบสารบรรณอิเล็กทรอนิกส์

ชั้นที่ ๓ ข้อมูลลับ

- ข้อมูลที่กรมที่ดินพิจารณาแล้วว่าไม่สามารถเปิดเผยให้ผู้ใช้งานทุกคนทราบได้ กำหนดให้เฉพาะผู้ที่เกี่ยวข้อง และจำเป็นต้องใช้ในการปฏิบัติงานทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่ควรทราบเพื่อให้เพียงพอต่อการปฏิบัติงาน ข้อมูลมีความสำคัญต่อการดำเนินการของกรมที่ดิน เป็นข้อมูลภายใน และไม่สามารถเปิดเผยต่อบุคคลภายนอกกรมที่ดินที่ไม่เกี่ยวข้องตามกฎหมายได้ เนื่องจากข้อมูลนี้จะสร้างความเสียหายให้กับกรมที่ดินได้

- การเปิดเผยข้อมูลจะต้องได้รับความเห็นชอบจากเจ้าของข้อมูล หรือจากคณะทำงานเพื่อดำเนินการตามพระราชบัญญัติข้อมูลข่าวสารของกรมที่ดิน พ.ศ. ๒๕๔๐ หรือการบังคับตามกฎหมาย เช่นข้อมูลเงินเดือน ข้อมูลการลงโทษทางวินัย

ชั้นที่ ๔ ข้อมูลลับมาก

- ข้อมูลที่ใช้ภายในกรมที่ดินแต่เป็นข้อมูลลับ ใช้งานโดยผู้ใช้งานบางกลุ่มของกรมที่ดิน ซึ่งมีรหัสพิเศษในการเข้าใช้งานและไม่สามารถเปิดเผยต่อบุคคลภายนอกได้ เนื่องจากข้อมูลมีความจำเป็นต่อการปฏิบัติงานของกรมที่ดิน จะทำให้เกิดผลเสียหายร้ายแรงต่อกรมที่ดิน

- การเปิดเผยข้อมูล จะต้องได้รับการเห็นชอบจากเจ้าของข้อมูล หรือคณะทำงานเพื่อดำเนินการตาม พรบ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ หรือการบังคับตามกฎหมาย เช่น ข้อมูลการจราจรทางคอมพิวเตอร์ ข้อมูลจดหมายอิเล็กทรอนิกส์

ชั้นที่ ๕ ข้อมูลลับที่สุด

- ข้อมูลที่ใช้ภายในกรมที่ดินแต่เป็นข้อมูลลับ ใช้งานโดยผู้บริหารระดับสูงของกรมที่ดินเท่านั้น ซึ่งมีรหัสพิเศษในการเข้าใช้งาน และเป็นการใช้เพื่อการวินิจฉัย และตัดสินใจที่สำคัญของกรมที่ดิน ไม่สามารถเปิดเผยต่อบุคคลภายนอกกรมที่ดินได้ เนื่องจากข้อมูลมีความจำเป็นต่อการปฏิบัติงานของกรมที่ดิน ทำให้เกิดผลเสียหายร้ายแรงต่อกรมที่ดิน

- การเปิดเผยข้อมูล ไม่สามารถทำได้ เว้นแต่การบังคับตามกฎหมาย เช่น ข้อมูลข้อสอบคัดเลือก

(๓) การควบคุมการขอข้อมูล ขอใช้ ขอตรวจสอบ หรือขอเข้าดูข้อมูล

- เจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศไม่มีสิทธิที่จะให้ข้อมูลแก่ผู้ขอข้อมูลใด ๆ โดยที่ไม่ได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย เว้นแต่ในการพัฒนาระบบ ซึ่งเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศและบริษัทผู้รับจ้างรับผิดชอบในการถ่ายโอนข้อมูลเข้าสู่ระบบใหม่

- กรณีหน่วยงานภายในกรมที่ดินเป็นผู้ขอข้อมูลซึ่งหน่วยงานภายในกรมที่ดินอื่น ๆ เป็นเจ้าของข้อมูล ให้หน่วยงานผู้ขอทำบันทึกขออนุญาตจากหน่วยงานเจ้าของข้อมูล โดยเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศจะให้บริการเกี่ยวกับข้อมูลเมื่อได้รับทราบการได้รับอนุญาตนั้นแล้วเท่านั้น

