กรมวิทยาศาสตร์การแพทย์
Department of Medical Sciences

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของกรมวิทยาศาสตร์การแพทย์

จัดทำโดย
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
พฤษภาคม 2568

คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีวัตถุประสงค์เพื่อให้การดำเนินกิจกรรมหรือการให้บริการของภาครัฐ มีความมั่นคงปลอดภัยและน่าเชื่อถือ กรมวิทยาศาสตร์การแพทย์จึงกำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น โดยอ้างอิงมาตรฐานสากล ISO/IEC 27001:2022 INFORMATION SECURITY MANAGEMENT ซึ่งมุ่งเน้นให้ระบบสารสนเทศสามารถให้บริการได้อย่างต่อเนื่อง ข้อมูลของหน่วยงานมีความถูกต้องพร้อมใช้และได้รับการป้องกันภัยคุกคามในรูปแบบต่าง ๆ อย่างเหมาะสม

การประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในครั้งนี้ จะช่วยลดผลกระทบจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศของกรมฯ ถูกบุกรุกหรือถูกโจมตี รวมไปถึงเมื่อเกิดการบุกรุกหรือโจมตีแล้ว จะต้องฟื้นฟูระบบกลับมาได้อย่างรวดเร็ว

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หวังเป็นอย่างยิ่งว่าบุคลากรของกรมวิทยาศาสตร์การแพทย์ จะสามารถนำไปปฏิบัติตามได้อย่างถูกต้อง เหมาะสม มีประสิทธิภาพและประสิทธิผล ส่งผลให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของกรมวิทยาศาสตร์การแพทย์มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมวิทยาศาสตร์การแพทย์
พฤษภาคม 2568

สารบัญ

สารจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม
(Department Chief Information Officer : DCIO)

นายแพทย์พิเชฐ บัญญัติ รองอธิบดีกรมวิทยาศาสตร์การแพทย์ ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) มอบแนวทางการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปี 2568 ดังนี้

กรมวิทยาศาสตร์การแพทย์ มุ่งเน้นการดำเนินงานด้านเทคโนโลยีสารสนเทศ ตามแนวคิด ***"เชื่อม แชร์ โชว์ ใช้ ชอบ"*** ภายใต้หลักการ **"ONESYSTEM MULTIPLE PROGRAMS"** รวมไปถึงดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศที่ส่งผลกระทบต่อความมั่นคงของรัฐและมุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคลของผู้ปฏิบัติงานและผู้รับบริการของกรมฯ ซึ่งต้องดำเนินการให้สอดคล้องตามพระราชบัญญัติดังกล่าวข้างต้น โดยกรมแจ้งวัตถุประสงค์ของการจัดเก็บ รวบรวม การใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไว้อย่างชัดเจนที่เว็บไซต์ของส่วนราชการ เพื่อให้เจ้าของข้อมูลรับทราบและมั่นใจในการให้ข้อมูลส่วนบุคคลกับกรม ที่สำคัญยิ่งอีกสิ่งหนึ่งคือการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามมาตฐาน ISO/IEC 27001 ที่กรมผ่านการรับรองมาตั้งแต่ปี 2565 และต้องธำรงรักษาไว้อย่างต่อเนื่องตลอดไป โดยกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศเพื่อเป็นแนวทางในการปฏิบัติงาน ดังนี้

1. การจัดซื้อ จัดหา และใช้โปรแกรมคอมพิวเตอร์ ต้องเป็นโปรแกรมที่ได้มาโดยชอบด้วยกฎหมายและขอให้พิจารณาติดตั้งโปรแกรมต่างๆ ลงในคอมพิวเตอร์ตามความจำเป็นในการใช้งานอย่างเหมาะสม
2. บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Risk Management) เพื่อลดผลกระทบต่อข้อมูล อันเนื่องมาจากภัยคุกคามทั้งภายในและภายนอก รวมถึงภัยพิบัติต่างๆ
3. ควบคุมการเข้า-ออก พื้นที่จัดวางอุปกรณ์ด้านเทคโนโลยีสารสนเทศ รวมไปถึงป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม
4. แบ่งแยกโซนระบบเครือข่ายคอมพิวเตอร์สำหรับภายในและภายนอกองค์กรอย่างชัดเจน
5. การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภายในและภายนอก การพัฒนาระบบสารสนเทศของหน่วยงานต้องคำนึงถึงความปลอดภัยของข้อมูลเป็นสิ่งสำคัญ
6. ควบคุมการปฏิบัติงานของผู้รับจ้างภายนอกตลอดเวลาการเข้ามาปฏิบัติงาน และให้มีการทำข้อตกลงประมวลผลข้อมูลส่วนบุคคล
7. กำหนดให้มีการลงนามรักษาความลับสำหรับผู้รับผิดชอบด้านข้อมูลสารสนเทศ
8. ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์การแพทย์อย่างเคร่งครัด และปฏิบัติตามกฎหมายที่เกี่ยวข้อง

(นายพิเชฐ บัญญัติ)
รองอธิบดีกรมวิทยาศาสตร์การแพทย์
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม
8 พฤษภาคม 2568

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมวิทยาศาสตร์การแพทย์

กรมวิทยาศาสตร์การแพทย์กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์การแพทย์สามารถให้บริการได้อย่างต่อเนื่องและมีความมั่นคงปลอดภัยเป็นไปตามมาตรฐาน ISO/IEC 27001:2022 รวมถึงป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง หรือจากภัยคุกคามในรูปแบบต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สินของหน่วยงานได้

คำนิยาม

“กรม” หมายถึง กรมวิทยาศาสตร์การแพทย์

“หน่วยงาน” หมายถึง สำนัก สถาบัน ศูนย์ กอง และหน่วยงานที่มีฐานะเทียบเท่า กอง รวมถึงศูนย์วิทยาศาสตร์การแพทย์ ที่อยู่ในสังกัดกรมวิทยาศาสตร์การแพทย์

“ผู้ใช้งาน” หมายถึง ข้าราชการ ลูกจ้าง พนักงานราชการ และพนักงานกระทรวงสาธารณสุข ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายและระบบสารสนเทศของหน่วยงาน

“ผู้บริหารระดับสูง” หมายถึง อธิบดี รองอธิบดี หรือเทียบเท่า

“**หัวหน้าหน่วยงาน**” หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ ผู้อำนวยการสำนัก/สถาบัน/ศูนย์/กอง/หน่วยงานที่มีฐานะเทียบเท่ากอง และศูนย์วิทยาศาสตร์การแพทย์

“**ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม**” (Department Chief Information Officer: DCIO) หมายถึง ผู้บริหารระดับสูง ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบบริหารจัดการด้านระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์การแพทย์

“ผู้บริหารเทคโนโลยีสารสนเทศระดับกอง” (Division Information Officer: DIO) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานให้มีหน้าที่รับผิดชอบบริหารจัดการด้านระบบเทคโนโลยีสารสนเทศ ของสำนัก/สถาบัน/ศูนย์/กอง/หน่วยงานที่มีฐานะเทียบเท่ากอง และศูนย์วิทยาศาสตร์การแพทย์

“**ผู้ดูแลระบบ**” (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“เจ้าของข้อมูล”หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“**สิทธิของผู้ใช้งาน**” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์

“**สินทรัพย์**” หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย อาทิเช่น โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN) เป็นต้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” (information security event) หมายถึง การเกิดเหตุการณ์สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“จดหมายอิเล็กทรอนิกส์” (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

“รหัสผ่าน” (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“ชุดคำสั่งไม่พึงประสงค์” หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

หมวดที่ 1

นโยบายและมาตรการควบคุมขององค์กร (Organizational controls)

วัตถุประสงค์

1. เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจของหน่วยงานของรัฐ

3. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่งคงปลอดภัย

4. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ส่วนที่ 1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

