แผนการตรวจสอบและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และสารสนเทศของกรมกิจการเด็กและเยาวชน ประจำปี พ.ศ. 2566

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญและมีบทบาทอย่างมากสำหรับองค์กร ซึ่งจะช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และประหยัดต้นทุนในการดำเนินงานด้านต่าง ๆ เช่น การมีเว็บไซต์สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสารต่าง ๆ และการรับ – ส่งจดหมายอิเล็กทรอนิกส์ เป็นต้น และถึงแม้ว่าระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และช่วยอำนวยความสะดวกในด้านต่าง ๆ แต่ในขณะเดียวกันก็มีความเสี่ยงสูง ซึ่งอาจก่อให้เกิดความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้บริการเชื่อมโยงข้อมูลผ่านเครือข่ายคอมพิวเตอร์จากที่ต่าง ๆ ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น และอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ สิ่งเหล่านี้ล้วนเป็นการสร้างความเสียหายต่อระบบเทคโนโลยีสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้น ผู้ใช้งาน ผู้ดูแลระบบ และผู้พัฒนาระบบเทคโนโลยีสารสนเทศของกรมกิจการเด็กและเยาวชน จึงต้องตระหนักและให้ความสำคัญ ในการควบคุม ดูแล และรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการเด็กและเยาวชน ร่วมกัน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการเด็กและเยาวชน ฉบับนี้ ได้จัดทำขึ้นเพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง อย่างไรก็ตามการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือและถือปฏิบัติอย่างเคร่งครัดจากทุกหน่วยงาน ซึ่งต้องมีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงให้สอดคล้องกับการพัฒนางานด้านเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไปอย่างรวดเร็ว กองยุทธศาสตร์และแผนงาน จึงหวังเป็นอย่างยิ่งว่า แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมกิจการเด็กและเยาวชนฉบับนี้ จะเป็นประโยชน์กับผู้ใช้งาน ผู้ดูแลระบบ และผู้พัฒนา รวมถึงผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของกรมกิจการเด็กและเยาวชน ทุกคน เพื่อใช้เป็นเครื่องมือและแนวปฏิบัติในการดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานต่อไป

กรมกิจการเด็กและเยาวชน

สิงหาคม ๒๕๖๖

สารบัญ

เรื่อง **หน้า**

แนวทางการตรวจสอบและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของกรมกิจการเด็กและเยาวชน ประจำปี พ.ศ. ๒๕๖๖

บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีผลบังคับใช้เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ เพื่อให้สามารถป้องกัน หรือรับมือภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ซึ่งกรมกิจการเด็กและเยาวชนมีภารกิจเกี่ยวกับการส่งเสริมและพัฒนาศักยภาพของเด็ก เยาวชน การคุ้มครองและพิทักษ์สิทธิเด็ก การส่งเสริมสวัสดิการเด็กและครอบครัว ดังนั้นเพื่อให้การดำเนินงานตามภารกิจของหน่วยงานสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายอื่น ๆ ที่เกี่ยวข้อง และเพื่อเป็นการสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐและเอกชนให้บรรลุตามเป้าหมายที่กำหนดไว้ รวมทั้งให้สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวง เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งช่วยลดโอกาสที่จะเกิดความเสียหายต่อการดำเนินงาน ทรัพย์สิน และบุคลากรของหน่วยงาน

ดังนั้น กรมกิจการเด็กและเยาวชน (ดย.) จึงได้จัดทำแผนการตรวจสอบและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของ ดย. ประจำปี พ.ศ. ๒๕๖๖ ฉบับนี้ขึ้น เพื่อใช้เป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของ ดย. ซึ่งบุคลากรของ ดย. และหน่วยงานภายนอกที่เกี่ยวข้อง จะต้องปฏิบัติตามอย่างเคร่งครัด ทั้งนี้ ได้กำหนดมาตรการ แนวทางและขั้นตอนการปฏิบัติ ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ได้อย่างปลอดภัยและคุ้มค่า

วัตถุประสงค์

๑. เพื่อให้มีวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของ ดย. ซึ่งสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อถือปฏิบัติอย่างเคร่งครัด

๒. เพื่อสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ให้แก่เจ้าหน้าที่ทุกระดับของ ดย. และบุคคลที่เกี่ยวข้อง

๓. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของ ดย.

องค์ประกอบ

๑. คำนิยาม

คำนิยามที่ใช้ ประกอบด้วย

(๑) **ดย.** หมายความว่า กรมกิจการเด็กและเยาวชน

(๒) **สท.** หมายความว่า กลุ่มสารสนเทศและเทคโนโลยี กองยุทธศาสตร์และแผนงาน

(๓) **ผู้ใช้งาน** หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้าง และบุคคลอื่นที่ได้รับอนุญาตให้ใช้งานเครือข่ายคอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต หรือ E-mail ที่ ดย. จัดสรรให้

(๔) **ผู้ดูแลระบบ** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบสารสนเทศ หรือระบบเครือข่าย หรือระบบคอมพิวเตอร์

(๕) **เจ้าหน้าที่** หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของ ดย.

(๖) **สิทธิ์ของผู้ใช้งาน** หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของ ดย.

(๗) **สินทรัพย์** หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับ ดย.

(๘) **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๙) **ความมั่นคงปลอดภัยด้านสารสนเทศ** (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

(๑๐) **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๑) **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของ ดย. ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๑๒) **ระบบเครือข่าย** หมายความว่า กลุ่มของคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และสื่อนำสัญญาณ ที่ถูกนำมาเชื่อมต่อกัน ผ่านอุปกรณ์ด้านการสื่อสารหรือสื่ออื่นใด ซึ่งทาง ดย. เป็นผู้กำหนด และทำให้ผู้ใช้ในระบบเครือข่ายสามารถติดต่อสื่อสารแลกเปลี่ยนและใช้อุปกรณ์หรือทรัพยากรต่าง ๆ ของเครือข่ายร่วมกันได้ โดยเครือข่ายคอมพิวเตอร์จะครอบคลุมทั้งเครือข่ายภายในหรือแลน (Local Area Network : LAN) แลนไร้สายหรือไวเลสแลน (Wireless LAN , WLAN) และเครือข่ายวงกว้างหรือแวน (Wide Area Network : WAN) ของ ดย.

(๑๓) **ระบบสารสนเทศ** หมายความว่า ระบบที่ประกอบด้วย ส่วนต่าง ๆ ได้แก่ Hardware, Software, User, Data และ Procedure ซึ่งทุกองค์ประกอบนี้ทำงานร่วมกัน เพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งาน เพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์ และติดตามผลการดำเนินงานของ ดย.

(๑๔) **การใช้งานอินเทอร์เน็ต** หมายความว่า การใช้บริการต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ตของ ดย.

(๑๕) **คอมพิวเตอร์** หมายความว่า คอมพิวเตอร์ที่มีการเชื่อมต่อเพื่อใช้งานเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต ที่ ดย.

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

(๑๗) **รหัสผ่าน** (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๑๘) **จดหมายอิเล็กทรอนิกส์** (E-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

(๑๙) **ชุดคำสั่งไม่พึงประสงค์** หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(๒๐) **หน่วยงานภายนอก** หมายความว่า องค์กรหรือหน่วยงานที่ ดย. อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของ ดย. โดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล หรือหน่วยงานที่ ดย. ดำเนินการส่งหรือเข้าถึงข้อมูลสารสนเทศ

๒. โครงสร้างการจัดการความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๒.๑ กำหนดหน้าที่ความรับผิดชอบด้านไซเบอร์

เพื่อให้เกิดความชัดเจนในการปฏิบัติงานของผู้ปฏิบัติงานและเป็นการยืนยันตัวบุคคล ซึ่งเป็นการลดความเสี่ยงในการเข้าถึงและใช้งานทรัพย์สินสารสนเทศ ให้หน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้อง ต้องดำเนินงานดังนี้

๑) จัดทำทะเบียนรายชื่อผู้มีหน้าที่ความรับผิดชอบ ซึ่งมอบหมายหน้าที่ให้แก่ผู้ปฏิบัติงานในการเข้าถึงส่วนสำคัญของระบบงาน และกำหนดหน้าที่ความรับผิดชอบของงานในแต่ละหน้าที่ที่ปฏิบัติงานอยู่อย่างชัดเจนเป็นลายลักษณ์อักษร ประกอบด้วย รายชื่อผู้ดูแลระบบเครือข่าย (Network Administrator) รายชื่อผู้พัฒนาระบบ (Developer Administrator) ผู้ดูแลระบบงาน (Application Administrator) ผู้ดูแลระบบ (System Administrator) ผู้ดูแลห้องคอมพิวเตอร์ ผู้ดูแลพื้นที่ควบคุม รายชื่อผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ รายชื่อผู้ควบคุมข้อมูลส่วนบุคคล และรายชื่อผู้ดูแลระบบที่จัดเก็บข้อมูลส่วนบุคคล

๒) กำหนดบุคลากรสำรองในงานที่สำคัญ เพื่อทำงานทดแทนในกรณีจำเป็น เช่น ผู้ดูแลระบบงาน (Application Administrator) ผู้บริหารระบบ (System Administrator)

๓) หน่วยงานต้องประเมินความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ รวมทั้งบริหารจัดการความเสี่ยงอย่างมีประสิทธิภาพ

๔) หน่วยงานต้องระบุและตรวจสอบทะเบียนทรัพย์สินสารสนเทศของหน่วยงาน รวมทั้งทบทวนปรับปรุงให้ทันสมัยอยู่เสมอ

๕) หน่วยงานต้องทำการประเมินความสามารถและข้อจำกัดต่าง ๆ ในการปฏิบัติตามมาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๒.๒ แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ

<u>บทบาทและความรับผิดชอบ</u>

การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ ต่อ ดย. หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ดย. และป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่น และการเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยได้กำหนดบทบาทและความรับผิดชอบให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย ดังนี้

๑) อธิบดีกรมกิจการเด็กและเยาวชนเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย.

๒) ผู้อำนวยการกองยุทธศาสตร์และแผนงาน มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ดย. โดยกำหนดมาตรการ และกำกับดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ดย.

๓) ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ดย.

๔) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ตามสิทธิ์ที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ดย.