- กรณีหน่วยงานภายนอกกรมที่ดิน ไม่ว่าจะเป็นหน่วยงานราชการ หรือหน่วยงานเอกชน เป็นผู้ขอ โดยไม่มีการทำบันทึกข้อตกลงระหว่างหน่วยงานกันไว้ก่อน ต้องทำหนังสือขออนุญาตจากอธิบดีกรมที่ดินทุกครั้งที่ขอ หากมีการทำบันทึกข้อตกลงกันไว้ ต้องควบคุมดูแลให้ขอบเขตของข้อมูลที่ขอเป็นไปตามบันทึกข้อตกลง

- กรณีบุคคลหรือนิติบุคคลเป็นผู้ขอข้อมูลกับกรมที่ดิน ซึ่งมีแนวทางหรือระเบียบปฏิบัติที่กรมที่ดินได้กำหนดไว้แล้ว ให้ดำเนินการตามแนวทางหรือระเบียบปฏิบัติที่กำหนด

(๔) การกำหนดเวลาและช่องทางเข้าถึงข้อมูล

- การกำหนดเวลาเข้าถึงข้อมูล ข้อมูลที่เป็นระบบปฏิบัติงาน สามารถเข้าถึงได้ในวันและเวลาราชการ หรือเป็นไปตามบันทึกข้อตกลงของหน่วยงานนั้น ๆ ส่วนข้อมูลที่เผยแพร่ด้วยช่องทางอินเทอร์เน็ต สามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง

- การกำหนดช่องทางการเข้าถึงข้อมูล ผู้ใช้งานภายในกรมที่ดิน ใช้ผ่านช่องทางอินทราเน็ตและอินเทอร์เน็ต สำหรับผู้ใช้งานภายนอกกรมที่ดินใช้ผ่านช่องทางอินเทอร์เน็ตและตามบันทึกข้อตกลงระหว่างหน่วยงาน

๕.๕.๒ การบริหารจัดการระบบคอมพิวเตอร์

(๑) จัดทำทะเบียนคุมสินทรัพย์ในระบบคอมพิวเตอร์

(๒) การรักษาความปลอดภัยระบบคอมพิวเตอร์ โดย

- กำหนดชื่อและ IP Address ในระบบคอมพิวเตอร์

- กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของโปรแกรมระบบอย่างชัดเจน

- มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์

- ในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานผู้ดูแลรับผิดชอบโดยทันที

- เปิดใช้บริการ (Service) เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบการรักษาความปลอดภัย ต้องมีมาตรการเพิ่มเติม

- มีการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติการ DBMS และ Web server อย่างสม่ำเสมอ

- ทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

(๓) บำรุงรักษาอุปกรณ์ ในระบบคอมพิวเตอร์ให้สามารถทำงานได้อย่างมีประสิทธิภาพ โดยควบคุมดูแลให้มีการบำรุงรักษาอุปกรณ์ในระบบคอมพิวเตอร์ตามระยะเวลาที่กำหนดในสัญญาจ้างบำรุงรักษาฯ

๕.๕.๓ การบริหารจัดการโปรแกรม

(๑) จัดทำทะเบียนคุมโปรแกรม

(๒) ลงทะเบียนขอใช้โปรแกรมจากเจ้าของลิขสิทธิ์

(๓) ปรับปรุงโปรแกรมเมื่อมีการเปลี่ยนแปลงรุ่นของโปรแกรม

(๔) มีการควบคุมเวอร์ชั่นของโปรแกรมประยุกต์ (Application)

(๕) มีการติดตั้งโปรแกรมที่ถูกต้องตามลิขสิทธิ์หรือโปรแกรมสำหรับใช้งานฟรี (Freeware, Open Source) และติดตั้งเท่าที่จำเป็นต่อการใช้งาน

๕.๕.๔ การบริหารจัดการเครือข่ายสื่อสาร

(๑) มีการจัดแบ่งแยกส่วนเครือข่าย/กลุ่ม (VLAN / Zone)

(๒) จัดทำทะเบียนคุมการใช้งานเครือข่ายสื่อสาร

(๓) จัดทำแผนผังและขอบเขตของระบบเครือข่ายสื่อสาร

(๔) ตรวจสอบการใช้งานเครือข่ายสื่อสารให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

(๕) ควบคุมการจัดเส้นทางบนเครือข่ายสื่อสารและกำหนดวิธีการเข้าถึงเครือข่ายสื่อสารกรมที่ดิน