แนวปฏิบัติ

ข้อ 1. ระดับนโยบาย ได้แก่

- ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO)
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)
- ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง ประจำกรม (CISO)
- ผู้อำนวยการสถาบัน/กอง/สำนัก/ศูนย์ หรือเทียบเท่า ระดับผู้อำนวยการ

ความรับผิดชอบ

(1) กำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

(2) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(3) กรณีระบบคอมพิวเตอร์หรือ ข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อ ความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น”

(อ้างอิง: ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556)

ข้อ 2. ระดับบริหาร ได้แก่

- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ/หัวหน้ากลุ่ม/ฝ่าย/งาน หรือเทียบเท่าหัวหน้ากลุ่ม/ฝ่าย/งาน

- หัวหน้ากลุ่ม/ฝ่าย/งาน หรือเทียบเท่าหัวหน้ากลุ่ม/ฝ่าย/งาน ของสถาบัน/กอง/สำนัก/ศูนย์ หรือเทียบเท่า

ความรับผิดชอบ

(1) กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(2) ควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

ข้อ 3. ระดับปฏิบัติ ได้แก่

- ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการกรมเช่น ผู้บริหารเทคโนโลยีสารสนเทศระดับกอง (DIO)
- นักวิชาการคอมพิวเตอร์ ผู้ดูแลระบบคอมพิวเตอร์ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
    - ผู้ดูแลระบบฐานข้อมูล (Database Administrator)
    - ผู้ดูแลระบบ (System Administrator)
    - ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์(Network Admin)
- นักวิชาการคอมพิวเตอร์ ผู้ดูแลระบบคอมพิวเตอร์ ของของสถาบัน/กอง/สำนัก/ศูนย์ หรือเทียบเท่า

ความรับผิดชอบ

(1) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม

(2) ประสานการปฏิบัติงานแผนบริหารความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศของกรม

(3) ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(4) สำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(5) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(6) รักษาความปลอดภัยระบบอินเตอร์เน็ต

(7) ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม

ส่วนที่ 2 ข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย (Threat intelligence)

ข้อ 1. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการจัดทำแนวทางเฝ้าระวังภัยคุกคามทางไซเบอร์ กำหนดทีมงานและหน้าที่ในการการเฝ้าระวังภัยคุกคามทางไซเบอร์ ช่องทางการรับข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัยทางไซเบอร์

ข้อ 2. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สื่อสารข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัยทางไซเบอร์ไปยังกลุ่มผู้บริหารเทคโนโลยีสารสนเทศระดับกอง (DIO) เพื่อสื่อสารและร่วมดำเนินการป้องกันภัยคุกคามทางไซเบอร์

ข้อ 3. กรณีเกิดเหตุภัยคุกคามทางไซเบอร์ ให้ผู้พบเหตุแจ้งข้อมูลผ่านทางผู้บริหารเทคโนโลยีสารสนเทศระดับกอง (DIO) หรือ กลุ่มพัฒนาระบบความมั่นคงปลอดภัย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารโดยตรง

ส่วนที่ 3 การบริหารจัดการสินทรัพย์ (Assets Management)

การควบคุมทรัพย์สินสารสนเทศ ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล และแฟ้มข้อมูล เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงระบบสารสนเทศและข้อมูลสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ มีแนวทางปฏิบัติ ดังนี้

ข้อ 1. ผู้ใช้งานต้องป้องกันทรัพย์สินของกรม และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศ ที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยให้ครอบคลุมเรื่องต่างๆ ประกอบด้วย

- การจัดการบริเวณล้อมรอบ
- การควบคุมการเข้า - ออก พื้นที่
- การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์
- ระบบและอุปกรณ์สนับสนุนการทำงาน

ข้อ 2. การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

ข้อ 3. ต้องมีการป้องกันเครื่องคอมพิวเตอร์หรือระบบงานของกรม ก่อนเข้าใช้งาน โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสม

ข้อ 4. ต้องมีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของกรม
- จัดเก็บเอกสาร ข้อมูลในการทำงาน ข้อมูลสำคัญหรือลับ หรือสื่อบันทึกข้อมูล ไว้ในสถานที่ที่มีความปลอดภัยภายหลังจากใช้งานเสร็จ เช่น เก็บไว้ในตู้ที่ล็อคกุญแจได้ เป็นต้น
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ล็อกเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันเครื่องโทรสารที่ใช้ในการติดต่อสื่อสารหรือส่งข้อมูลสำคัญ เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารสำคัญหรือลับออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ
- ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่างๆ เช่น เอกสาร สื่อบันทึก คอมพิวเตอร์ หรือสารสนเทศ ออกจากกรม ต้องขออนุญาตจากผู้บังคับบัญชาก่อนทุกครั้ง

ข้อ 5. ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

ข้อ 6. ผู้ดูแลระบบต้องบริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์และระบบเครือข่ายหลักของกรม เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหายใช้งานไม่ได้ หรือสูญหาย

ข้อ 7. ผู้ดูแลระบบต้องเก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

ข้อ 8. ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Operation Center) หมายถึง สถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่าย) ที่เป็นเขตหวงห้าม โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 9. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 10. ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อประกอบธุรกิจส่วนบุคคล

ข้อ 11. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ 12. ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์ จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่หน่วยงานมอบหมาย

ข้อ 13. กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมาย

ข้อ 14. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊ค ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

ข้อ 15. ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่างๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศ ต่างๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อกรม

ข้อ 16. ผู้ใช้งานมีหน้าที่ต้องชดใช้ ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ 17. การยืม – คืน ทรัพย์สิน

(1) ให้ปฏิบัติตามประกาศกรมวิทยาศาสตร์การแพทย์ เรื่อง ข้อปฏิบัติในการยืมทรัพย์สินของกรมวิทยาศาสตร์การแพทย์

(2) ก่อนคืนทรัพย์สินทุกครั้ง ผู้ยืมต้องลบข้อมูลที่เป็นความลับออกจากตัวเครื่องก่อนเสมอ

ส่วนที่ 4 การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล (Classification of information) และการบ่งชี้ข้อมูล (Labeling of information)

ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ 2) พ.ศ. 2561 และประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ.2567 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(1) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ประเภทขอมูลที่เกี่ยวกับการดำเนินงานดานการสนับสนุนการสงมอบบริการ เช่น ข้อมูลการควบคุมกับกับดูแลโครงการ, ข้อมูลการพัฒนานโยบายและแนวปฏิบัติ, ร่างกฎระเบียบ ข้อบังคับ, แผนงานและงบประมาณ, การจัดเก็บรายได้, ข้อมูลบริการและผลิตภัณฑ์ของกรม, ข้อมูลข่าวประชาสัมพันธ์

- ประเภทขอมูลที่เกี่ยวกับการบริหารจัดการทรัพยากรของรัฐ เช่น ขอมูลการจัดการสิ่งอำนวยความสะดวก ยานพาหนะ, ขอมูลการจัดการความมั่นคงปลอดภัย, ข้อมูลการจัดการทางการเงิน. การจัดการทรัพยากรบุคคล, การจัดการเทคโนโลยีสารสนเทศ

- ประเภทขอมูลที่เกี่ยวกับภารกิจการใหบริการประชาชน เช่น ข้อมูลผลการตรวจวิเคราะห์ด้านยา ด้านอาหาร ชันสูตรโรค สมุนไพร ชีววัตถุ , ข้อมูลความปลอดภัยของผูบริโภค, ขอมูลที่เกี่ยวกับการวิจัยดานการดูแลสุขภาพและการศึกษาของผูปฏิบัติงาน

- ประเภทขอมูลที่เกี่ยวกับกลไกสงมอบบริการ เช่น การจัดการความรู้, ข้อมูลการบังคับใช้กฎระเบียบ

(2) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด เช่น ข้อมูลทางการแพทย์ การเงิน เป็นต้น
- ข้อมูลที่มีระดับความสำคัญปานกลาง เช่น วิธีการตั้งค่าเครือข่าย เป็นต้น
- ข้อมูลที่มีระดับความสำคัญน้อย เป็นข้อมูลข่าวสารที่สามารถเผยแพร่ได้