๒.๓ หน้าที่ความรับผิดชอบของผู้ดูแลระบบ

๑) จัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

๒) บริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์ และระบบเครือข่ายหลักของ ดย. เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหาย ใช้งานไม่ได้ หรือสูญหาย

๓) เก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

๔) กำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ตามที่ได้รับมอบหมาย โดยกำหนดสิทธิ์ให้ผู้ใช้งานสามารถใช้งานได้ตามภารกิจของผู้ใช้งาน และสามารถเข้าใช้ได้แต่เพียงงานที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๕) บริหารจัดการการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ดย. ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันทีและในกรณีจำเป็น เพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นต่อ ดย. ให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานดังกล่าวทันที

๖) ติดตั้งและเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ที่ได้รับมอบหมาย และทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยเดือนละครั้ง

๗) บริหารจัดการข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เกี่ยวข้องกับการปฏิบัติงานของ ดย. สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง ให้มีความปลอดภัย

๘) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของ ดย. เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้งานและต้องเก็บรักษาไว้อย่างครบถ้วนถูกต้อง ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

๙) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

๑๐) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑๑) คืนทรัพย์สินของ ดย. ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้บริหารของ ดย. หรือผู้ที่ได้รับมอบหมาย เพื่อการตรวจสอบการคืนทรัพย์สิน

๒.๔ หน้าที่ความรับผิดชอบของผู้ใช้งาน

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีแนวทางปฏิบัติ ดังนี้

๑) การใช้งานรหัสผ่าน (Password Use) ผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

(๑) ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(๒) ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

(๓) ผู้ใช้งานต้องจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

(๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(๕) ผู้ใช้งานต้องตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำกำหนดไว้

(๖) ผู้ใช้งานต้องตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

(๗) ผู้ใช้งานต้องไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

(๘) ผู้ใช้งานต้องหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วย อักขระที่เรียงกัน เช่น ๑๒๓, abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑, aaa เป็นต้น

(๙) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด หรืออย่างน้อยทุก ๖ เดือน

(๑๐) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(๑๑) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอิน (Log in) เข้าสู่ระบบงาน

(๑๒) ผู้ใช้งานต้องไม่กำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง

(๑๓) ผู้ใช้งานต้องไม่ใช้รหัสผ่านของตนร่วมกับผู้อื่น

(๑๔) ผู้ใช้งานต้องหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ใช้งาน

๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

(๑) ผู้ใช้งานต้องออกจากระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. โดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องโน้ตบุ๊ก

(๒) ผู้ใช้งานต้องล็อค (Lock) อุปกรณ์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

(๓) ผู้ใช้งานต้องป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศและการสื่อสารของตน โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

(๔) ผู้ใช้งานและผู้ดูแลระบบต้องตั้งให้เครื่องคอมพิวเตอร์ล็อค (Lock) หน้าจอหลังจากที่ไม่ได้ใช้งาน มาช่วงระยะเวลาหนึ่ง เช่น ๑๕ นาที หลังจากที่มีการล็อค (Lock) หน้าจอแล้วนั้น ต้องใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบงานได้

(๕) ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้เจ้าหน้าที่เข้าใจในมาตรการป้องกันที่ได้กำหนดไว้นั้น

(๖) ปิดเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือไม่มีการใช้งานนานเกินกว่า ๑ ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องแม่ข่ายที่ให้บริการ ซึ่งต้องใช้งานตลอด ๒๔ ชั่วโมง

(๗) ตั้งค่าให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้ใช้งานนานเกินกว่า ๑๕ นาที

๓) การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์

(๑) การควบคุมทรัพย์สินสารสนเทศ (clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูลและแฟ้มข้อมูล เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงระบบสารสนเทศและข้อมูลสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ มีแนวทางปฏิบัติ ดังนี้

(๑.๑) ผู้ใช้งานต้องป้องกันทรัพย์สินของ ดย. และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยให้ครอบคลุมเรื่องต่าง ๆ ประกอบด้วย

- การจัดการบริเวณล้อมรอบ
- การควบคุมการเข้า - ออกพื้นที่
- การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์
- ระบบและอุปกรณ์สนับสนุนการทำงาน

(๑.๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

(๑.๓) ต้องมีการป้องกันเครื่องคอมพิวเตอร์หรือระบบงานของ ดย. ก่อนเข้าใช้งานโดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสม

(๑.๔) ต้องมีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของ ดย.
- จัดเก็บเอกสาร ข้อมูลในการทำงาน ข้อมูลสำคัญหรือลับ หรือสื่อบันทึกข้อมูล ไว้ในสถานที่ที่มีความปลอดภัยภายหลังจากใช้งานเสร็จ เช่น เก็บไว้ในตู้ที่ล็อคกุญแจได้ เป็นต้น

- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน

- ป้องกันเครื่องโทรสารที่ใช้ในการติดต่อสื่อสารหรือส่งข้อมูลสำคัญ เมื่อไม่มีผู้ใช้งาน

- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น

- นำเอกสารสำคัญหรือลับออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

- ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึกคอมพิวเตอร์ หรือสารสนเทศ ออกจาก ดย. ต้องขออนุมัติจากผู้บังคับบัญชาก่อนทุกครั้ง

(๑.๕) ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

(๑.๖) ผู้ดูแลระบบต้องบริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์ และระบบเครือข่ายหลักของ ดย. เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหายใช้งานไม่ได้ หรือสูญหาย

(๑.๗) ผู้ดูแลระบบต้องเก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

(๑.๘) การทำลายข้อมูลอิเล็กทรอนิกส์ มีวิธีการ ดังนี้

- ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในแผ่น CD/DVD ใช้วิธีการย่อยทำลายแผ่น CD/DVD

- ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในเทป DDS, DAT, LTO จะต้องทำการลบข้อมูลทั้งม้วนเทป (Erase) ผ่าน Tape Device ก่อนการทำลายม้วนเทป

- ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในฮาร์ดดิสก์ (Hard Disk) หรือ Memory Devices เช่น USB flash drive, SD cards ให้ทำลายข้อมูลโดยใช้เทคโนโลยีซอฟต์แวร์ Wiping ที่สอดคล้องกับมาตรฐาน DoD ๕๒๒๐-๒๒M 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) ในการลบแฟ้มข้อมูล/ไฟล์ข้อมูล โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://eraser.heidi.ie/download.php

(๒) การเข้าถึงและควบคุมการใช้งานระบบคอมพิวเตอร์หรือสารสนเทศ ต้องจัดทำนโยบายและแนวปฏิบัติในการควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงอย่างน้อยปีละ ๑ ครั้ง

โดยการจัดทำนโยบายนี้ จะพิจารณาจากความต้องการทางการปฏิบัติงาน และทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ ซึ่งมีแนวทางปฏิบัติ ดังนี้

(๒.๑) การควบคุมการเข้าถึงเครือข่าย (Network access control)

- ต้องจัดทำนโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้งานได้ บริการใดไม่สามารถใช้งานได้

- ต้องมีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ทั้งภายในและภายนอก ดย. (User authentication for external connections) ก่อนที่จะอนุญาตให้เข้าใช้งานเครือข่ายและระบบสารสนเทศของ ดย. ได้

- ต้องมีการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks) ให้สามารถระบุและพิสูจน์ตัวตน เพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

- ต้องมีการแบ่งแยกเครือข่าย (Segregation in networks) ตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

- ต้องมีการควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) โดยต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายในการควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางการปฏิบัติงานได้ระบุไว้

- ต้องมีการควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) เพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายในการควบคุมการเข้าถึง

(๒.๒) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

- ต้องมีการปฏิบัติตามขั้นตอนในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures) สำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ

- ต้องมีการระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication) โดยต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

- ต้องจัดให้มีระบบบริหารจัดการรหัสผ่าน (Password management system) ที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

- ต้องมีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (User of system utilities) เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว

- ต้องกำหนดให้มีการหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out) โดยต้องกำหนดให้ระบบตัดการใช้งานของผู้ใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่ง

- ต้องมีการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ของระบบสารสนเทศที่มีความสำคัญสูง

(๒.๓) การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (Application and information access control)

- ต้องมีการจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอพพลิเคชั่น (Information access restriction) โดยการเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

- ต้องมีการแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation) ไว้ในบริเวณที่แยกต่างหากออกมา สำหรับระบบนี้โดยเฉพาะ

๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ มีแนวปฏิบัติ ดังนี้

(๑) ทำการประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสม สำหรับข้อมูลที่จำเป็นต้องป้องกัน

(๒) กำหนดหลักการทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล

(๓) การจัดเก็บ username และ password ของระบบสารสนเทศลงในฐานข้อมูลใด ๆ จะต้องทำการเข้ารหัสด้วย MD๕ ใน field ของ password ก่อนบันทึกลงในฐานข้อมูลทุกครั้ง

(๔) ต้องมีการเชื่อมต่อโดยการเข้ารหัส SSL ผ่านโปรโตคอล https สำหรับระบบสารสนเทศแบบ web application เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่างเบราว์เซอร์และเว็บเซิร์ฟเวอร์

(๕) กำหนดช่องทางการรับ – ส่งข้อมูลสำคัญหรือข้อมูลลับที่เหมาะสมกับ ดย. สำหรับช่องทาง ดังต่อไปนี้

- ระบบการสื่อสารข้อมูล ซึ่งรวมถึง LAN และอินเทอร์เน็ต
- เครือข่ายไร้สายและอุปกรณ์เครือข่ายไร้สาย
- สื่อบันทึกข้อมูลที่สามารถถอดแยกได้ (จากตัวเครื่องคอมพิวเตอร์)

(๖) กำหนดวิธีการในการบริหารจัดการและการใช้งานกุญแจสำหรับการเข้ารหัสข้อมูล ดังนี้

- วิธีการป้องกันกุญแจที่ใช้สำหรับการเข้ารหัสข้อมูล
- วิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจเกิดการสูญหายหรือถูกทำให้เสียหาย
- บทบาทและผู้มีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการเข้ารหัสข้อมูล ประกอบด้วย ผู้ทำหน้าที่ควบคุมและดูแลกุญแจ การสร้างกุญแจ ผู้ทำหน้าที่ทำลาย ผู้ใช้งาน ผู้ทำหน้าที่จัดการกรณีกุญแจเกิดการสูญหาย

(๗) ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับ หรือวิธีการรักษาความลับของข้อมูล ดังนี้

- ต้องแสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ด้วยการใช้การเข้ารหัสข้อมูลตามมาตรฐานที่ ดย. กำหนด

- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการกำหนดรหัสผ่านสำหรับไฟล์ที่มีการใช้งาน

(๘) ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายของ ดย. เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

(๙) ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอ ในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูล ว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

(๑๐) ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

(๑๑) ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

๓. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๓.๑ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย มีแนวทางปฏิบัติ ดังนี้

๑) กยผ. โดย สท. ทำหน้าที่กำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ และระบบข้อมูล เพื่อจุดประสงค์ในการเฝ้าระวัง การควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจจะเกิดขึ้นได้

๒) การกำหนดและจำแนกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ประกอบด้วย พื้นที่ส่วนต่างๆ ตามตำแหน่งของพื้นที่ใช้งาน แบ่งออกเป็นพื้นที่ทำงานทั่วไปของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศและผู้ดูแลระบบ พื้นที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) และจัดเก็บข้อมูลคอมพิวเตอร์ พื้นที่ติดตั้งอุปกรณ์ระบบเครือข่าย (Network Equipment area) พื้นที่ห้องควบคุมระบบไฟฟ้าสำรอง พื้นที่ห้องปฏิบัติงาน และ Help Desk

๓) การกำหนดสิทธิ์ให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิ์เข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย และทำการปรับปรุงรายการผู้มีสิทธิ์เข้า - ออกพื้นที่ ทุกครั้งที่มีการเปลี่ยนแปลง