(๖) จัดทำระบบป้องกันการบุกรุกและการใช้งานที่ผิดปกติผ่านระบบเครือข่ายสื่อสาร

(๗) ทดสอบการบุกรุกโจมตีเครือข่ายสื่อสาร และจัดทำรายงานการโจมตี

(๘) กำหนดผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ของระบบเครือข่ายสื่อสารและอุปกรณ์ที่เชื่อมต่อ

(๙) ทบทวนการกำหนดค่า Parameter อย่างน้อยปีละ ๑ ครั้ง

(๑๐) ทำการบำรุงรักษาระบบเครือข่ายสื่อสารเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ โดยควบคุมดูแลให้มีการบำรุงรักษาระบบเครือข่ายตามระยะเวลาที่กำหนดในสัญญาจ้างบำรุงรักษาฯ

๕.๕.๕ การบริหารจัดการสินทรัพย์

(๑) จัดทำทะเบียนคุมสินทรัพย์

- กำหนดผู้รับผิดชอบต่อสินทรัพย์
- จัดหมวดหมู่สินทรัพย์

(๒) การเบิกใช้ครุภัณฑ์คอมพิวเตอร์และเครือข่าย

- ผู้ใช้ที่ต้องการขอเบิกใช้ครุภัณฑ์ต้องกรอกข้อมูลคำขอลงใน “แบบฟอร์มการขอเบิกใช้ครุภัณฑ์คอมพิวเตอร์และเครือข่าย” โดยระบุรายการครุภัณฑ์ที่ต้องการเบิกใช้รวมถึงสถานที่จัดเก็บหรือติดตั้ง และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการพิจารณาอนุมัติ
- เจ้าหน้าที่ผู้รับผิดชอบพิจารณาตามขั้นตอนและความเหมาะสมในการขอเบิกใช้งานครุภัณฑ์ดังกล่าวโดยขอความเห็นชอบจากผู้บริหารหน่วยงานเจ้าของสินทรัพย์ หรือผู้ที่ได้รับมอบหมาย
- เมื่อมีการอนุมัติให้เบิกใช้ครุภัณฑ์ เจ้าหน้าที่ผู้รับผิดชอบต้องบันทึกข้อมูลสถานที่จัดเก็บหรือติดตั้งใหม่ของครุภัณฑ์ดังกล่าวลงในแบบคำขอลงทะเบียนครุภัณฑ์คอมพิวเตอร์และเครือข่ายสื่อสารเพื่อจัดเก็บเป็นประวัติครุภัณฑ์

(๓) การแจ้งซ่อมบำรุงครุภัณฑ์คอมพิวเตอร์และเครือข่าย

- เมื่อผู้ใช้งานพบการทำงานที่ผิดไปจากปกติของครุภัณฑ์ หรือไม่สามารถใช้งานครุภัณฑ์ในการดำเนินงานได้ ผู้ใช้งานต้องแจ้ง ให้ดำเนินการซ่อมบำรุง โดยกรอกข้อมูลครุภัณฑ์ที่ต้องการแจ้งลงใน “แบบฟอร์มการแจ้งซ่อมบำรุงครุภัณฑ์คอมพิวเตอร์และเครือข่าย” และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการส่งซ่อม
- เจ้าหน้าที่ผู้รับผิดชอบวิเคราะห์อาการเสียหายของครุภัณฑ์ จากข้อมูลใน “แบบฟอร์มการแจ้งซ่อมบำรุงครุภัณฑ์คอมพิวเตอร์และเครือข่าย” และจากการทดสอบการทำงานด้วยตนเอง รวมถึงพิจารณาข้อมูลประกอบโดยเฉพาะในส่วนของระยะเวลาประกันของครุภัณฑ์ดังกล่าว ซึ่งหากอยู่ในระยะเวลาประกัน เจ้าหน้าที่สามารถส่งครุภัณฑ์เข้ารับการซ่อมบำรุงที่ศูนย์บริการของบริษัทผู้ผลิตครุภัณฑ์ได้ โดยไม่เสียค่าใช้จ่ายในส่วนที่ระบุในประกัน หากครุภัณฑ์ดังกล่าวไม่อยู่ในระยะเวลาประกัน เจ้าหน้าที่ผู้รับผิดชอบต้องพิจารณาจากความเสียหายของครุภัณฑ์ หากเสียหายมากอาจจำเป็นจะต้องจำหน่ายครุภัณฑ์ดังกล่าว หรือหากความเสียหายของครุภัณฑ์สามารถแก้ไขได้ให้ดำเนินการแก้ไข