(3) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด ผลกระทบระดับร้ายแรงที่สุดที่อาจคุกคามความมั่นคงของประเทศ เช่น แผนปฏิบัติการลับของรัฐบาล เป็นต้น
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง ผลกระทบร้ายแรงต่อองค์กรหรือหน่วยงานสำคัญ เช่น ข้อมูลการเงิน ข้อมูลการร้องเรียน เป็นต้น
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย ผลกระทบจำกัดต่อองค์กรหรือบุคคลในวงแคบ เช่น ข้อมูลส่วนบุคคล เป็นต้น
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้ ปกติจะนำเข้าและรับส่งข้อมูลผ่านระบบสารบรรณฯ ยกเว้นข้อมูลลับทั้งสามประเภทจะไม่นำไฟล์ข้อมูลเข้าสู่ระบบ

(4) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(5) รูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น TEXT Format, Document Format, PDF Format (Portable Document Format)
- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ มีรูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format, Bitmapping Format ฯลฯ
- รูปแบบสื่อมัลติมีเดีย (Multimedia Format) เช่น MPEG Format, AVI Format, MP4 Format ฯลฯ

ส่วนที่ 5 นโยบายและมาตรการควบคุมการเชื่อมโยงและแลกเปลี่ยนข้อมูล(Information transfer)

เพื่อควบคุมคุณภาพและมาตรฐานการปฏิบัติงานในการเชื่อมโยงแลกเปลี่ยนข้อมูลสารสนเทศระหว่างหน่วยงานให้เป็นระบบ มีมาตรฐานสามารถแลกเปลี่ยนข้อมูลได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัย และใช้เป็นคู่มือพื้นฐานสำหรับผู้บริหาร เจ้าหน้าที่ฝ่ายปฏิบัติงาน รวมทั้งเจ้าหน้าที่ด้านเทคนิคในการเขียนข้อกำหนดทางเทคนิคของโครงการพัฒนาระบบเพื่อการเชื่อมโยงข้อมูลและใช้เป็นคู่มือในการสร้างระบบสารสนเทศที่มีความสามารถในการเชื่อมโยงบริการและแลกเปลี่ยนข้อมูล และปฏิบัติการร่วมระหว่างระบบอิเล็กทรอนิกส์ให้เหมาะสมและคุ้มค่า

แนวทางการเชื่อมโยงและแลกเปลี่ยนข้อมูล

1. หน่วยงานทำหนังสือถึงหัวหน้าส่วนราชการเพื่อขออนุมัติเชื่อมโยงแลกเปลี่ยนข้อมูล
2. ศึกษาความเป็นไปได้ กำหนดขอบเขตการดำเนินงานและจัดทำแผนการดำเนินงานร่วมกัน
3. ลงนามข้อตกลงความร่วมมือในการเชื่อมโยงแลกเปลี่ยนข้อมูลร่วมกัน
4. พัฒนาและทดสอบระบบเชื่อมโยงแลกเปลี่ยนข้อมูลตามมาตรฐานที่กำหนด

4.1 มาตรฐานการแลกเปลี่ยนข้อมูล (Data Exchange Specification) ได้แก่

ลำดับ	การนำไปใช้	ชื่อมาตรฐาน
1	Data integration metadata/metalanguage	Extensible Markup Language XML v1.1
2	Data integration metadata definition	XML Schema
3	Data transformation	Extensible Stylesheet language XSL v1.1
		Extensible Stylesheet Language Transformation
4	Data Description language	Resource Description Framework
5	Data modelling exchange	XMI Metadata Exchange XML ME v1.1
6	Minimum interoperable character set	8 bit Unicode Transformation Format ISO/IEC 10646:Amd5:2008(E)

**หมายเหตุ : อ้างอิงตามมาตรฐานทางเทคนิคของ TH e-GIF

4.2 มาตรฐานรูปแบบการจัดเก็บและนำเสนอข้อมูล (Storage & Presentation Specification) ได้แก่

ลำดับ	การนำไปใช้	ชื่อย่อ	ชื่อมาตรฐาน
1	Content management metadata definition	XML	XML Schema
		DSML	Directory Service Markup Language DSML v2.0
2	Content syndication	RSSv1	RDF Site Summary v.1
		RSSv2	Really Simple Syndication v.2
3	Distributed searching	ISO 23950	Information Retrieval Z39.50
4	Identifiers for digital objects using ASN.1	OID	Object Identifiers x.667
5	Radio tracking identification	RFID	Radio Frequency Identifier
6	Document file type	RFT	Rich Text Format
		HTML	Hyper Text Markup Language
		ODF	Open Document Format
7	Spreadsheet file type	XLS	Microsoft Excel Spreed Sheet File
		CSV	Comma-separated Value
8	Presentation file type	PPS	Microsoft Power Point Show file
9	Graphical/still image information exchange specifications	JPEG	Joint photographic Expert Group
		GIF	Graphic Interchange Format
		PNG	Portable Network Graphic
10	Vector Graphics	SVG	Scalable Vector Graphics
11	Audio/video streaming data	WMV	Window Media Audio
		MP3	Moving Picture Experts Group3
		F4V	Flash Video
12	Web Animation	SWF	Shock Wave File
13	General purpose file and compression	ZIP	Data Compressed file format
14	Hypertext interchange formats	HTML	Hyper Text Markup Language
15	Data modelling language	UML	Unified Modelling Language
		E-R diagram	Entity Relation Diagram

**หมายเหตุ : อ้างอิงตามมาตรฐานทางเทคนิคของ TH e-GIF

ส่วนที่ 6 การควบคุมการเข้าถึง (Access control)

ข้อ 1. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งาน ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ 2. บุคคลภายนอกหน่วยงานที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของหน่วยงานต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงาน

ข้อ 3. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมกับการใช้งานและหน้าที่ความรับผิดชอบ รวมทั้งทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

(1) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงข้อมูลสารสนเทศ ดังนี้

(1.1) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น อ่านอย่างเดียว สร้างข้อมูล บันทึกข้อมูล แก้ไขข้อมูล ลบข้อมูล อนุมัติ ไม่มีสิทธิ์ ฯลฯ

(1.2) กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

ข้อ 4. ผู้ดูแลระบบ ต้องติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ 5. ผู้ดูแลระบบ ต้องบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ 6. ผู้ดูแลระบบ ต้องบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ 7. ระบบสารสนเทศด้านงานบริการ Front Office และ Back Office สำหรับผู้ใช้งาน ให้สามารถเข้าถึงได้ตามเวลาที่หน่วยงานกำหนด

การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ 8. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(1) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

(2) ตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(3) ตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อการใช้งาน (ตามส่วนที่ 1 ข้อ 3)

(4) กำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ 9. ผู้ดูแลระบบ กำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์ผู้ใช้งานเฉพาะการปฏิบัติงานในหน้าที่ซึ่งได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษรหรือทางระบบอิเล็กทรอนิกส์ที่สามารถยืนยันตัวบุคคลได้

ข้อ 10. ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งาน อย่างสม่ำเสมอ ปีละ 1 ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(1) จัดทำรายชื่อของผู้ที่ยังมีสิทธิ์ในระบบ

(2) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่ หรือดำเนินการอื่นใดทางอิเล็กทรอนิกส์เพื่อเป็นการยืนยัน/ทบทวนสิทธิ์

(3) ดำเนินการแก้ไขข้อมูล สิทธิ์ต่างๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

(4) ในกรณีหน่วยงานเป็นผู้ทบทวนสิทธิ์และส่งคำร้องขอมาให้ผู้ดูแลระบบดำเนินการแก้ไข ทบทวนสิทธิ์ตามที่ได้รับคำร้องขอจากหน่วยงาน

ข้อ 11. ผู้ดูแลระบบยกเลิกสิทธิ์การใช้งานภายหลังจากได้รับการแจ้งจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร

ข้อ 12. การบริหารจัดการรหัสผ่าน

(1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือ เกษียณอายุราชการ หรือยกเลิกการใช้งาน ภายหลังจากได้รับการแจ้งจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร

(2) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งาน โดยต้องไม่ซ้ำกัน

(3) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (Email) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(4) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password) ผ่านช่องทางที่สามารถยืนยันตัวตนได้ เช่น การเซ็นรับทราบ หรือ การแจ้งกลับผ่านทาง e-mail

(5) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(6) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และกำหนดสิทธิ์พิเศษที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(7) ในกรณีเกษียณอายุราชการ กรมจะคงสิทธิ์การใช้งาน e-mail และระบบแจ้งเงินเดือนออนไลน์ (Payslip) ให้สามารถใช้งานได้ต่อเนื่อง แต่หากในระยะเวลา 1 ปี ไม่มีการเข้าถึงระบบดังกล่าวกรมจะดำเนินการยกเลิกสิทธิ์ของท่านโดยอัตโนมัติ เพื่อเคลียร์พื้นที่ให้สำหรับผู้ใช้งานท่านใหม่

ข้อ 13. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลดังนี้

(1) กำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(2) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(3) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(4) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(5) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(6) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง เพื่อมั่นใจว่าสิทธิ์ต่างๆ ยังคงมีความเหมาะสม

ข้อ 14. ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างกรมหรือหน่วยงานที่มาขอเชื่อมโยง

(1) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

(2) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(3) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

(4) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(5) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ 15. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

(1) ป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองตามลักษณะงานที่เกี่ยวข้อง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

(2) การกำหนดรหัสผ่าน

(2.1) ความยาวไม่น้อยกว่า 8 ตัว ประกอบด้วย ตัวอักษร (Alphabet) พิมพ์เล็กพิมพ์ใหญ่ ตัวเลข (Numerical character) และควรมีอักขระพิเศษ (Special character)

(2.2) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผนและง่ายต่อการคาดเดา เช่น “abcdef” “aaaaaa” “123456” “123456”

(2.3) ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

(3) ไม่ใช้รหัสผ่านส่วนบุคคลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(4) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ครอบครองอยู่

(5) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(6) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานในลักษณะที่ยากต่อการคาดเดาและการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(7) เปลี่ยนรหัสผ่าน (Password) และต่ออายุการใช้งาน เมื่อระบบแจ้งเตือนว่าหมดอายุการใช้งาน

(8) เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจมีการรั่วไหล

ข้อ 16. นำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

ข้อ 17. การกระทำใดๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ 18. ผู้ใช้งานต้องทำการการยืนยันตัวตนหรือพิสูจน์ตัวตน (Authentication) ทุกครั้ง เช่น ใส่ชื่อผู้ใช้และรหัสผ่าน (Username & Password) ก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดี หรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

(1) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
(2) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง
(3) การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้
(4) เมื่อไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง
(5) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งค่าประหยัดพลังงาน (Power Save mode) เมื่อไม่ใช้งาน และต้องมีการพิสูจน์ตัวตนเมื่อเข้าสู่หน้าจอการใช้งาน

ข้อ 19. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของกรมหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ 20. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญต้องอยู่ในการครอบครอง/ดูแลของหน่วยงาน

ข้อ 21. ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ 22. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อสินทรัพย์ ข้อมูลของกรมและข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด รวมทั้ง การเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ 23. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่างๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ 24. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กรมให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่กรมต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับกรมซึ่งกระทรวงสาธารณสุขอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ 25. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (คือ กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน โดยที่แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ 26. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ 27. ห้ามใช้สินทรัพย์ของหน่วยงานที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของกรม

ข้อ 28. ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกรม

ข้อ 29. ห้ามใช้สินทรัพย์ของกรมเพื่อประโยชน์ทางการค้า

ข้อ 30. ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของกรมโดยเด็ดขาด ไม่ว่าด้วยวิธีการใดๆ ก็ตาม

ข้อ 31. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ 32. ห้ามใช้ระบบสารสนเทศของกรมเพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ 33. ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ 34. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเข้าถึงระบบสารสนเทศของกรม โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ 35. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน ในกรณีที่เป็น เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อเข้ากับระบบโดเมน (Join Domain)

ข้อ 36. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

(1) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบตามข้อกำหนดในส่วนที่ 3

(2) หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

(3) ผู้ใช้งานต้องตั้งค่าประหยัดพลังงาน (Power Save mode) เมื่อไม่ใช้งานเครื่องคอมพิวเตอร์อย่างน้อย 30 นาที เพื่อทำการ ล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้อง ใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(4) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

(5) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

(6) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

(7) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงานกรม

(8) ซอฟต์แวร์ที่กรมใช้มีลิขสิทธ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ <u>หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว</u>

(9) ซอฟท์แวร์ที่กรมจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

(10) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกรมเพื่อประโยชน์ทางการค้า

(11) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(12) ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ 37. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ 38. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งาน โปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการ ดังนี้

(1) การใช้งานโปรแกรมยูทิลิตี้ ผู้ใช้งานต้องปฏิบัติให้สอดคล้องกับประกาศกรม เรื่อง นโยบายและแนวปฏิบัติการใช้งานคอมพิวเตอร์ที่ถูกต้องตามกฎหมาย หากมีการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้น รวมทั้งหัวหน้าหน่วยงานต้องรับผิดชอบในความเสียหายที่เกิดขึ้นร่วมกัน

(2) ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

ข้อ 39. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session time-out)

(1) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งาน หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 60 นาที

(2) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบสารสนเทศที่มีความเสี่ยงสูง

ข้อ 40. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

(1) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนด และให้ใช้งานได้ตามช่วงเวลาการทำงานที่หน่วยงานกำหนดเท่านั้น

(2) กำหนดให้ระบบเทคโนโลยีสารสนเทศ ที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ข้อ 41. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งาน ในการใช้งานตามความจำเป็น

ข้อ 42. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น

ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (Email) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าว อย่างสม่ำเสมอ

ข้อ 43. ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน 60 นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ 44. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน หรือยกเลิกการใช้งาน

(2) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(3) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(4) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ 45. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(1) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(2) กำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(3) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(5) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(6) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ 46. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

(1) แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่นๆ

(2) มีการควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

(3) มีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น

ข้อ 47. การใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(1) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(2) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(3) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(4) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่รับคืนด้วย

(5) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ข้อ 48. การใช้งานระบบสารสนเทศจากต่างประเทศ

ผู้ขอใช้งานที่ไปปฏิบัติงาน ณ ต่างประเทศ และมีความประสงค์จะใช้ระบบสารสนเทศของกรม ต้องดำเนินการดังนี้

1. จัดทำหนังสือราชการเพื่อขอใช้งานระบบสารสนเทศจากต่างประเทศ โดยให้ระบุวันที่และช่วงเวลาที่ประสงค์เข้าใช้งาน พร้อมแนบแบบฟอร์ม 0626 FM 0017 แบบฟอร์มขอสิทธิ์เข้าใช้งานระบบเครือข่ายเสมือนสำหรับทำงานจากระยะไกล ผ่านผู้บังคับบัญชาลงนามให้ความเห็นชอบ ตามลำดับชั้น ส่งถึงศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยให้ดำเนินการก่อนเดินทางไปต่างประเทศ อย่างน้อย 7 วัน

2. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พิจารณาอนุมัติและมอบหมายให้ฝ่ายพัฒนาระบบคอมพิวเตอร์ดำเนินการและให้คำปรึกษาแนะนำการเข้าใช้งาน

3. ผู้ขอใช้งาน ต้องดูแลรักษาเครื่องคอมพิวเตอร์/อุปกรณ์ที่นำมาใช้ และปฏิบัติตามนโยบายและแนวปฏิบัติในการใช้สิทธิ์ในการทำงานจากภายนอกหน่วยงาน (Teleworking) ของกรม ตามหมวดที่ 1 นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ อย่างเคร่งครัด

4. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ขอสงวนสิทธิ์การใช้งานตามระยะเวลาที่กำหนดเท่านั้น เพื่อเป็นไปตามระบบรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศของกรม

การควบคุมการส่งข้อความทางอิเล็กทรอนิกส์

ข้อ 49. ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (Email) ต้องทำการกรอกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (Email) ตามแบบฟอร์มสมัครสมาชิกเครือข่ายกรมวิทยาศาสตร์การแพทย์ (0600 FM 0101) และส่งคำขอมาที่ศูนย์เทคโนโลยีสารสนเทศ

ข้อ 50. รหัสผ่านของจดหมายอิเล็กทรอนิกส์ (Email) ต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “X” หรือ “O” หรือ “ เ” หรือ “*” ในการพิมพ์แต่ละตัวอักษร

ข้อ 51. เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (Email) และมีการเข้าสู่ระบบในครั้งแรกนั้นควรเปลี่ยนรหัสผ่าน (Password) โดยทันที และกำหนดให้สอดคล้องกับผู้ให้บริการระบบเมลกลางภาครัฐ

ข้อ 52. ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ หรือจุดที่เข้าถึงรหัสผ่านได้ง่าย

ข้อ 53. เปลี่ยนรหัสผ่าน (Password) ทุก 3 หรือ 6 เดือน หรือเมื่อมีสัญญาณเตือนว่ารหัสผ่านรั่วไหล หรือสอดคล้องตามที่ผู้ให้บริการระบบเมลกลางภาครัฐ

ข้อ 54. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (Email) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (Email) ของตน หากมีการกระทำผิดความผิดเกิดขึ้น เจ้าของผู้ใช้งานต้องรับผิดชอบโดยไม่มีข้อยกเว้น

ข้อ 55. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Email) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ 56. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (Email) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลที่หน่วยงานกำหนดไว้ ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ในจดหมายอิเล็กทรอนิกส์ (Email) ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ 57. ห้ามส่ง Email ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ 58. ห้ามส่ง Email ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ 59. ห้ามส่ง Email ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือละเมิดสิทธิของบุคคลอื่น

ข้อ 60. ห้ามส่ง Email ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ 61. ให้ระบุชื่อของผู้ส่งใน Email ทุกฉบับที่ส่งไป

ข้อ 62. ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ (Email) ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าหน่วยงานจะทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ (Email) ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้นจดหมายอิเล็กทรอนิกส์ (Email) ที่มีระยะเวลาส่งเมื่อนานมาแล้ว และจำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

ข้อ 63. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ (Email) ก่อนการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส (Antivirus) เป็นการป้องกันในการเปิดไฟล์ที่สามารถเข้าถึงระบบปฏิบัติการ (Executable file) เช่น .exe .com เป็นต้น

ข้อ 64. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก หรือแอบอ้างเป็นบุคคลอื่น หรือองค์กร จากจดหมายอิเล็กทรอนิกส์ (Email) และสื่อสังคมออนไลน์ (Social Media) ต่างๆ ที่มีเนื้อหาในการขอข้อมูลที่มีความอ่อนไหว เช่น ข้อมูลส่วนบุคคล รหัสผ่าน เป็นต้น

ข้อ 65. ผู้ใช้งานต้องใช้ข้อความที่สุภาพในการรับส่งจดหมายอิเล็กทรอนิกส์ (Email) รวมไปถึงสื่อสังคมออนไลน์ (Social Media) ต่างๆ ของทางราชการ และไม่ใช้ข้อความที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์ (Email) และสื่อสังคมออนไลน์ (Social Media) ต่างๆ

ข้อ 66. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Email) ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ (Email) ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ (Email) ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่บนระบบจดหมายอิเล็กทรอนิกส์ (Email)

ข้อ 67. ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ (Email) ที่ใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ (Email) ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์ (Email)

ข้อ 68. ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในระบบราชการ ตามมติคณะรัฐมนตรีเมื่อวันที่ 18 ธันวาคม 2550 เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

ข้อ 69. กรณีใช้แอฟพลิเคชั่นไลน์ (Line) จัดตั้งกลุ่มเพื่อสื่อสารข้อมูลของทางราชการให้ใช้ชื่อตามตัวแรก เป็น GCC ตามด้วยระดับของหน่วยงาน ตามด้วยอักษรย่อสังกัดกระทรวง อักษรย่อกรม และอักษรย่อหน่วยงาน

การควบคุมการใช้อินเตอร์เน็ต (Internet)

ข้อ 70. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ 71. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ต ผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการยืนยันตัวตนเข้าสู่ระบบ (Login) รวมถึงต้องมีการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) และทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ 72. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ 73. ไม่ใช้ระบบอินเตอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์ เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ 74. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

ข้อ 75. ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเตอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ 76. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Social Network) ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่ทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ 77. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

ข้อ 78. หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบ (Logout) และให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อ 79. ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พ.ศ. 2560 อย่างเคร่งครัด

ส่วนที่ 7 ความมั่นคงปลอดภัยสารสนเทศ สำหรับการใช้บริการ Cloud (Information security for use of cloud services)

ข้อที่ 1. การวางแผนการนำระบบงานไปติดตั้งบนคลาวด์

(1) คัดเลือกผู้ให้บริการคลาวด์ที่มีความน่าเชื่อถือด้านความมั่นคงปลอดภัย

(2) การจัดการส่วนที่เกี่ยวข้องกับเขตอำนาจรัฐ รัฐบาลประเทศไทย และกฎหมายระหว่างประเทศ (ที่เกี่ยวข้อง)

(3) ระบุระบบงานและข้อมูลของระบบงานที่จะนำขึ้นคลาวด์

(4) ระบุชั้นความลับและเจ้าของข้อมูลว่าสอดคล้องกับนโยบายการนำระบบงานและข้อมูลไปติดตั้งบนคลาวด์ที่องค์กรกำหนดไว้หรือไม่

(5) ดำเนินการจัดการกับข้อมูลตามชั้นความลับของข้อมูล

(6) จัดทำบัญชีทรัพย์สินขององค์ประกอบของระบบที่จะนำขึ้นคลาวด์

(7) ประเมินความเสี่ยงกับระบบและจัดทำแผนการลดความเสี่ยง

(8) กำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงาน

(9) กำหนดข้อตกลงการควบคุมการเชื่อมต่อระบบ (The Agreed and Finalized Interface Control Document : ICD)

ข้อที่ 2. การวิเคราะห์และออกแบบความมั่นคงปลอดภัยทางเครือข่าย

(1) ออกแบบและจัดทำผังเครือข่ายของระบบ

(2) แบ่งแยกเครือข่ายตามผังเครือข่ายที่กำหนด

(3) แยกเครื่องคอมพิวเตอร์แม่ข่ายเสมือนสำหรับการทดสอบไว้ในเครือข่ายที่แยกต่างหากจากเครื่องคอมพิวเตอร์แม่ข่ายเสมือนสำหรับการให้บริการจริง

(4) ศึกษาการจราจร (Traffic) ที่เข้าออกเครือข่ายทั้งหมด เพื่อกำหนดเป็น Traffic ที่อนุญาตและไม่อนุญาต ซึ่งเป็นการกำหนดการไหลของข้อมูลในเครือข่าย

(5) กำหนดนโยบาย (Policy) ไฟร์วอลล์ (Firewall) เพื่อจำกัด Traffic ที่เข้า-ออกเครือข่าย

(6) ติดตั้งไฟร์วอลล์และกำหนด Rule บนไฟร์วอลล์ตามนโยบายไฟร์วอลล์ที่กำหนดไว้

(7) ติดตั้งระบบป้องกันการบุกรุก

(8) ติดตั้งระบบป้องกันไวรัส

(9) ติดตั้งระบบ VPN สำหรับผู้ดูแลระบบใช้งาน

(10)ติดตั้งระบบตั้งสัญญาณนาฬิกาให้ตรง

ข้อที่ 3. การวิเคราะห์และออกแบบระบบงานด้านความมั่นคงปลอดภัย

(1) กำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงานอย่างน้อย ดังต่อไปนี้