๓.๒ การควบคุมการเข้า – ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย ดย.(Server Room) มีแนวทางปฏิบัติ ดังนี้

๑) ผู้ดูแลระบบจัดทำเอกสารแบบฟอร์มการบันทึกการเข้า - ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ซึ่งต้องระบุรายละเอียดอย่างน้อยดังนี้ ชื่อ-นามสกุล ตำแหน่ง หน่วยงาน พื้นที่หรือเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับสิทธิ์ รายละเอียดกิจกรรม ระยะเวลาดำเนินการ และบันทึกการเข้า - ออกพื้นที่ใช้งานอย่างสม่ำเสมอ

๒) ผู้ดูแลระบบตรวจสอบการบันทึกการเข้า - ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ทุกครั้งที่มีการใช้งาน และบันทึกรายการอุปกรณ์ให้ถูกต้อง โดยผู้ดูแลระบบจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา รวมทั้งตรวจสอบการบันทึกการเข้า - ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) เป็นประจำอย่างน้อยเดือนละ ๑ ครั้ง

๓) ผู้ดูแลระบบควรมีระบบป้องกันและตรวจสอบการเข้า - ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) อย่างปลอดภัย เช่น สมาร์ทการ์ด (Smartcard) เป็นต้น

๔) ผู้ใช้งานที่ต้องการเข้าใช้ห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) จะต้องขออนุญาตและบันทึกการเข้า - ออกพื้นที่ทุกครั้ง

๕) หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าใช้ห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ผู้ดูแลระบบต้องตรวจสอบเหตุผลและความจำเป็นก่อนอนุญาต และจดบันทึกการเข้า - ออกพื้นที่ไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

๓.๓ ผู้ดูแลระบบห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) มีแนวทางปฏิบัติ ดังนี้

๑) สิทธิ์ในการเข้า - ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยีหรือผู้ดูแลระบบที่ได้รับมอบหมาย เป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room)

๒) การเข้าถึงห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ต้องมีการลงบันทึกไว้ในเอกสารแบบฟอร์มการเข้า - ออกทุกครั้ง

๓) ต้องจัดทำระบบการจัดเก็บบันทึกการเข้า - ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ไว้ด้วย

๔) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้า - ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ผู้ดูแลระบบจะต้องควบคุมอย่างรัดกุม

๓.๔ <u>ผู้ติดต่อจากหน่วยงานภายนอก</u> มีแนวทางปฏิบัติ ดังนี้

๑) ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผู้ติดต่อ ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ใน ดย.

๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานเข้ามาปฏิบัติงานในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ต้องลงบันทึกรายการอุปกรณ์ ตามที่ระบุไว้ในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ให้ถูกต้องชัดเจน

๓) ผู้ดูแลระบบ ควรตรวจสอบความถูกต้องของข้อมูลที่บันทึกในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) เป็นประจำทุกเดือน

๔. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

๔.๑ การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

๑) Wireless Policy ครอบคลุมทุกโฮสต์ในเครือข่ายของ ดย. และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง Wireless Policy อาจมีการเปลี่ยนแปลงตามเทคโนโลยีใหม่ และกระบวนการที่สอดคล้องและเหมาะสมในอนาคต

๒) ผู้ดูแลระบบ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าการให้บริการ และการเชื่อมต่อเครื่องไร้สายทั้งหมด

๓) การจัดการจุดเชื่อมต่อไร้สายในพื้นที่ ดย. จะต้องถูกตรวจสอบอุปกรณ์ติดตั้ง และกำหนดค่าโดยผู้ดูแลระบบเท่านั้น

๔) ทุกจุดเชื่อมต่อเครือข่ายไร้สาย และอุปกรณ์ที่เกี่ยวข้อง เช่น Access Point จุดเชื่อมต่อสายสัญญาณ Switch จะต้องมีความปลอดภัย มีรูปแบบในการจัดเก็บ และเข้าถึงอุปกรณ์

๕) ฟังก์ชันที่ใช้ในการตั้งค่าของจุดเชื่อมต่อจะต้องสามารถเข้าถึงได้เฉพาะผู้ที่มีหน้าที่ในการดูแลระบบ

๖) จุดเชื่อมต่อจะต้องมีการกำหนดค่า Gateway ที่เป็นค่าที่กำหนดไว้ของเครือข่ายส่วนนั้นเท่านั้น

๗) ผู้ดูแลระบบ ต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๘) SSID ที่กำหนดจะต้องถูกต้องตามรูปแบบที่ กยผ. โดย สท. กำหนดไว้ และจะต้องไม่มีการบ่งบอก หรือแสดงตำแหน่งของสายที่จุดเชื่อม LAN หรือ ชื่ออื่นๆ

๙) SSID จะต้องถูกยกเลิกค่าการ Broadcast ยกเว้น จุดที่ กยผ. โดย สท. อนุญาต

๑๐) อุปกรณ์จะไม่สามารถเชื่อมต่อกับเครือข่ายไร้สายได้ จนกว่าจะสามารถระบุ SSID ที่ถูกต้อง ในกรณีที่มีการยกเลิกค่าการ Broadcast

๑๑) เลือกใช้เทคโนโลยี Authentication และมีการกำหนดค่าการเข้ารหัสในการเชื่อมต่อ

๑๒) อุปกรณ์ที่ใช้ในการเข้าถึงเครือข่ายของ ดย. จะต้องรองรับมาตรฐาน IEEE ๘๐๒.๑๑g การเชื่อมต่อจะต้องมีซอฟต์แวร์ป้องกันไวรัส

๑๓) ทุกจุดเชื่อมจะต้องกำหนดรหัสผ่านเพื่อเข้าใช้งาน คุณลักษณะการจัดการรหัสผ่านนี้ จะถูกเก็บไว้และส่งในรูปแบบที่เข้ารหัส

๑๔) SNMP จะต้องถูกยกเลิกหากไม่จำเป็นสำหรับการบริหารจัดการเครือข่าย หรือหากมีความจำเป็นต้องใช้ จะต้องมีการเปลี่ยนค่า Community String

๑๕) อุปกรณ์เครือข่ายไร้สายทั้งหมดต้องผ่านความเห็นชอบจาก ดย.

๑๖) ห้ามไม่ให้เจ้าหน้าที่ หรือทีมงานเครือข่ายบอกค่าติดตั้งของเครือข่ายไร้สายกับผู้ใช้งานหรือบุคคลภายนอก

๑๗) สท. มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายไร้สายของอุปกรณ์ทุกชนิด ที่ไม่เป็นไปตามนโยบาย หรือมีความเสี่ยงต่อระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้ล่วงหน้า

๑๘) ผู้ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

๔.๒ การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

๑) ผู้ดูแลระบบ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

๒) การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๓) ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อกโดยไฟร์วอลล์

๔) ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Log in Account ก่อนการใช้งานทุกครั้ง

๕) ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๖) การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๗) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๘) การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทาง ดย. อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือจากที่กำหนด จะต้องได้รับความยินยอมจาก ดย.

๙) การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

๑๐) จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๑๑) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีๆไป

๑๒) สท. มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

๑๓) การเชื่อมต่อในลักษณะของการ Remote Log in จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการ ตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจาก กยผ. โดย สท.

๑๔) ผู้ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

๔.๓ การรักษาความมั่นคงปลอดภัยของระบบตรวจจับการบุกรุก (Intrusion Detection System/Intrusion Prevention System Policy : IDS/IPS Policy)

๑) IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายใน ดย. ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

๒) IDS/IPS Policy ครอบคลุมทุกโฮสต์ในเครือข่ายของ ดย. และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

๓) ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๔) ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

๕) โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๖) มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

๗) มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๘) IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

๙) เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๑๐) พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

๑๑) พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงนับจากที่ตรวจพบ

๑๒) การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๑๓) มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

๑๔) กยผ. โดย สท. มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้ล่วงหน้า

๑๕) ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของ ดย. การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบ ของ ดย. จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

๔.๔ <u>การป้องกันไวรัสและภัยคุกคามอื่น ๆ ในการใช้งานคอมพิวเตอร์</u>

๑) ผู้ใช้งานควรทำการสำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้ เช่น บนแผ่น CD หรือ DVD หรือ Flash Drive หรือ Memory Card เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

๒) ห้ามผู้ใช้งานปรับแต่ง หรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันไวรัส ที่ ดย. ติดตั้งให้

๓) ผู้ใช้งานควรมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบว่ามีการ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้ กยผ. โดย สท. ทราบ หากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

๔) ผู้ใช้งานต้องแจ้งให้ กยผ. โดย สท. ทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อสงสัยว่ามีการติดไวรัส

๕) ผู้ใช้งานต้องตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นทุกครั้ง เมื่อมีการติดตั้งหรือใช้งานด้วยซอฟต์แวร์ป้องกันไวรัส และหากตรวจพบไวรัสจะต้องรีบจัดการทำลายไวรัสโดยเร็วที่สุด หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมนั้น ห้ามทำการเปิดข้อมูลหรือติดตั้งโปรแกรมลงไปบนเครื่องที่ใช้งานอยู่เด็ดขาด

๔.๕ <u>การใช้เครื่องคอมพิวเตอร์อย่างปลอดภัยและมีประสิทธิภาพ</u>

๑) ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์คอมพิวเตอร์ใด ๆ ลงบนเครื่องคอมพิวเตอร์ หากมีความจำเป็นในการติดตั้งซอฟต์แวร์จะต้องแจ้งให้ผู้ดูแลระบบทราบ

๒) ห้ามผู้ใช้งานติดตั้งอุปกรณ์เครือข่ายเพิ่มเติม เว้นแต่จะให้ กยผ. โดย สท. ดำเนินการให้

๓) ผู้ใช้งานที่ต้องการนำคอมพิวเตอร์มาใช้งานภายใต้เครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตที่ ดย. จัดสรรให้ จะต้องมีซอฟต์แวร์ป้องกันไวรัส ซึ่งสามารถ Update ให้เป็นปัจจุบัน และต้องสามารถตรวจจับ Malware อื่น ๆ เช่น Spyware ได้ด้วย หรือแจ้ง กยผ. โดย สท. ให้ทำการติดตั้งซอฟต์แวร์ป้องกันไวรัสให้

๔) ห้ามผู้ใช้งานใช้โปรแกรมประเภทดักจับข้อมูลผู้ใช้งานบนเครือข่าย

๔.๖ <u>การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ</u>

๑) เสริมเนื้อหาแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ดย. เข้ากับหลักสูตรฝึกอบรมต่าง ๆ ตามแผนการฝึกอบรมของ ดย.

๒) เผยแพร่ประชาสัมพันธ์/รณรงค์ให้ความรู้ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในลักษณะเกร็ดความรู้หรือข้อระวัง ในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๕. แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน

แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) มีวิธีการปฏิบัติ ดังนี้

๕.๑ การลงทะเบียนผู้ใช้งาน (User Registration)

๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. โดยต้องระบุข้อมูลพื้นฐานเป็นอย่างน้อย เช่น ชื่อ นามสกุล ตำแหน่ง และหน่วยงาน

๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานว่าไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๕) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. โดยทันที เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๖) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. โดยไม่ได้รับอนุญาต

๕.๒ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

๑) ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒) ผู้ดูแลระบบต้องกำหนดระดับสิทธิ์ในการเข้าถึงที่เหมาะสม สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย.