- ในระหว่างที่เจ้าหน้าที่ผู้รับผิดชอบส่งครุภัณฑ์เข้ารับการซ่อมบำรุงนั้น หากมีครุภัณฑ์อื่นที่สามารถใช้งานทดแทนครุภัณฑ์ดังกล่าวได้ ให้เจ้าหน้าที่ดำเนินการแจ้งแก่ผู้ใช้ โดยให้ผู้ใช้ทำเรื่องเบิกใช้งานครุภัณฑ์ โดยกรอกข้อมูลลงใน‘แบบฟอร์มการขอเบิกใช้ครุภัณฑ์คอมพิวเตอร์และเครือข่าย โดยระบุรายการครุภัณฑ์ที่ต้องการเบิกใช้รวมถึงสถานที่จัดเก็บหรือติดตั้ง และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการพิจารณาอนุมัติ และเจ้าหน้าที่ผู้ดูแลทะเบียนครุภัณฑ์ทำการบันทึกข้อมูลครุภัณฑ์ใหม่ลงใน “แบบฟอร์มทะเบียนครุภัณฑ์คอมพิวเตอร์และเครือข่าย” เพื่อจัดเก็บเป็นประวัติครุภัณฑ์ของกรมที่ดิน

- หลังจากที่เจ้าหน้าที่ผู้รับผิดชอบส่งครุภัณฑ์ที่พบความเสียหายเข้ารับการแก้ไขเรียบร้อยแล้ว ต้องดำเนินการทดสอบในส่วนที่พบความเสียหายอีกครั้ง ก่อนจัดส่งครุภัณฑ์คืนผู้ใช้ โดยเจ้าหน้าที่ผู้รับผิดชอบกรอกข้อมูลรายละเอียดการซ่อมบำรุง และการทดสอบครุภัณฑ์ลงใน “แบบฟอร์มการแจ้งซ่อมบำรุงครุภัณฑ์คอมพิวเตอร์และเครือข่าย” และส่งคืนครุภัณฑ์พร้อมเอกสารดังกล่าวให้กับผู้ใช้

- ผู้ใช้ทำการตรวจสอบครุภัณฑ์ หากสามารถใช้ดำเนินงานได้ตามปกติ ให้ลงลายมือชื่อ เพื่อรับครุภัณฑ์กลับไปใช้งาน แต่หากยังพบว่ามีความเสียหายในส่วนเดิมหรือส่วนอื่น ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบ เพื่อดำเนินการแก้ไขตามขั้นตอนต่อไป

(๔) การนำสินทรัพย์ของกรมที่ดินออกนอกสถานที่

- ให้มีการบันทึกขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์ออกนอกสถานที่ เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

- ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

(๕) การจำหน่ายครุภัณฑ์คอมพิวเตอร์และเครือข่าย

- กรณีที่ครุภัณฑ์เสียหายเกินกว่าที่จะแก้ไขได้ รวมถึงไม่อยู่ในระยะเวลาประกัน ประกอบกับเมื่อพิจารณาถึงมูลค่าของครุภัณฑ์กับค่าใช้จ่ายในการซ่อมบำรุงแล้ว จำเป็นต้องดำเนินการจำหน่ายครุภัณฑ์ดังกล่าว ให้เจ้าหน้าที่ผู้รับผิดชอบกรอกรายละเอียดครุภัณฑ์ลงใน “แบบฟอร์มการส่งคืนครุภัณฑ์คอมพิวเตอร์และเครือข่าย” ให้เจ้าหน้าที่ผู้เป็นเจ้าของงาน/โครงการ ซึ่งเป็นผู้ใช้หรือผู้จัดหาครุภัณฑ์รับทราบและพิจารณาเห็นชอบ

- เจ้าหน้าที่ผู้เป็นเจ้าของงาน/โครงการ พิจารณาเรื่องการส่งคืนครุภัณฑ์ หากเห็นชอบให้ลงลายมือชื่อใน “แบบฟอร์มการส่งคืนครุภัณฑ์คอมพิวเตอร์และเครือข่าย” หากไม่เห็นชอบให้ระบุเหตุผลและส่งเรื่องคืนเจ้าหน้าที่ผู้รับผิดชอบ