1) ด้านการตรวจสอบข้อมูลนำเข้าและออกจากระบบงาน

2) ด้านการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่สำคัญและอาจจำเป็นต้องตรวจสอบในภายหลัง

3) ด้านกลุ่มผู้ใช้งาน บทบาท และสิทธิ์การเข้าถึงระบบงาน

4) ด้านการลงทะเบียนและถอดถอนการเข้าถึงระบบงาน

5) ด้านการตัดหรือหมดเวลาใช้งาน

6) ด้านการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย

7) ด้านหน้าจอการล็อคอิน (Login) ที่มีความมั่นคงปลอดภัย
8) ด้านการติดตามปริมาณการใช้ระบบและขีดความสามารถ หรือประสิทธิภาพของระบบ
9) ด้านการป้องกันข้อมูลรหัสผ่าน (Password) ของผู้ใช้งาน
10) ด้านการป้องกันข้อมูลสำคัญที่จัดเก็บไว้ในระบบงาน
11) ด้านการป้องกันข้อมูลสำคัญที่มีการส่งผ่านเครือข่าย
12) ด้านการเข้ารหัสข้อมูลและการลงลายมือชื่อดิจิตอล
13) ด้านการวิเคราะห์จุดอ่อนของซอร์สโค้ด (Source Code)
14) ด้านการกู้คืนระบบงาน

(2) ดำเนินการวิเคราะห์และออกแบบระบบด้านความมั่นคงปลอดภัย

ข้อที่ 4. การทดสอบระบบ

(1) ทดสอบระบบให้ครอบคลุมตามความต้องการด้านความมั่นคงปลอดภัยของระบบงานที่กำหนดไว้ (Security Test)

(2) ป้องกันข้อมูลสำคัญ (Data Masking Technique) ก่อนนำไปทดสอบกับระบบ
1) เจ้าของข้อมูลต้องลบข้อมูลส่วนที่สามารถบ่งชี้ตัวบุคคลทิ้งไปก่อนทดสอบกับระบบ
2) เจ้าของข้อมูลต้องลบข้อมูลส่วนที่เป็นความลับทิ้งไปก่อนนำไปทดสอบกับระบบ

(3) ทดสอบโดยการป้อนอินพุท (Input) ที่จะทำให้ระบบทำงานผิดพลาด ไม่ถูกต้อง ทำให้ระบบล่ม หรือถึงขั้นระบบถูกบุกรุกได้ (Fuzzing Technique)

(4) ทดสอบและรับรองระบบ (User Acceptance Test)

ข้อที่ 5. การติดตั้งระบบ

(1) จัดทำแผนการติดตั้งระบบงาน

(2) ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่าง ๆ ที่เกี่ยวข้องกับระบบงานให้แล้วเสร็จ ก่อนที่จะติดตั้งระบบงาน

(3) ปิดบริการ (Service) ที่ไม่มีความจำเป็นต้องใช้งานในระบบงาน

(4) จัดทำพื้นฐานด้านความปลอดภัยในการใช้งาน (Security Baseline) ของระบบที่จะทำการติดตั้ง

(5) ปรับแต่งค่าพารามิเตอร์ต่าง ๆ ที่มีผลต่อความมั่นคงปลอดภัยของระบบงานตาม Security Baseline ของระบบที่ได้กำหนดไว้

(6) จำกัดการเข้าถึงซอร์สโค้ด (Source Code) ของระบบงาน หลีกเลี่ยงการติดตั้งซอร์สโค้ดของระบบงานบนเครื่องให้บริการ (ยกเว้นในกรณีที่ระบบงานต้องเรียกใช้โดยตรงในขณะที่ทำงาน)

(7) ตรวจสอบและปิดช่องโหว่ในระบบที่ทำการติดตั้ง

(8) ติดตั้งโปรแกรมเพื่อติดตามและตรวจสอบการเปลี่ยนแปลงแก้ไขไฟล์ต่าง ๆ ของระบบโดยไม่ได้รับอนุญาต

(9) ทำแผนการตรวจสอบและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Log) บนเครื่องคอมพิวเตอร์แม่ข่ายสำหรับให้บริการระบบงานที่ทำการติดตั้ง

(10)ทำแผนการสำรองข้อมูลของระบบงานและดำเนินการตามแผนฯ

(11)ทำแผนการตรวจสอบและติดตามสภาพความพร้อมใช้ของระบบงานและ ดำเนินการตามแผนฯ

(12)ทำแผนการตรวจสอบและติดตามทรัพยากรของระบบงานและดำเนินการตามแผนฯ

ข้อ 6. ทำแผนการกู้คืนระบบงานและดำเนินการทดสอบปีละครั้ง

ข้อ 7. การใช้คลาวด์ส่วนบุคคล (Private Cloud)

(1) กรมอนุญาตให้ใช้คลาวด์ส่วนบุคคล (Pirvate Cloud) เช่น Google drive, dropbox ในเครื่องคอมพิวเตอร์ของกรม และระบบเครือข่ายของกรมได้เฉพาะในกรณีที่เป็นไฟล์ส่วนบุคคลเท่านั้น **ห้าม**นำไฟล์งาน ข้อมูลงานตามภารกิจของกรมหรืองานราชการเข้าสู่ระบบคลาวด์ส่วนบุคคล (Pirvate Cloud)

(2) กรณีที่มีความจำเป็นต้องใช้คลาวด์ส่วนบุคคล (Pirvate Cloud) เพื่อติดต่อกับหน่วยงานภายนอก จะต้องทำบันทึกขออนุญาตผู้บริหารของหน่วยงานและผู้ดูแลระบบก่อนการใช้งาน

(3) งานตามภารกิจของกรมอนุญาตให้ใช้ได้เฉพาะคลาวด์ one drive ของ workD Space ภายใต้โดเมน dmsc.mail.go.th เท่านั้น

3.1 กรณีที่เป็นข้อมูลที่ต้องจำกัดผู้รับรู้ หรือมีชั้นความลับ ให้มีการตั้งค่าคลาวด์ one drive ของ workD Space ให้เข้าถึงได้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

3.2 เมื่อสิ้นสุดระยะเวลาดำเนินการต้องดำเนินการยกเลิกสิทธิการเข้าถึงของ คลาวด์ one drive ของ workD Space

(4) เจ้าหน้าที่ที่ได้รับมอบหมาย ทำการสุ่มตรวจการใช้คลาวด์ส่วนบุคคล อย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 8 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

ข้อ 1. กรมให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น ซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้น รวมทั้งหัวหน้าหน่วยงานต้องรับผิดชอบในความเสียหายที่เกิดขึ้นร่วมกัน

ข้อ 2. ซอฟต์แวร์ (Software) ที่หน่วยงานติดตั้งบนคอมพิวเตอร์ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่นๆ ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์ รวมถึงไม่ติดตั้งซอฟต์แวร์ที่จะก่อให้เกิดอันตรายกับระบบเครือข่าย เช่น การใช้โปรแกรมสปาย (Spyware), Ad-aware, bitcoin mining software, bittorrent mining, ScanPC, Baidu PC faster, Hao123 เป็นต้น

ข้อ 3. ซอฟต์แวร์ (Software) ที่หน่วยพัฒนาถือเป็นทรัพย์สินทางปัญญาของกรมวิทยาศาสตร์กาแพทย์ ห้ามเผยแพร่ Source code หรือการตั้งค่าส่วนหนึ่งส่วนใดไปให้หน่วยงาน/องค์กร ภายนอกใช้งานโดยไม่ได้รับอนุญาตจากคณะกรรมการบริหารและพัฒนาระบบสารสนเทศ ของกรมวิทยาศาสตร์การแพทย์

หมวดที่ 2

นโยบายและมาตรการด้านบุคลากร (People controls)