๓) ผู้ดูแลระบบต้องมอบหมายสิทธิ์ ให้มีความสอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

๔) ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

๕) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด โดยให้มีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และให้มีการกำหนดสิทธิ์พิเศษที่ได้รับด้วยว่า การเข้าถึงได้นั้นสามารถเข้าถึงได้ในระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๖) ผู้ใช้บริการต้องรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. และต้องปฏิบัติตามอย่างเคร่งครัด

๕.๓ ระบบบริหารจัดการรหัสผ่าน (Password Management System)

๑) ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

๒) ระบบบริหารจัดการรหัสผ่าน ต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนปฏิบัติ เพื่อยืนยันรหัสผ่านที่ตั้งใหม่

๓) ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเลือกรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น เช่น ไม่ใช้ชื่อ นามสกุล วันเกิด หมายเลขโทรศัพท์ เป็นต้น

๔) ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๖ เดือน

๕) ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชีผู้ใช้งาน และทำการล็อกอิน (Log in) เข้าใช้งานระบบงานเป็นครั้งแรก

๖) ระบบบริหารจัดการรหัสผ่าน ต้องสามารถระบุข้อผิดพลาดในการตั้งรหัสผ่านของผู้ใช้งานได้ เช่น รหัสผ่านมีความยาวของตัวอักขระน้อยกว่าที่กำหนด มีชื่อผู้ใช้งานอยู่ในรหัสผ่าน เป็นต้น

๗) ระบบบริหารจัดการรหัสผ่าน ต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน (Log in) เช่น ให้แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอ เป็นต้น

๘) ระบบบริหารจัดการรหัสผ่าน ต้องมีการจัดเก็บรหัสผ่านเดิมที่ผู้ใช้งานเคยตั้งไปแล้ว เพื่อตรวจสอบไม่ให้นำกลับมาใช้ใหม่ตามระยะเวลาที่เหมาะสม

๙) การจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานจะต้องแยกต่างหากจากข้อมูลของระบบงาน

๑๐) ระบบบริหารจัดการรหัสผ่าน ควรป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้ และ/หรือ ที่จำเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น โดยการเข้ารหัสข้อมูลการคำนวณผลรวม (Hash) เพื่อซ่อนข้อมูลไว้

๕.๔ <u>การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)</u>

๑) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนาม เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งาน ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย.

๒) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติ สำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๓) ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น

๔) ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น และต้องกำหนดรหัสผ่านที่แตกต่างกัน

๕) ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์ (E-mail) เป็นช่องทางในการส่ง และกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

๕.๕ <u>การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)</u>

๑) ผู้ดูแลระบบดำเนินการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๒) ผู้ดูแลระบบทบทวนสิทธิ์สำหรับผู้ที่มีสิทธิ์ในระดับสูง เช่น สิทธิ์ในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๓) ผู้ดูแลระบบทบทวนสิทธิ์ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

๔) ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิ์ในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

๕) ผู้ดูแลระบบต้องดำเนินการตรวจสอบสิทธิ์และติดตามการใช้งานตามสิทธิ์ที่ได้รับของแต่ละระบบ

๖) ผู้ดูแลระบบต้องกำหนดให้มีการเพิกถอนสิทธิ์หรือระงับการใช้งานของแต่ละสิทธิ์แตกต่างกันไป ตามหน้าที่ที่รับผิดชอบในแต่ละระบบ

๖. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต มีดังต่อไปนี้

๖.๑ การใช้งานบริการระบบเครือข่าย มีแนวทางปฏิบัติ ดังนี้

๑) ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานต้องรับรองว่า หากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของ ดย.

๒) ดย. ไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๓) ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว ดย. ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๔) ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

๕) ดย. ให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ ให้กับผู้อื่นไม่ได้

๖) บัญชีผู้ใช้งาน (User Account) ที่ ดย. ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๗) ผู้ใช้บริการระบบเครือข่าย ดย. ต้องพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้บริการ

๘) การใช้งานบริการระบบเครือข่าย ดย. กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๙) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

๑๐) ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง ในระหว่างปฏิบัติงาน

๖.๒ ผู้ดูแลระบบห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) มีแนวทางปฏิบัติ ดังนี้

๑) ผู้ดูแลระบบห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ต้องทำการกำหนดสิทธิ์บุคคลในการเข้า-ออกห้องปฏิบัติการฯ โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในห้องปฏิบัติการฯ และต้องจัดทำบันทึกผู้มีสิทธิ์เข้า-ออกพื้นที่ไว้ด้วย เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

๒) สิทธิ์ในการเข้า-ออกภายในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยีหรือผู้ดูแลระบบที่ได้รับมอบหมายเป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องปฏิบัติการฯ

๓) การเข้าถึงห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ต้องมีการลงบันทึกไว้ในเอกสารแบบฟอร์มการเข้า-ออกห้องปฏิบัติการฯ ทุกครั้ง

๔) ต้องจัดทำระบบการจัดเก็บบันทึกการเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ไว้ด้วย

๕) หากเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ผู้ดูแลระบบจะต้องควบคุมอย่างรัดกุม

๖.๓ ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการลงบันทึกข้อมูลในเอกสารแบบฟอร์มการเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room)

๒) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน เข้ามาปฏิบัติงานที่ห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ต้องลงบันทึกรายการอุปกรณ์ไว้ในแบบฟอร์มการเข้า-ออกห้องปฏิบัติการฯ ให้ถูกต้องชัดเจน

๓) เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลที่บันทึกในเอกสารแบบฟอร์มการเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) เป็นประจำทุกเดือน

๔) ในกรณีที่ผู้ใช้งานต้องการเข้าถึงเครือข่ายจากภายนอก ดย. ต้องขออนุญาตและได้รับอนุญาตจากผู้มีอำนาจก่อน และเป็นผู้ที่ได้รับสิทธิ์ในการเข้าใช้บริการแล้วเท่านั้น การเข้าสู่ระบบเครือข่ายจะต้องเชื่อมผ่านด้วยวิธีการ Remote Access VPN โดยผู้ใช้งานจะต้องพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการป้อนชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) เพื่อยืนยันตัวตนของผู้ใช้งาน ในการเข้าถึงเครือข่ายในส่วนที่ได้รับอนุญาต

๖.๔ การระบุอุปกรณ์บนเครือข่าย มีแนวทางปฏิบัติ ดังนี้

๑) ทำการระบุหมายเลขอุปกรณ์บนเครือข่าย ประกอบด้วย หมายเลขเทอร์มินัล หมายเลข MAC Address และหมายเลข IP Address

๒) ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

๓) มีการใช้ไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่น ๆ เพื่อกำหนดว่าหมายเลขระบุอุปกรณ์ใดจะสามารถเข้าถึงเครือข่ายส่วนใดของ ดย.

๔) มีการรักษาความมั่นคงปลอดภัยทางกายภาพต่ออุปกรณ์คอมพิวเตอร์หรือเครือข่าย เพื่อป้องกันการเปลี่ยนแปลงแก้ไขหมายเลขระบุอุปกรณ์เหล่านั้น

๕) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๖) กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่

๗) จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

๘) ทำการทบทวนแผนผังเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

๖.๕ <u>การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ</u> มีแนวทางปฏิบัติ ดังนี้

๑) ทำการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ทั้งทางกายภาพ และโดยการล็อกอิน (Log in) เข้ามาใช้งาน

๒) ทำการล็อคอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันด้วยกุญแจ เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

๓) ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๔) ผู้ดูแลระบบต้องกำหนดการเปิด-ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงและก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๕) ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ เช่น อย่างน้อยสัปดาห์ละ ๒ ครั้ง เป็นอย่างน้อย

๖) ต้องกำหนดสิทธิ์บุคคล ในการเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) โดยให้เฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องเท่านั้น

๗) ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) หากมีความจำเป็นต้องเข้า จะต้องให้เจ้าหน้าที่ของ กยผ. โดย สท. เป็นผู้รับผิดชอบนำพาเข้าไป

๘) บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) จะต้องลงชื่อในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการฯ ให้ถูกต้อง และได้รับการอนุมัติจากผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยีก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

๙) บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้อำนวยการกลุ่มการพัฒนาระบบเทคโนโลยีก่อน

๑๐) ต้องติดตั้งระบบป้องกันและตรวจสอบการเข้า-ออกห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) อย่างปลอดภัย เช่น สมาร์ทการ์ด (Smartcard) และติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรกรรม เป็นต้น

๖.๖ <u>การแบ่งแยกเครือข่าย</u> มีแนวทางปฏิบัติ ดังนี้

๑) ดย. แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่าย โดยไม่ได้รับอนุญาต

๒) ดย. จัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยหน่วยงานของ ดย. สามารถใช้งานระบบผ่านระบบเครือข่ายภายในได้ แต่ไม่สามารถใช้งานระบบผ่านเครือข่ายภายนอกได้ เพื่อความปลอดภัยของฐานข้อมูล

๓) ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการ ผู้ใช้งาน และระบบงานต่าง ๆ ของ ดย.

๔) ผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่ง จะไม่สามารถเข้าถึงข้อมูลที่อยู่ในอีกวงเครือข่ายหนึ่งได้โดยตรง

๕) ต้องควบคุมการเข้าถึงทางกายภาพสำหรับเครือข่ายย่อย เพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อยและป้องกันการเปลี่ยนแปลงแก้ไขสายสัญญาณ ดักแอบดูข้อมูลบนเครือข่าย หรืออื่น ๆ โดยไม่ได้รับอนุญาต

๖) ต้องใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย ๆ

๗) ต้องกรองและจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อย

๘) ต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอก ดย. ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของ ดย.

๙) ต้องแยกวงเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่น ๆ ของ ดย.

๑๐) ต้องแยกกลุ่มเครือข่ายเป็น ๔ ประเภทใหญ่ๆ คือ ๑) ระบบเครือข่ายภายใน ๒) ระบบเครือข่ายภายนอก ๓) ส่วนที่มีความสำคัญสูง (DMZ Zone : Demilitarized Zone) ที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก และ ๔) เครือข่ายสำหรับติดตั้งระบบงานสารสนเทศต่าง ๆ ของ ดย.

๑๑) ต้องจัดทำผังเครือข่ายที่แสดงถึงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก โดยมีการปรับปรุงให้เป็นปัจจุบันหรืออย่างน้อยปีละครั้ง

๖.๗ <u>การควบคุมการเชื่อมต่อทางเครือข่าย</u> มีแนวทางปฏิบัติ ดังนี้

๑) ต้องตรวจสอบ และจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่าย ที่สอดคล้องกับนโยบายควบคุมการเข้าถึงและข้อกำหนดของระบบงานที่ได้ระบุไว้

๒) ต้องจำกัดสิทธิ์และความสามารถของผู้ใช้งาน ในการเชื่อมต่อเข้าสู่ระบบเครือข่าย ดย.