- ส่งเรื่องให้หน่วยงานที่มีอำนาจอนุมัติการจำหน่ายครุภัณฑ์พิจารณาดำเนินการต่อไป

(๖) การควบคุมเอกสาร (Print out) ที่พิมพ์ออกจากระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- มีการกำหนดสิทธิการพิมพ์เอกสาร

- กำหนดให้มีเจ้าหน้าที่ควบคุมการเข้าถึงเอกสาร (Print out)

- จัดเก็บเอกสารที่เกี่ยวข้องกับระบบไว้ในสถานที่มั่นคงปลอดภัย โดยจัดเก็บตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ หรือระเบียบอื่น ๆ ที่เกี่ยวข้อง

- เอกสารที่ไม่ใช้งานหรือมีความผิดพลาดจากการพิมพ์ ให้ทำลาย

- มีการบันทึกขออนุญาตก่อนนำเอกสารออกนอกสถานที่เพื่อเป็นหลักฐานป้องกันการสูญหาย

๕.๖ การรักษาความมั่นคงปลอดภัยการสำรองข้อมูลและกู้คืนข้อมูล

๕.๖.๑ มีระบบจัดเก็บและสำรองข้อมูล ตามประเภทของข้อมูล ได้แก่ โปรแกรมระบบปฏิบัติการ โปรแกรมประยุกต์หรือแอพลิเคชั่น ชุดคำสั่ง และข้อมูล อย่างน้อยหนึ่งชุดแยกสถานที่จากกัน เพื่อความมั่นคงปลอดภัยและใช้งานได้อย่างต่อเนื่อง

๕.๖.๒ กำหนดผู้รับผิดชอบในการสำรองข้อมูล ตรวจสอบความมีอยู่อย่างถูกต้อง ครบถ้วน ของข้อมูล อย่างน้อยปีละหนึ่งครั้ง และมีการบันทึกรายละเอียดการตรวจสอบ ในกรณีตรวจพบข้อมูลสูญหาย ไม่ถูกต้องครบถ้วน ให้ดำเนินการปรับปรุง แก้ไขข้อมูลให้มีความสมบูรณ์ครบถ้วนในทันที

๕.๖.๓ กำหนดความถี่ในการสำรองข้อมูลของระบบงาน และทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ (ระบบงานที่มีการเปลี่ยนแปลงบ่อย ควรจะมีความถี่ในการสำรองข้อมูลมากขึ้น) และมีการนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

(๑) กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์

(๒) ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วน หรือไม่

(๓) ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ หรือไม่

๕.๖.๔ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะเวลาที่กำหนด โดยมีแนวทางปฏิบัติสำหรับการกู้คืนข้อมูลจากภัยพิบัติ โดย

(๑) มีการกำหนดระบบงานที่มีความสำคัญทั้งหมดของกรมที่ดิน และจัดทำเป็นบัญชีรายชื่อของระบบงาน ดังกล่าว รวมทั้งปรับปรุงบัญชีรายชื่อนี้ให้มีความทันสมัยอยู่เสมอตามระบบงานที่มีความสำคัญที่เกิดขึ้นใหม่

(๒) ประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงที่พบให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

(๓) กำหนดชนิดของข้อมูล เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบงาน หรือข้อมูลในฐานข้อมูล

(๔) กำหนดความถี่ในการสำรองข้อมูล และวิธีการสำรอง เช่น แบบ Full Backup หรือ Incremental Backup ของระบบงานที่มีความสำคัญเหล่านั้น

(๕) จัดทำแผนกู้คืนเพื่อรับมือกับภัยพิบัติที่อาจเกิดขึ้นได้ แผนกู้คืนต้องมีรายละเอียดดังต่อไปนี้

- การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด
- การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้
- การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน
- การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้
- การทดสอบตามแผนเตรียมความพร้อมฯ อย่างน้อยปีละ ๑ ครั้ง
- การกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์
- การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

(๖) ให้ทำการปรับปรุงแผนกู้คืนอย่างน้อยปีละ ๑ ครั้ง

(๗) ให้ทำการสำรองข้อมูลตามชนิด ความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลที่สำรองไปนั้นมีความครบถ้วน

(๘) ให้ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้นั้น ว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่ อย่างน้อยปีละ ๑ ครั้ง ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไข และบันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

(๙) ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนกู้คืน รวมทั้งเมื่อมีการปรับปรุงแผนกู้คืนใหม่จะต้องจัดประชุมใหม่ และแจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