วัตถุประสงค์

1. เพื่อให้มั่นใจว่าบุคลากรทุกคนที่ได้รับการคัดเลือกให้ปฏิบัติงานในตำแหน่งซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ มีคุณสมบัติและความเหมาะสมตามที่กำหนดไว้ และยังคงมีคุณสมบัติและความเหมาะสมดังกล่าวอย่างต่อเนื่องตลอดระยะเวลาการปฏิบัติงาน ทั้งนี้ เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นต่อความมั่นคงปลอดภัยของระบบสารสนเทศและทรัพยากรของหน่วยงาน
2. เพื่อให้มั่นใจว่าบุคลากรมีความเข้าใจถึงหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับตำแหน่งงานที่ได้รับการพิจารณาให้ดำรงหรือปฏิบัติงาน
3. เพื่อให้บุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องรับทราบและปฏิบัติตามหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

แนวปฏิบัติ

ส่วนที่ 1 การคัดเลือกและการสรรหาบุคลากร (Screening) เงื่อนไขการจ้างงาน (Terms and conditions of employment) กระบวนการทางวินัย (Disciplinary process)

ข้อ 1. การคัดเลือกและการสรรหาบุคลากรให้เป็นไปตามพระราชบัญญัติระเบียบข้าราชการพลเรือน พ.ศ. 2551 แล้ว ยังจะต้องมีคุณสมบัติเฉพาะสำหรับตำแหน่งตามที่กำหนดไว้ในมาตรฐานกำหนดตำแหน่ง และระเบียบต่าง ๆ ที่เกี่ยวข้องของกระทรวงสาธารณสุข

ข้อ 2. การจ้างบุคคลรวมถึง Outsource

(1) พิจารณาคุณสมบัติการจ้างบุคคลตามพระราชบัญญัติระเบียบข้าราชการพลเรือน พ.ศ. 2551 หมวด 3 การสรรหา การบรรจุ และการแต่งตั้ง ตามมาตรา 52 ถึงมาตรา 71 และตามแบบบรรยายลักษณะงาน (Job Description) ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงพิจารณาคุณสมบัติตามประกาศกรมในการจ้างแต่ละตำแหน่ง

(2) กำหนดคุณสมบัติทั่วไปของผู้มีสิทธิสมัครไว้ในประกาศกรมในการจ้างแต่ละตำแหน่ง

(3) กำหนดคุณลักษณะต้องห้าม เช่น เป็นผู้อยู่ในระหว่างสั่งพักราชการหรือสั่งให้ออกจากราชการ เป็นผู้เคยต้องรับโทษจำคุกโดยคำพิพากษา เป็นผู้เคยกระทำการทุจริตในการสอบเข้ารับราชการ เป็นต้น ไว้ในประกาศกรมในการจ้างแต่ละตำแหน่ง

(4) ผู้ปฏิบัติงานต้องดำเนินการตามแบบมอบหมายงานของหน่วยงาน

(5) ก่อนเริ่มปฏิบัติงานต้องลงนามข้อตกลงรักษาความลับของข้อมูล ตามแบบฟอร์มที่หน่วยงานกำหนดไว้

(6) กรณีที่บุคคลนั้นกระทำความผิดให้พิจารณาความผิดตามบทลงโทษที่ได้กล่าวไว้ในข้อ 5.

ข้อ 3.การลงนามข้อตกลงรักษาความลับของข้อมูล (Confidentiality or nondisclosure agreements)

(1) ผู้ปฏิบัติงาน ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องลงนามข้อตกลงการรักษาความลับ

(2) ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัยของสารสนเทศต้องลงนามข้อตกลงการรักษาความลับ

(3) กำหนดให้มีการลงนามข้อตกลงการรักษาความลับไว้ในสัญญาจ้างของทุกโครงการ

(4) ผู้รับจ้างจากภายนอกทุกโครงการ ต้องลงนามข้อตกลงการรักษาความลับ ก่อนดำเนินงาน

ข้อ 4. การเลิกจ้างบุคคลรวมถึง Outsource

<u>กรณีโอนย้าย</u>

(1) หน่วยงานต้นสังกัดเดิมแจ้งมายังฝ่ายไอทีทันที่ที่มีบุคคลโอนย้าย พร้อมกับพิจารณาทบทวนสิทธิการเข้าถึงระบบงานหรือข้อมูลสารสนเทศที่พนักงานพ้นจากหน้าที่เดิมแล้วยังจำเป็นต้องเข้าถึงระบบงานและข้อมูลใดบ้าง คงสิทธิให้เข้าถึงเฉพาะที่จำเป็นเท่านั้น (ตามหลัก least privilege)

(2) ฝ่ายไอทีทำการยกเลิกสิทธิการเข้าถึงระบบและข้อมูลสารสนเทศตามที่หน่วยงานต้นสังกัดเดิมแจ้งมา

(3) ฝ่ายอาคารสถานที่ พิจารณาว่าพนักงานที่โอนย้ายจำเป็นต้องให้สิทธิผ่านเข้าหน่วยงานใหม่และยกเลิก Access Control ที่ประตูหน่วยงานเดิมหรือไม่ กรณีนี้แล้วแต่ความจำเป็นและสภาพแวดล้อมของพื้นที่ปฏิบัติงาน

(4) ฝ่ายการเจ้าหน้าที่/ผู้ที่ได้รับหมอบหมายให้ปฏิบัติงานด้านบริหารงานบุคลล พิจารณาความจำเป็นที่ต้องเรียกคืนทรัพย์สินที่ได้รับในตำแหน่งเดิม เช่น Notebook ,External Hardisk ฯลฯ หรือไม่

<u>กรณีลาออกหรือหมดสัญญา รวมถึงกรณี Outsource จบงาน</u>

(1) หน่วยงานต้นสังกัดแจ้งมายังฝ่ายไอทีทันที่ที่มีการลาออกของบุคคล/Outsource จบงาน เพื่อให้ถอนสิทธิออกจากทุกระบบงาน

(2) ฝ่ายไอทีทำการยกเลิกสิทธิการเข้าถึงระบบและข้อมูลสารสนเทศตามที่แจ้งมา

(3) ผู้ที่ได้รับหมอบหมายให้ปฏิบัติงานด้านบริหารงานบุคลล เรียกคืนทรัพย์สินทุกอย่างขององค์กร หากมีรายการทรัพย์สินที่มอบให้พนักงานเพื่อใช้ปฏิบัติงานก็ต้องทำการตรวจสอบทรัพย์สินที่เรียกคืน

(4) การตรวจสอบสภาพของทรัพย์สิน ประเด็นนี้ขึ้นอยู่กับความเข้มงวดหรือข้อตกลงของแต่ละหน่วยงาน

(5) ฝ่ายอาคารสถานที่ถอนสิทธิการผ่านเข้าออกประตูอัตโนมัติ

ข้อ 5. บทลงโทษ

(1) ให้ปฏิบัติตามบทลงโทษที่อยู่ในพระราชบัญญัติระเบียบข้าราชการพลเรือน พ.ศ. 2551 ฉบับแก้ไขเพิ่มเติม รวมถึงพระราชบัญญัติระเบียบข้าราชการพลเรือน พ.ศ. 2562 (ฉบับที่ 3)

(2) ให้ปฏิบัติตามบทลงโทษที่อยู่ในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ปี 2550 และที่แก้ไขเพิ่มเติม ปี 2560

(3) ปฏิบัติตามบทลงโทษ ดังนี้

1. โทษขั้นต้น ว่ากล่าวตักเตือนด้วยวาจา และ/หรือ ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่าย เป็นระยะเวลา 2 วัน หรือจนกว่าผู้ดูและระบบจะดำเนินการตรวจสอบแก้ไขระงับเหตุแล้วเสร็จ

2. โทษขั้นกลาง ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่าย เป็นเวลา 15 วัน หรือตักเตือนเป็นลายลักษณ์อักษร

3. โทษขั้นสูง ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่าย เป็นเวลา เดือน และ/หรือ หากละเมิด ฝ่าฝืนก่อให้เกิดความเสียหาย ต่อผู้อื่น หรือต่อทรัพย์สินทั้งของทางราชการอย่างร้ายแรง จะต้องรับโทษตามระเบียบส่วนราชการ หรือรับโทษ ตามกฎหมายโดยลำดับต่อไป