๓) ต้องระบุอุปกรณ์และเครื่องมือที่ใช้ในการควบคุมการเชื่อมต่อระบบเครือข่าย ดย.

๔) ต้องควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่าย ดย. โดยไม่ได้รับอนุญาต

๕) ต้องใช้ไฟร์วอลล์ ทำการกรองข้อมูลที่ไหลเวียนในเครือข่าย ให้เป็นไปตามหรือสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายที่ได้กำหนดไว้

๖) ต้องจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานต่อระบบงานต่าง ๆ ของ ดย. อาทิ ระบบงานที่ใช้ในการส่งข้อความ (Messaging applications) เช่น ระบบ E-mail ระบบงานสำหรับการโอนย้ายไฟล์ ระบบงานต่าง ๆ สำหรับใช้งานภายใน ดย.

๗) ต้องจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งาน ตามวัน เวลา หรือช่วงเวลาที่อนุญาตให้ใช้งาน

๘) การเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก ดย. จะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก ซึ่งมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware)

๙) ต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้ระบบเครือข่ายของ ดย. ในลักษณะที่ผิดปกติ

๑๐) มีการป้องกันเลขที่อยู่ของไอพี (IP Address) ของระบบเครือข่ายภายใน ดย. มิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๑๑) ห้ามเปิดช่องทางการเชื่อมต่อทางเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายใน ดย. เพื่อให้สามารถเข้าถึงเครื่องแม่ข่ายสำหรับระบบงานได้จากระยะไกล ยกเว้นในกรณีที่มีความจำเป็น หรือมีความเร่งด่วนสูง ซึ่งจะต้องได้รับอนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ

๑๒) กำหนดระยะเวลาที่แน่นอนของการเชื่อมต่อจากระยะไกล เช่น ให้ใช้ในระยะเวลา ๗ วัน และหลังจากที่สิ้นสุดการใช้งาน ให้ทำการปิดช่องทางการเชื่อมต่อนั้นโดยทันที

๖.๘ <u>การควบคุมการจัดเส้นทางบนเครือข่าย</u> มีแนวทางปฏิบัติ ดังนี้

๑) ต้องใช้เกตเวย์หรืออุปกรณ์เครือข่ายเพื่อตรวจสอบ IP Address ของทั้งต้นทางและปลายทาง และควบคุมการไหลของข้อมูลผ่านเครือข่ายต่าง ๆ จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง

๒) ต้องควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๓) ต้องกำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อยหรือเครือข่ายภายในและภายนอก

๔) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย เพื่อไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

๕) ต้องกำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการเข้าใช้บริการระบบเครือข่าย ดย.

๗. แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต มีดังต่อไปนี้

๗.๑ ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานระบบปฏิบัติการที่มีความมั่นคงปลอดภัย ซึ่งเริ่มตั้งแต่การลงทะเบียน การกำหนดสิทธิ์ การบริหารจัดการรหัสผ่าน และการทบทวนสิทธิ์ต่าง ๆ รวมถึงข้อกำหนดเกี่ยวกับการอนุญาตให้เข้าใช้ และกำหนดรายละเอียดอื่นๆ เพิ่มเติม โดยมีแนวทางปฏิบัติ ดังนี้

๑) ผู้ใช้งานระบบปฏิบัติการต้องได้รับการอนุมัติจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร

๒) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพ เมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๔) ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User name และ Password ทุกครั้ง

๕) มีการจำกัดระยะเวลาในการป้อนรหัสผ่าน และหากผู้ใช้งานป้อนรหัสผ่านผิดเกิน ๓ ครั้ง ระบบจะทำการล็อคสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ผู้ใช้งานรายนั้นไม่สามารถเข้าถึงระบบปฏิบัติการได้อีกจนกว่าผู้ดูแลระบบจะดำเนินการปลดล็อคให้

๖) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

๗) ผู้ใช้งานต้องทำการลงบันทึกออก (Log out) ทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๘) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

๙) ซอฟต์แวร์ที่มีลิขสิทธิ์ของ ดย. ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

๑๐) ซอฟต์แวร์ที่ ดย. จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๑๑) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของ ดย. เพื่อประโยชน์ทางการค้า

๑๒) ในกรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม

๑๓) ห้ามผู้ใช้งานใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ในการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๗.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวทางปฏิบัติ ดังนี้

๑) มีการตั้งชื่อบัญชีผู้ใช้งานในระบบงานที่แตกต่างกัน เช่น บัญชีของผู้ใช้งานทั่วไป บัญชีของผู้ดูแลระบบ บัญชีของผู้ดูแลฐานข้อมูล บัญชีของผู้พัฒนาระบบ บัญชีของเจ้าหน้าที่ทางเทคนิคอื่น ๆ เป็นต้น

๒) ผู้ใช้งานทุกคนต้องมีชื่อผู้ใช้งานแยกจากกันของแต่ละบุคคล เพื่อใช้ในการพิสูจน์ตัวตนที่แตกต่างกัน

๓) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง ก่อนใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. โดยใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๔) ผู้ใช้งานสำหรับระบบงานที่มีความสำคัญสูง ต้องทำการพิสูจน์ตัวตนด้วยวิธีการทางเทคนิคที่มีความมั่นคงปลอดภัยสูง เช่น ใช้วิธีการเข้ารหัสข้อมูล การใช้ลายนิ้วมือ เป็นต้น

๕) ผู้ใช้งานที่สามารถเข้าถึงระบบปฏิบัติการได้ จะต้องได้รับการอนุมัติสิทธิ์การเข้าถึงระบบปฏิบัติการ จากผู้บังคับบัญชาของหน่วยงานหรือเจ้าของระบบงานเท่านั้น

๖) ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น

๗) ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้ (Account) ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น

๘) ผู้ใช้งานต้องลงบันทึกเข้า (Log in) โดยใช้บัญชีผู้ใช้ (Account) ของตนเอง และทำการลงบันทึกออก (Log out) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๗.๓ <u>การใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)</u>

ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว โดยมีแนวทางปฏิบัติ ดังนี้

๑) มีการจัดทำบัญชีรายชื่อโปรแกรมประเภทยูทิลิตี้ที่อนุญาตให้ใช้งานได้เท่านั้น

๒) มีการจำกัดผู้ที่สามารถใช้งานโปรแกรมยูทิลิตี้ และไม่อนุญาตให้ผู้ใช้งานทั่วไปสามารถใช้งานได้

๓) ผู้ใช้งานที่ต้องการใช้งานโปรแกรมยูทิลิตี้ ต้องแจ้งความจำเป็นในการขอใช้และทำการขออนุญาตจากผู้ดูแลระบบ พร้อมระบุเหตุผลความต้องการใช้งาน โดยต้องมีการลงนามเห็นชอบจากผู้บังคับบัญชาของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร

๔) การใช้งานโปรแกรมยูทิลิตี้ จะต้องได้รับอนุญาตให้ใช้งานตามระดับสิทธิ์ในการใช้งานที่ ดย. กำหนดไว้แล้ว โดยจะได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้เป็นรายครั้งไป

๕) จำเป็นต้องทำการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ทุกครั้ง แม้จะเป็นการใช้งานเพียงชั่วคราว

๖) มีการแยกจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน เช่น แยกไว้ในไดเร็คทอรี่ต่างหาก เพื่อให้ง่ายในการควบคุมและจัดการโปรแกรมเหล่านี้

๗) มีการบันทึกข้อมูลล็อคแสดงการใช้งานโปรแกรมยูทิลิตี้

๘) มีการยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้ที่ไม่มีความจำเป็นในการใช้งานแล้ว

๙) ต้องทำการตรวจสอบบันทึกการเรียกใช้งานอย่างสม่ำเสมอ

๗.๔ <u>การหมดเวลาใช้งานระบบสารสนเทศ</u>

ผู้ดูแลระบบต้องกำหนดให้ระบบสารสนเทศยุติตัวเองลง เมื่อไม่มีการใช้งานในช่วงเวลาหนึ่ง โดยมีแนวทางปฏิบัติ ดังนี้

๑) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. เช่น ระบบงาน และอุปกรณ์เครือข่าย มีการตัดและหมดเวลาการใช้งาน รวมถึงการปิดการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๑๕ นาที

๒) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. ทำการล้างหน้าจอ หลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๑๕ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

๓) กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. สำหรับระบบที่มีความเสี่ยงสูง จะต้องมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔) กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ดย. สำหรับระบบที่มีความสำคัญสูง จะต้องมีการตัดและหมดเวลาการใช้งาน โดยมีกำหนดให้ไม่เกิน ๑ ชั่วโมงต่อการพิสูจน์ตัวตนเข้าใช้งาน

๕) ต้องมีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศอีกครั้ง หลังจากที่ระบบได้หมดเวลาการใช้งานไปแล้ว

๘. แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น (Application) และสารสนเทศ

๘.๑ การจำกัดการเข้าถึงสารสนเทศ

ผู้ดูแลระบบต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชั่น (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยมีวิธีการปฏิบัติ ดังนี้

๑) ผู้ดูแลระบบต้องป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง โดยไม่ได้รับอนุญาต เช่น การใช้กุญแจล็อคที่ตัวเครื่อง การพิสูจน์ยืนยันตัวตน เป็นต้น

๒) ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบ โดยกำหนดขั้นตอนและแบบฟอร์มการใช้งานระบบคอมพิวเตอร์ ประกอบด้วยรายละเอียดอย่างน้อยดังนี้ ชื่อผู้ใช้บริการ เหตุผลในการขอใช้ ระยะเวลาในการใช้บริการ

๓) ผู้ดูแลระบบต้องจำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานในช่วงเวลาที่กำหนด

๔) เจ้าของข้อมูลหรือเจ้าของระบบต้องกำหนดรายการข้อมูลสำหรับการให้บริการ ประกอบด้วยรายละเอียดอย่างน้อยดังนี้ ประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง เป็นต้น

๕) เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ สำหรับข้อมูลสำคัญในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้บริการและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

(๕) ต้องเปลี่ยนรหัสผ่านของข้อมูลหรือระบบที่มีลำดับความสำคัญตามระยะเวลาที่กำหนด

๖) ต้องใช้เมนูเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชันต่าง ๆ ของระบบงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

๗) ต้องลงทะเบียนผู้ใช้งาน เพื่อควบคุม จำกัด หรือให้สิทธิ์การเข้าถึงข้อมูลและฟังก์ชันต่าง ๆ ของระบบงาน เช่น การให้สิทธิ์ในการอ่าน เขียน ลบ หรือสั่งให้โปรแกรมทำงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

๘) ต้องควบคุมหรือจำกัดสิทธิ์การเข้าถึงระบบงานซึ่งถูกเข้าถึงจากอีกระบบงานหนึ่ง โดยควบคุมให้สามารถเข้าถึงได้เฉพาะข้อมูลและฟังก์ชันต่าง ๆ ที่จำเป็นต้องใช้งานเท่านั้น