๕.๖.๕ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ เพื่อให้การปฏิบัติงานเป็นไปอย่างต่อเนื่อง

(๑) ให้เตรียมแบบฟอร์ม / แบบพิมพ์ที่สามารถใช้ทดแทนแบบฟอร์ม / แบบพิมพ์ที่พิมพ์ได้จากระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ให้ปฏิบัติงานตามกระบวนงานเดิมก่อนที่จะนำระบบเทคโนโลยีสารสนเทศและการสื่อสารปัจจุบันมาใช้ เช่น การใช้ระบบมือ (Manual System)

(๓) เมื่อระบบเทคโนโลยีสารสนเทศและการสื่อสารสามารถใช้งานได้ตามปกติ ให้นำข้อมูลที่เกิดขึ้นระหว่างที่เกิดเหตุฉุกเฉินฯ เข้าระบบ

๕.๗ การรักษาความมั่นคงปลอดภัยด้านการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๕.๗.๑ มีการแต่งตั้งคณะทำงานบริหารความเสี่ยงของสำนักเทคโนโลยีสารสนเทศ เพื่อดำเนินการ

(๑) จัดลำดับความสำคัญของความเสี่ยง

(๒) จัดทำแผนบริหารความเสี่ยง

(๓) ดำเนินการตามแผนบริหารความเสี่ยง

๕.๗.๒ มีการตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์อย่างน้อยปีละหนึ่งครั้ง

๕.๗.๓ มีกลุ่มตรวจสอบภายในกรมที่ดิน เป็นผู้ตรวจสอบและประเมินความเสี่ยง

๕.๗.๔ มีการรายงานการตรวจสอบและประเมินความเสี่ยงเสนอผู้รับผิดชอบ และหน่วยงานที่รับผิดชอบ และจะดำเนินการปรับปรุงตามคำแนะนำหน่วยงานที่รับผิดชอบนั้นโดยทันที

๕.๗.๕ มีการกำหนดความรับผิดชอบของผู้ใช้งานหรือผู้บริหาร ให้ผู้ใช้งานและผู้บริหารรับผิดชอบในกรณีเกิดความเสียหายหรืออันตรายอันเนื่องมาจากผู้ใช้งานหรือผู้บริหารบกพร่องหรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แล้วแต่กรณี

๕.๘ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๕.๘.๑ มีการเผยแพร่ประชาสัมพันธ์และฝึกอบรม ให้เจ้าหน้าที่กรมที่ดินรับทราบ เข้าใจและไม่กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และกฎหมายอื่น ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ รวมถึงมีความรับผิดชอบในการใช้ทรัพยากรทางด้านเทคโนโลยีสารสนเทศของกรมที่ดินอย่างเหมาะสม

๕.๘.๒ ให้ผู้มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ ทางเว็บไซต์กรมที่ดินจะต้องดำเนินการด้วยตนเอง โดยห้ามมิให้ผู้อื่นดำเนินการแทน

๕.๘.๓ มีการทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้มีความทันสมัย และเป็นมาตรฐานที่ยอมรับอย่างน้อยปีละหนึ่งครั้ง

๖. บทลงโทษและการบังคับใช้

๖.๑ ผู้ใช้งานที่มีเจตนาฝ่าฝืนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมที่ดิน ตามเอกสารฉบับนี้ แม้ว่าการฝ่าฝืนนั้นจะกระทำไม่บรรลุผลโดยสมบูรณ์ ให้ถือว่ามีความผิดโดยสมบูรณ์

๖.๒ หากผู้ใช้งานไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมที่ดิน ก่อให้เกิดความเสียหายต่อบุคคลอื่น หรือต่อทรัพย์สินของทางราชการ จะต้องรับโทษตามบทลงโทษต่อไปนี้

(๑) โทษขั้นต้น ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร เป็นเวลา ๗ วัน

(๒) โทษขั้นกลาง ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร เป็นเวลา ๓๐ วัน

(๓) โทษขั้นสูง ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร เป็นเวลา ๓ เดือน

(๔) โทษขั้นร้ายแรง ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่ายสื่อสาร เป็นเวลา ๑ ปี และหากการละเมิดฝ่าฝืนให้เกิดความเสียหายต่อผู้อื่น หรือต่อทรัพย์สินของทางราชการอย่างร้ายแรง ให้ลงโทษผู้กระทำความผิดตามระเบียบกฎหมายที่เกี่ยวข้องนั้น ๆ

.....