๙) ต้องควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงาน เพื่อให้สามารถเข้าถึงได้เฉพาะข้อมูลที่เกี่ยวข้องและจำเป็นสำหรับการนำไปใช้งานเท่านั้น

๑๐) ต้องแสดงเฉพาะข้อมูลพื้นฐาน เพื่อให้ผู้ใช้งานได้รับทราบข้อมูลที่จำเป็นเท่านั้น

๑๑) ต้องแสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่ล็อคอิน (Log in) เสร็จแล้ว

๑๒) ต้องมีข้อความแสดงเตือน ห้ามผู้ไม่มีสิทธิ์เข้าถึงระบบงาน

๑๓) ต้องมีข้อจำกัดไม่ให้ระบบแสดงความช่วยเหลือใด ๆ กรณีมีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นกับระบบ

๑๔) ต้องมีการตรวจสอบข้อมูลการล็อคอิน (Log in) หลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว

๑๕) ต้องมีข้อจำกัดไม่ให้ระบบแสดงข้อความผิดพลาดจากการทำงานหรือการใช้งานในลักษณะที่เปิดเผยข้อมูลภายในของระบบงาน

๑๖) ต้องมีการจำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลการล็อคอิน (Log in) ผิด

๑๗) ต้องมีการกำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบงานได้ ภายหลังจากที่ใส่ข้อมูลการล็อคอิน (Log in) ผิดเกินกว่าจำนวนครั้งที่กำหนด

๑๘) ต้องมีการส่งข้อความเตือนไปยังผู้ดูแลระบบให้ทราบว่ามีผู้ใช้งานพยายามล็อคอิน (Log in) แต่ผิดพลาดเป็นจำนวนหลายครั้ง

๑๙) ต้องมีการบันทึกข้อมูลการล็อคอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ

๒๐) ต้องมีการจำกัดช่วงระยะเวลาที่นานที่สุด ที่ผู้ใช้งานจะต้องล็อคอิน (Log in) เข้าใช้งานให้สำเร็จ

๒๑) ต้องมีการแสดงวันเวลาของการล็อคอิน (Log in) ครั้งที่แล้ว (ทั้งที่สำเร็จและไม่สำเร็จ)

๘.๒ <u>ระบบที่ไวต่อการรบกวน</u>

ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติในการดูแลและรักษาความมั่นคงปลอดภัยระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อ กย. โดยจำเป็นต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ รวมทั้งต้องควบคุมการเข้าถึงโดยการเข้าผ่านอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอก กย. โดยมีวิธีการปฏิบัติ ดังนี้

๑) ต้องระบุระดับความสำคัญของระบบงาน ซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อ กย.

๒) ต้องติดตั้งระบบงานที่มีความสำคัญสูงแยกไว้ในเครื่องคอมพิวเตอร์เครื่องหนึ่งต่างหาก

๓) ต้องประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่นๆ ที่มีความสำคัญน้อยกว่า เช่น ความเสี่ยงในการใช้เครื่องๆ เดียวกันในการให้บริการ

๔) ต้องควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

๕) ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอก กย. ที่เกี่ยวข้องกับระบบดังกล่าว

๖) ต้องทำการควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก ตามข้อกำหนดที่ตั้งค่าไว้ใน Firewall

๘.๓ <u>การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่</u>

ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติอย่างเป็นทางการ สำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา อาทิ เครื่องคอมพิวเตอร์โน้ตบุ๊ค รวมทั้งกำหนดมาตรการการใช้งานอย่างปลอดภัยและเหมาะสม โดยมีแนวทางปฏิบัติ ดังนี้

๑) ต้องวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา

๒) สร้างความตระหนักเพื่อให้ผู้ใช้งานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น การใช้งานในที่สาธารณะ ห้องประชุม นอกสถานที่ ซึ่งรวมถึงการเชื่อมต่อผ่านทางเครือข่ายสาธารณะภายนอก ดย. เป็นต้น

๓) ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์ฯ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการเข้ารหัสข้อมูล

๔) ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือลับในอุปกรณ์ฯ

๕) สำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์ฯ อย่างสม่ำเสมอ

๖) ต้องควบคุมการเข้าถึงระบบงานของ ดย. จากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์แบบพกพา ซึ่งเชื่อมต่อผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตสาธารณะ

๗) ต้องระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย สำหรับการเข้าถึงระบบงานของ ดย. จากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์แบบพกพา

๘) ต้องควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ ในอุปกรณ์คอมพิวเตอร์แบบพกพาของ ดย.

๙) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน เข้ามาปฏิบัติงานภายในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า - ออกพื้นที่ ให้ถูกต้องชัดเจน และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ด้วยการลงนามอย่างเป็นลายลักษณ์อักษร

๑๐) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน โดยมีการจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ผู้เกี่ยวข้องรับทราบโดยทั่วกัน เช่น พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless area) เป็นต้น

๘.๔ <u>การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)</u>

ผู้ดูแลระบบต้องกำหนดมาตรการควบคุมการปฏิบัติงานของผู้ปฏิบัติงานจากระยะไกล รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้มีความมั่นคงปลอดภัยเพียงพอ โดยมีแนวทางปฏิบัติ ดังนี้

๑) มีแผนและขั้นตอนการปฏิบัติงานสำหรับเจ้าหน้าที่ของ ดย. ที่จำเป็นต้องปฏิบัติงานของ ดย. จากภายนอกสำนักงานหรือจากระยะไกล

๒) ดย. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

๓) ผู้ใช้งานระบบจากระยะไกล ต้องได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบงานอย่างเป็นทางการ และต้องใช้งานตามระยะเวลาการเข้าถึงที่กำหนดไว้

๔) ผู้ใช้งานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

๕) มีข้อกำหนดเฉพาะสำหรับการปฏิบัติงานจากระยะไกล ดังนี้

- ชนิดของงานที่อนุญาตและไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล
- ระบบงานหรือบริการต่าง ๆ ที่อนุญาตให้เข้าถึงได้จากระยะไกล
- ชั่วโมงหรือช่วงระยะเวลาการปฏิบัติงาน
- ชั้นความลับของข้อมูลที่อนุญาตให้เข้าถึงได้

๖) ต้องควบคุมทางกายภาพที่จำเป็นสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

๗) ต้องป้องกันข้อมูลสำหรับการสื่อสารระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลกับระบบงานต่าง ๆ ภายใน ดย.

๘) ต้องกำหนดระดับความสำคัญของข้อมูลที่จะมีการรับส่งหรือสื่อสารกันระหว่าง ดย. กับสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

๙) ไม่อนุญาตให้ครอบครัวหรือเพื่อนของผู้ปฏิบัติงานจากระยะไกล เข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลของ ดย.

๑๐) ต้องควบคุมสำหรับการใช้งานเครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ ดย. จากระยะไกล รวมทั้งมาตรการควบคุมการใช้บริการเครือข่ายไร้สายจากที่บ้าน ทั้งนี้เพื่อป้องกันการเข้าถึงระบบหรือข้อมูลของ ดย. โดยไม่ได้รับอนุญาต

๑๑) ต้องป้องกันทรัพย์สินทางปัญญาที่เกิดขึ้นจากการปฏิบัติงานจากระยะไกล เพื่อป้องกันการโต้แย้งกันว่าใครเป็นเจ้าของทรัพย์สินทางปัญญานั้น

๑๒) ต้องสงวนสิทธิ์ในการเข้าถึงอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ ดย. จากระยะไกล เช่น เพื่อทำการตรวจสอบโปรแกรมไม่พึงประสงค์ในอุปกรณ์นั้น เพื่อทำการตรวจสอบข้อมูลในอุปกรณ์สำหรับการดำเนินการสอบสวนกรณีที่มีเหตุเกิดขึ้น

๑๓) ต้องตรวจสอบว่าซอฟต์แวร์ที่ใช้งานบนอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ ดย. จากระยะไกล มีใบอนุญาตการใช้งานที่ถูกต้องและครบถ้วน

๑๔) ต้องติดตั้งซอฟต์แวร์พื้นฐานที่จำเป็น เช่น ซอฟต์แวร์ป้องกันไวรัส ไฟร์วอลล์ ในอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ ดย. จากระยะไกล

๑๕) ต้องจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการปฏิบัติงานจากระยะไกล ซึ่งรวมถึงอุปกรณ์สำหรับการจัดเก็บข้อมูล และอุปกรณ์สื่อสาร

๑๖) ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ ดย. จากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดย ดย.

๑๗) ต้องบำรุงรักษาและให้บริการสนับสนุนสำหรับซอฟต์แวร์และฮาร์ดแวร์ต่าง ๆ ที่ใช้งานจากระยะไกล

๑๘) ต้องสำรองข้อมูลสำหรับการปฏิบัติงานจากระยะไกล

๑๙) ต้องตรวจสอบความมั่นคงปลอดภัยของสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

๙. แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

๙.๑ วิธีการบริหารจัดการการเข้าถึงของผู้ใช้งาน มีวิธีการปฏิบัติ ดังนี้

๑) ดย. ต้องกำหนดขั้นตอนปฏิบัติของการลงทะเบียนเจ้าหน้าที่ใหม่อย่างเป็นทางการตามความจำเป็น โดยผู้ใช้งานเป็นผู้ร้องขอเพื่อเข้าใช้ระบบงาน ซึ่งมีผู้บังคับบัญชาเป็นผู้ให้การรับรอง และผู้ดูแลระบบเป็นผู้บริหารจัดการบัญชีผู้ใช้งาน

๒) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออก ต้องทำภายใน ๒๔ ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานภายใน ต้องทำภายใน ๗ วัน

๓) กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๔) ผู้ใช้ต้องลงนามรับทราบสิทธิ์ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด รวมทั้งเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

๙.๒ วิธีการบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน มีวิธีการปฏิบัติ ดังนี้

๑) ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ

๒) ต้องกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน

๓) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

(๑) ต้องได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้น ๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ

(๒) ต้องควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

(๓) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

(๔) ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๙.๓ วิธีการบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย มีวิธีการปฏิบัติ ดังนี้

๑) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์ เข้าด้วยกัน)

๒) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๓) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๔) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ครอบครองอยู่

๕) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๖) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ ให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้ต้องเป็นไปอย่างปลอดภัย

๙.๔ วิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ มีวิธีการปฏิบัติ ดังนี้

๑) การจัดแบ่งประเภทของข้อมูล ประกอบด้วย

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลคำรับรอง ข้อมูลงบประมาณการเงินและบัญชี และข้อมูลระบบบริหารราชการ (Back Office)
- ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลผู้รับบริการทางสังคม

๒) การจัดแบ่งระดับความสำคัญของข้อมูลแต่ละประเภทข้างต้น ดังนี้

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๓) การจัดแบ่งลำดับชั้นความลับของข้อมูลแต่ละประเภทข้างต้น ดังนี้

- ลับที่สุด
- ลับมาก
- ลับ

๔) การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภทข้างต้น ดังนี้

- สามารถเข้าถึงได้เฉพาะผู้มีสิทธิ์สูงสุดในการบริหารจัดการระบบสารสนเทศ
- สามารถเข้าถึงได้เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิ์จากเจ้าของระบบงานแล้วเท่านั้น
- สามารถเข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง
- สามารถเข้าถึงได้โดยทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว

๕) การกำหนดเวลาการเข้าถึง ดังนี้

- การเข้าถึงสารสนเทศในเวลาราชการ (๐๘.๐๐ – ๑๗.๐๐ น.)
- การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา ๐๘.๐๐ – ๑๗.๐๐ น.)
- การเข้าถึงในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)
- การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงการเข้าถึงและจำนวนระยะเวลาการเข้าถึง)

๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึงได้ ดังนี้

- ระบบแลน (LAN) ในลักษณะ Client Server
- ระบบอินทราเน็ต (Intranet) ในลักษณะ Web Base Application
- ระบบอินเทอร์เน็ต (Internet) ในลักษณะ Web Base Application
- ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

ตารางสรุปแนวปฏิบัติในการเข้าถึงข้อมูลสารสนเทศของ ดย. มีรายละเอียด ดังนี้

เวลาการเข้าถึง	ประเภทข้อมูลสารสนเทศ	ระดับความสำคัญ	ระดับชั้นความลับ	ระดับชั้นการเข้าถึง	ช่องทาง
การเข้าถึงสารสนเทศในเวลาราชการ (๐๘.๐๐ – ๑๗.๐๐ น.)	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด - ปานกลาง - น้อย	-	- เฉพาะกลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว	ระบบอินเทอร์เน็ต (Internet) - ระบบแลน (LAN) - ระบบอินทราเน็ต (Intranet) - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา ๐๘.๐๐ – ๑๗.๐๐ น.)	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด - ปานกลาง - น้อย	-	- เฉพาะกลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว	- ระบบอินเทอร์เน็ต (Internet) - ระบบอินทราเน็ต (Intranet) - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
การเข้าถึงในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)	- ด้านการบริหาร - ด้านการให้บริการ	- ปานกลาง - น้อย	-	- เฉพาะกลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว	- ระบบอินเทอร์เน็ต (Internet) - ระบบอินทราเน็ต (Intranet) - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงการเข้าถึงและจำนวนระยะเวลาการเข้าถึง)	- ด้านการบริหาร - ด้านการให้บริการ	มากที่สุด	ลับที่สุด	- เฉพาะผู้มีสิทธิ์สูงสุดในการบริหารจัดการระบบสารสนเทศ - เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิ์จากเจ้าของระบบงานแล้วเท่านั้น	- ระบบอินทราเน็ต (Intranet) - ระบบอินเทอร์เน็ต (Internet) - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

๑๐. แนวปฏิบัติในการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอกหรือ Outsource มีวิธีการปฏิบัติ ดังนี้

๑. หน่วยงานภายนอกจะต้องแจ้งรายชื่อผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศล่วงหน้า มายัง ดย. ก่อนการดำเนินงาน ในกรณีที่มีการเปลี่ยนแปลงรายชื่อหน่วยงานภายนอกจะต้องแจ้งล่วงหน้าก่อนทุกครั้ง

๒. ในการเข้าไปปฏิบัติงานภายในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) หน่วยงานภายนอกจะต้องบันทึกรายละเอียดตามเอกสารที่ทาง ดย. จัดไว้ให้

๓. ทุกครั้งที่จะทำการแก้ไขค่า Config ของอุปกรณ์ทุกชนิดภายในห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) หน่วยงานภายนอกจะต้องทำการสำรองค่า Config เดิมไว้ก่อน รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไขทุกครั้ง หากการแก้ไขมีปัญหาเกิดขึ้น ไม่สามารถใช้งานได้ตามต้องการ จะต้องทำการเรียกข้อมูลที่ได้ทำการสำรองไว้กลับมา ให้สามารถใช้งานได้ตามสภาพเดิม

๔. ทุกครั้งที่มีการแก้ไขหรือเปลี่ยนแปลงค่า Config ระบบงานสารสนเทศหรือเปลี่ยนแปลงโครงสร้างฐานข้อมูล หน่วยงานภายนอกจะต้องทำการสำรองโปรแกรม/โมดูล หรือฐานข้อมูลเดิมที่มีการแก้ไข รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไขทุกครั้ง หากการแก้ไขมีปัญหาเกิดขึ้น ไม่สามารถใช้งานได้ตามต้องการ จะต้องทำการเรียกข้อมูลที่ได้ทำการสำรองไว้กลับมา ให้สามารถใช้งานได้ตามสภาพเดิม

๕. ในกรณีที่หน่วยงานภายนอกจะเข้ามาปฏิบัติงานที่ห้องปฏิบัติการคอมพิวเตอร์แม่ข่าย (Server Room) ในวันหยุดหรือนอกเวลาราชการ จะต้องขอความเห็นชอบจากผู้รับผิดชอบหรือผู้ดูแลระบบของ ดย. ล่วงหน้าก่อนทุกครั้ง และการดำเนินงานทุกครั้งจะต้องอยู่ในความดูแลของผู้รับผิดชอบหรือผู้ดูแลระบบของ ดย.

๖. หากหน่วยงานภายนอกจะทำการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายคอมพิวเตอร์ของ ดย. จะต้องแจ้งให้ผู้รับผิดชอบหรือผู้ดูแลระบบของ ดย. ทราบล่วงหน้าก่อนทุกครั้ง ซึ่งจะต้องระบุวัน เวลา ระยะเวลาในการทำงานให้ชัดเจน

๗. ในกรณีที่เจ้าหน้าที่ของหน่วยงานภายนอกประมาท ทำให้อุปกรณ์และระบบสารสนเทศของ ดย. ได้รับความเสียหายหรือสูญหาย หน่วยงานภายนอกนั้น จะต้องรับผิดชอบในการซ่อมแซมแก้ไขหรือเปลี่ยนใหม่ให้อยู่ในสภาพที่สามารถใช้งานได้ดังเดิม

๘. ในกรณีที่หน่วยงานภายนอกมีความจำเป็นต้องสำเนาฐานข้อมูลทุกประเภทออกจาก ดย. จะต้องทำหนังสือขอความเห็นชอบจาก ดย. ล่วงหน้าก่อนทุกครั้ง โดยจะต้องระบุเหตุผลในการนำไปใช้งานอย่างชัดเจน และต้องรับผิดชอบความเสียหายที่อาจเกิดขึ้นด้วย

๙. หน่วยงานภายนอกจะต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ดย. ที่กำหนดไว้ไม่มีข้อยกเว้น หากมีการฝ่าฝืน ดย. จะทำหนังสือแจ้งไปยังหน่วยงานภายนอกนั้น และจะไม่อนุญาตให้เจ้าหน้าที่ของหน่วยงานภายนอกนั้น เข้ามาดำเนินการใด ๆ ภายใน ดย.

๑๑. แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

๑๑.๑ การใช้ Internet Account หรือรหัสผ่านในการใช้งานอินเทอร์เน็ต มีวิธีการปฏิบัติ ดังนี้

๑) ผู้ใช้งานต้องลงทะเบียนเพื่อขอใช้งานอินเทอร์เน็ตจากผู้ดูแลระบบก่อน โดยต้องยอมรับและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ดย. อย่างเคร่งครัด

๒) ผู้ใช้งานที่ได้รับอนุญาตให้ใช้งานอินเทอร์เน็ตได้ จะได้รับ Account ซึ่งประกอบด้วย รหัสผู้ใช้งาน และรหัสผ่าน (Password) เพื่อเข้าใช้งานอินเทอร์เน็ต

๓) ผู้ใช้งานต้องไม่ใช้ Account ของผู้อื่นโดยไม่ได้รับความยินยอม ในการเข้าใช้งานอินเทอร์เน็ตของ ดย. โดยจะต้องใช้ Account ที่เป็นของตนเองในการแสดงตนเข้าใช้งานอินเทอร์เน็ตตามสิทธิ์ที่ได้รับเท่านั้น

๔) ในกรณีที่มีความจำเป็นต้องให้สิทธิ์บุคคลอื่นในการใช้งานอินเทอร์เน็ต ให้ทำการบันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และเปลี่ยน Password ใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

๕) ผู้ใช้งานต้องเป็นผู้รับผิดชอบ Account ที่ ดย. จัดสรรให้ ดังนั้น ผู้ใช้งาน (ผู้อนุญาตและผู้ได้รับอนุญาต) ต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันจะเกิดขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากการใช้งาน Account ของผู้ใช้งานนั้น ๆ ร่วมกัน เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น

๖) ผู้ใช้งานควรทำการเปลี่ยน Password ใหม่ทันที หากถูกเปิดเผยหรือสงสัยว่าถูกผู้อื่นนำ Password ไปใช้ โดย Password ที่ตั้ง ควรจะประกอบด้วย ตัวหนังสือ ตัวเลข และอักขระพิเศษ เพื่อให้ยากต่อการคาดเดา

๗) ผู้ใช้งานต้องเปลี่ยน Password ทุก ๆ ๖ เดือน หรือตามที่ผู้ดูแลระบบกำหนด

๘) ผู้ใช้งานต้องทำการ Logout ออกจากคอมพิวเตอร์ทันทีเมื่อเลิกใช้งาน หรือเมื่อไม่อยู่ที่หน้าจอคอมพิวเตอร์นานเกิน ๑๕ นาที

๙) ผู้ดูแลระบบมีสิทธิ์ระงับการใช้ Account หากผู้ใช้งานไม่มีการใช้งานเป็นเวลา ๓๐ วัน และถ้าไม่มีการติดต่อขอใช้งานเป็นเวลา ๙๐ วันนับจากวันที่ระงับการใช้งาน ผู้ดูแลระบบจะยกเลิก Account ดังกล่าวทันที

๑๑.๒ การใช้งานอินเทอร์เน็ต มีวิธีการปฏิบัติ ดังนี้

๑) การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเทอร์เน็ต ควรเชื่อมต่อผ่านระบบรักษาความมั่นคงปลอดภัยที่ ดย. จัดสรรไว้เท่านั้น

๒) ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ ดย. ในการเผยแพร่หรือใช้งานโดยมีวัตถุประสงค์ดังต่อไปนี้

(๑) เพื่อก่อให้เกิดความเสียหายแก่ ดย. และบุคคลอื่น หรือละเมิดสิทธิ์ หรือสร้างความรำคาญต่อผู้อื่น เช่น การตัดต่อภาพของผู้อื่นแล้วนำมาเผยแพร่ทำให้เกิดความอับอาย ลักลอบแก้ไขข้อมูลส่วนบุคคลของผู้อื่น การแสดงความเห็นดูหมิ่นผู้อื่นบนเว็บไซต์ เป็นต้น

(๒) เพื่อหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือการพาณิชย์ เช่น การจำลอง Mail Server โดยมีการใช้อินเทอร์เน็ตของ ดย. ในการส่ง mail จำนวนมาก การจำลอง Web Server เพื่อจัดทำเว็บไซต์สำหรับค้าขายโดยมีการใช้อินเทอร์เน็ตของ ดย. เป็นต้น

(๓) เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การเข้าสู่เว็บไซต์ที่ไม่เหมาะสม การใช้ข้อความที่สร้างความตื่นตระหนกกับสังคมโดยรวมบนเว็บบอร์ด เป็นต้น

(๔) เพื่อการเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาต ซึ่งได้มาจาก ดย. หรือผู้ที่มีสิทธิ์ในข้อมูลดังกล่าว

๓) ผู้ใช้งานไม่ควรดาวน์โหลดหรือใช้งานข้อมูลมัลติมีเดีย ที่มีลักษณะการยึดครองช่องสัญญาณการสื่อสารข้อมูลตลอดเวลา (Consume Bandwidth) ผ่านอินเทอร์เน็ตในเวลาราชการ เช่น เล่นเกม/ดูหนัง/ฟังเพลงออนไลน์ ดูคลิปวิดีโอผ่านเว็บไซต์ ดาวน์โหลดซอฟต์แวร์ที่มีขนาดใหญ่ผ่านเว็บไซต์ เป็นต้น ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องส่งข้อมูลที่มีขนาดใหญ่ ให้ติดต่อผู้ดูแลระบบดำเนินการเท่านั้น

๔) ผู้ใช้งานที่มีความจำเป็นต้องนำเครื่องคอมพิวเตอร์โน้ตบุ๊กไปเชื่อมต่อเข้ากับอินเทอร์เน็ตนอกเหนือเครือข่ายอินเทอร์เน็ตของ ดย. ต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่มีการ Update ไวรัส ให้มีความทันสมัยตลอดเวลา

๕) ผู้ใช้งานควรแจ้งข้อเท็จจริงต่อผู้ดูแลระบบ หากพบเห็นการใช้อินเทอร์เน็ตในเครือข่ายของ ดย. ไปในทางที่ไม่เหมาะสม หรือพบเห็นการบุกรุกหรือการละเมิดสิทธิ์ของ ดย.

๖) ผู้ใช้งานไม่ควรดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือหรือไม่มั่นใจว่าปลอดภัย เช่น Freeware โปรแกรมรักษาจอภาพ เกมส์ และโปรแกรมที่ลงท้ายด้วย exe หรือ com หากมีความจำเป็นต้องดาวน์โหลด ต้องมีการตรวจสอบด้วยโปรแกรมป้องกันไวรัสก่อนการนำไปใช้ทุกครั้ง

๑๒. แนวปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์

๑๒.๑ การรับ - ส่งจดหมายอิเล็กทรอนิกส์ มีวิธีการปฏิบัติ ดังนี้

๑) ผู้ใช้งานต้องลงทะเบียนเพื่อขอใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) จากผู้ดูแลระบบก่อน

๒) ผู้ใช้งานที่ได้รับอนุญาตให้ใช้งาน E-mail ได้ จะได้รับ Account ซึ่งประกอบด้วย รหัสผู้ใช้งาน และรหัสผ่าน (Password) เพื่อเข้าใช้งาน E-mail

๓) ห้ามผู้ใช้งานใช้ E-mail ที่ ดย. จัดสรรให้ ในการรับ - ส่ง หรือใช้งาน E-mail โดยมีวัตถุประสงค์ดังต่อไปนี้

(๑) เพื่อก่อให้เกิดความเสียหายแก่ ดย. และบุคคลอื่น หรือละเมิดสิทธิ์ หรือสร้างความรำคาญต่อผู้อื่น เช่น การจงใจส่งข้อมูลที่มีไวรัสให้กับผู้อื่น การส่งข้อความดูหมิ่นผู้อื่น การส่งจดหมายลูกโซ่ การส่ง Spam mail เป็นต้น

(๒) เพื่อใช้ประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือการพาณิชย์

(๓) เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การส่งภาพลามกให้กับผู้อื่น เป็นต้น

(๔) เพื่อการเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาต ซึ่งได้มาจาก ดย. หรือผู้ที่มีสิทธิ์ในข้อมูลดังกล่าว

๔) หากผู้ใช้งานต้องการส่ง E-mail ถึงเจ้าหน้าที่ทุกคนใน ดย. หรือกลุ่มของหน่วยงาน ควรแจ้งให้ผู้ดูแลระบบทราบ

๕) ผู้ใช้งานไม่ควรนำ E-mail ที่ ดย. จัดสรรให้ ไปให้ผู้อื่นใช้งาน และ ดย. จะไม่รับผิดชอบผลเสียหายต่าง ๆ อันจะเกิดขึ้นจากการยินยอมให้ผู้อื่นใช้ E-mail นั้น ยกเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น

๖) ห้ามผู้ใช้งานนำ E-mail ไปใช้งานบนเว็บไซต์ซึ่งเสี่ยงต่อการเกิด Spam mail เช่น การนำ E-mail ไปลงทะเบียนเพื่อสมัครงานบนเว็บไซต์สมัครงาน การระบุ E-mail เพื่อแสดงความคิดเห็นบนเว็บไซต์ขายสินค้า เป็นต้น

๗) ผู้ใช้งานไม่ควรเปิดหรือส่งต่อ E-mail ที่ไม่ทราบแหล่งที่มาหรือไม่น่าเชื่อถือ เช่น E-mail โฆษณาขายสินค้า E-mail ให้สินเชื่อ E-mail เสนอให้รางวัล E-mail หาคู่ เป็นต้น

๘) ผู้ใช้งานต้องตรวจสอบไวรัสกับไฟล์ที่แนบมาพร้อม E-mail ทุกครั้งเสมอ ถึงแม้ว่าจะมาจากผู้ส่งที่รู้จัก

๑๓. แนวปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศ

๑๓.๑ การสำรองข้อมูลและระบบคอมพิวเตอร์

ผู้ดูแลระบบหรือคณะทำงานที่เกี่ยวข้อง จะต้องระบุแนวปฏิบัติสำหรับการจัดทำระบบสำรองข้อมูลที่ชัดเจน เพื่อให้ระบบสารสนเทศอยู่ในสภาพพร้อมใช้อยู่เสมอ โดยมีวิธีการปฏิบัติ ดังนี้

๑) กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ซึ่งดูแลรับผิดชอบระบบสารสนเทศ และระบบสำรองข้อมูลของ ดย.

๒) ผู้ดูแลระบบต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการจัดทำระบบสำรองข้อมูลและสารสนเทศของ ดย.

๓) ทำการพิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นต้องจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้ตามลำดับความสำคัญ

๔) ระบบที่จะทำการสำรองข้อมูลต้องเป็นระบบที่มีความสำคัญต่อภารกิจของ ดย.

๕) มีการกำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ และความถี่ในการสำรอง

๖) จัดทำแผนการสำรองที่เหมาะสมกับความสำคัญของแต่ละระบบสารสนเทศ

๗) ดำเนินการตามกระบวนการสำรองข้อมูล สำหรับแต่ละระบบสารสนเทศโดยเคร่งครัด

๘) ต้องป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูล

๙) การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก

๑๐) มีขั้นตอนปฏิบัติในการสำรองข้อมูลและกู้คืนข้อมูล แยกตามระบบสารสนเทศแต่ละระบบอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

๑๑) การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๑๒) ให้มีการมอบหมายเจ้าหน้าที่สำรอง เพื่อทำหน้าที่สำรองข้อมูลในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

๑๓) ในกรณีที่พบปัญหาในการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหา และรายงานต่อผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยีทราบ

๑๔) ให้ผู้ดูแลระบบ กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๑๕) ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูล (Encrypted Backup) ในการสำรองข้อมูลที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๑๖) ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ (Backup Procedure) ตามนโยบายที่เกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) โดยเคร่งครัด

๑๓.๒ การปฏิบัติเกี่ยวกับการสำรองข้อมูล มีวิธีการปฏิบัติ ดังนี้

๑) ผู้ดูแลระบบต้องทำการสำรองข้อมูลแต่ละรายการ โดยจะใช้วิธีสำรองข้อมูลแบบ Full Backup ตามความถี่ ดังนี้

(๑) **Web servers** : สำรองข้อมูลเผยแพร่บนเว็บไซต์ ๑ ครั้งต่อเดือน

(๒) **Database servers** : สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ ๑ ครั้งต่อสัปดาห์

(๓) **Firewall server** : สำรองข้อมูล Rule ของ Firewall ๑ ครั้งต่อเดือน

(๔) **Server อื่น ๆ** : สำรองข้อมูลบนเซิร์ฟเวอร์อื่น ๆ เช่น ระบบงานต่าง ๆ ๑ ครั้งต่อเดือน

๒) ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่า การสำรองข้อมูลตามรายละเอียดข้างต้นนั้น ถูกต้อง สมบูรณ์หรือไม่

๑๓.๓ <u>การทดสอบและการกู้คืนระบบ</u>

ดย. ต้องกำหนดแผนการทดสอบกู้คืนข้อมูล ตามชนิดของการสำรองข้อมูลที่กำหนดไว้แล้ว เพื่อให้ระบบสารสนเทศมีสภาพพร้อมใช้งานอยู่เสมอ โดยมีวิธีการปฏิบัติ ดังนี้

๑) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย จนเป็นเหตุทำให้ต้องกู้คืนระบบ ผู้ดูแลระบบจะต้องดำเนินการแก้ไข พร้อมทั้งรายงานผลการแก้ไข บันทึก และสรุปผลการปฏิบัติงานต่อผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยีหรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยีทราบ

๒) การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

๓) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้ระบบทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๔) กำหนดให้มีการทดสอบและปรับปรุงแผนการกู้คืนระบบ อย่างน้อยปีละ ๑ ครั้ง

๑๓.๔ <u>การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน</u>

ดย. ต้องเตรียมการสำหรับจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ โดยมีวิธีการปฏิบัติ ดังนี้

๑) กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ซึ่งดูแลรับผิดชอบการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒) ผู้ดูแลระบบจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินของระบบเทคโนโลยีสารสนเทศ เพื่อรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ

๓) ผู้ดูแลระบบต้องทดสอบ/ประเมิน และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้ หากเกิดเหตุการณ์ขึ้นจริง

๔) ผู้ดูแลระบบต้องบันทึกเหตุการณ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้น โดยพิจารณาถึง ประเภท ปริมาณ และหลักฐานสำหรับอ้างอิง เพื่อใช้ในกรณีที่เหตุการณ์มีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย

๕) รายละเอียดที่ปรากฏในแผนเตรียมความพร้อมกรณีฉุกเฉิน ควรมีสาระครอบคลุมภัยพิบัติหรือสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบสารสนเทศของ ดย. โดยมีหัวข้อสำคัญ ดังนี้

- การเตรียมการเบื้องต้น
- ผู้รับผิดชอบ
- มาตรการความปลอดภัยและแผนดำเนินงาน ในการนำระบบคอมพิวเตอร์กลับสู่สภาพปกติเมื่อเกิดความเสียหายหรือหยุดทำงาน

กรมกิจการเด็กและเยาวชน
Department of Children and Youth