****หมายเหตุ : นิยามความหมาย “ผู้ฝ่าฝืน”**

<u>ผู้ฝ่าฝืนขั้นต้น</u> เกิดจากการฝ่าฝืนระเบียบโดยเล็กน้อยจากความไม่ตั้งใจ หรือโดย

บังเอิญ เช่น เปิดให้ใช้แฟ้มข้อมูลร่วม (Share File/Folder) หรือการใช้อุปกรณ์ร่วม (Share CD) โดยลืมกำหนดรหัสผ่าน (password) และ/ หรือไม่ทำ การยกเลิกการเปิดใช้แฟ้มข้อมูลร่วมกัน หลังจากการใช้งานเสร็จสิ้น เป็นต้น

ผู้ฝ่าฝืนขั้นกลาง

1. นำโปรแกรมคอมพิวเตอร์ หรือข้อมูลที่มีไวรัสคอมพิวเตอร์ มาติดตั้งใช้งานในเครือข่ายของกรมทำให้เกิดการแพร่กระจายในเครือข่าย โดยขาดความตระหนักด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ
2. ทำ การ Download ไฟล์ที่มีขนาดใหญ่ เกินกว่า 50 MB. โดยไม่จำเป็น และในระหว่างเวลาราชการซึ่งมีการใช้เครือข่ายอย่างหนาแน่น
3. ใช้ระบบ Internet ของกรมในการ ฟังเพลง Online หรือ เล่นเกมส์ Online หรือสนทนา Online VDO (Chat) เพื่อประกอบธุรกิจส่วนตัวในเวลาราชการ
4. ทำการติดตั้งเลขหมาย IP Address หรือนำ เลขหมาย IP Address ของกรมไปใช้ โดยไม่ได้รับอนุญาต ทำให้ความเสียหายแก่เครือข่าย
5. ทำการติดตั้งอุปกรณ์เครือข่ายเพิ่มเติม โดยไม่ได้รับอนุญาต ทำให้ความเสียหายแก่เครือข่ายของกรมในวงกว้าง

ผู้ฝ่าฝืนขั้นสูง เกิดจากการละเมิดกฎ และสร้างความเสียหายให้แก่กรม และระบบเครือข่ายของกรม เช่น

1. ใช้ จดหมายอิเล็กทรอนิกส์ (Email) ของกรม ส่ง mail แบบกระจาย ถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น หรือ การใช้ข้อความที่ไม่สุภาพส่งไปถึงบุคคลอื่นโดยส่งผลกระทบต่อภาพลักษณ์อันดีของกรม
2. ล่วงละเมิด บุกรุกหรือรันโปรแกรมจนเป็นเหตุให้ระบบของเซิร์ฟเวอร์ได้รับความเสียหาย
3. สร้างความเสียหายแก่โปรแกรมหรือข้อมูลหรือฮาร์ดแวร์ระบบ
4. การเข้าถึงระบบโดยปราศจากความยินยอมหรือการอนุญาตของผู้ดูแลระบบ พยายามขโมยรหัสผ่าน (Password) หรือข้อมูล หรือพยายามเจาะระบบรักษาความปลอดภัยของทั้งเครือข่ายภายในและภายนอกกรม
5. การสร้างโฮมเพจส่วนตัวที่แสดงออกในลักษณะที่ขัดต่อกฎหมาย กฎระเบียบ และศีลธรรม
6. นำ ข้อมูลที่ไม่เหมาะสมใส่ไว้ในโฮมเพจ แฟนเพจ ที่เป็นของหน่วยงาน อาทิเช่น
    - ข้อความไม่สุภาพ
    - ข้อมูลที่ขัดต่อพระราชบัญญัติลิขสิทธิ์และทรัพย์สินทางปัญญา
    - นำ เสนอภาพ ลามก อนาจาร
    - ลงโฆษณาหรือข้อมูลทางด้านการค้า
    - นำ เสนอภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของไทย
    - ล่วงละเมิดสิทธิของผู้อื่น
7. ก่อความวุ่นวายที่ขัดต่อกฎระเบียบนี้ หรือสร้างความเดือดร้อน รบกวนการทำงานของผู้ใช้อื่นในระบบเครือข่ายกรม
8. ละเมิดกฎระเบียบขั้นต้น ซ้ำมากกว่า 1 ครั้งโดยเจตนา

ส่วนที่ 2 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information security awareness, education and training)

ข้อ 1. ทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

ข้อ 2. สื่อสารนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร อย่างน้อย ปีละ 1 ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ

ข้อ 3. ติดประกาศประชาสัมพันธ์ แจ้งเวียน และเผยแพร่ทางเว็บไซต์หรือสื่อสังคมออนไลน์ เพื่อให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้ให้เป็นปัจจุบันอยู่เสมอ

ข้อ 4. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล การใช้งานของผู้ใช้งาน และสำรวจความต้องการของผู้ใช้งาน

ข้อ 5. ส่งเสริมให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ และให้รับทราบถึงขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

ข้อ 6. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของกรมวิทยาศาสตร์การแพทย์และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ส่วนที่ 3 การปฏิบัติงานจากระยะไกล(Remote working)

ข้อ 1. หากจำเป็นต้องปฏิบัติงานจากระยะไกลต้อง ขอสิทธิ์เข้าใช้งานระบบเครือข่ายเสมือนสำหรับทำงานจากระยะไกล (Virtual Private Network:VPN) โดยผ่านความเห็นชอบของหัวหน้าหน่วยงาน และได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย ต้องตรวจสอบอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัสและการใช้งาน ไฟร์วอลล์ (Firewall) ตามที่หน่วยงานกำหนดหรือไม่

ข้อ 2. ต้องมีการจัดเตรียมอุปกรณ์สำหรับ การจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Logs) จากการปฏิบัติงานจากระยะไกล

ข้อ 3. ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ 4. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

ข้อ 5. ไม่อนุญาตให้ใช้งานโปรแกรมประเภท Remote Desktop เช่น TeamViewer เพื่อเข้าใช้งาน Teleworking เข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของกรม กรณีจำเป็นต้องใช้อุปกรณ์ส่วนตัวให้ทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงานและได้รับอนุญาตจากผู้ดูแลระบบ ทั้งนี้ หากเกิดความเสียหายจากการใช้งานโปรแกรมดังกล่าวให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้น รวมทั้งหัวหน้าหน่วยงานต้องรับผิดชอบในความเสียหายที่เกิดขึ้นร่วมกัน

ข้อ 6. ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่าง ๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ 7. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ 4 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)

ข้อ 1. ระบบป้องกันผู้บุกรุก

ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีแอดเดรสของเครือข่ายที่เป็นผู้โจมตี

ข้อ 2. ระบบไฟร์วอลล์ (Firewall)

(1) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ 1 ครั้ง

(2) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพีแอดเดรส ของเครือข่ายใดถูก Block เป็นจำนวนมาก

(3) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งต่อผู้บริหารสูงสุดของหน่วยงานและศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อตัดสินใจดำเนินการแก้ไขปัญหา หรือหากไม่สามารถแก้ไขได้ให้รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือหน่วยงานที่เกี่ยวข้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ข้อ 3. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต ประกอบด้วย มัลแวร์, ไวรัส, หนอนอินเตอร์เน็ต, โทรจัน, สปายแวร์, Backdoor, Rootkit, DDoS Botnet, Spam Mail, Phishing, Snffing, Spam, Hacking, Hacker

(1) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- ภัยคุกคามทางอินเตอร์เน็ตประเภทใดถูกพบเป็นจำนวนมาก
- ภัยคุกคามทางอินเตอร์เน็ตถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งภัยคุกคามทางอินเตอร์เน็ตจากเครือข่ายภายในกรมวิทยาศาสตร์การแพทย์ไปยังภายนอกหรือไม่

(2) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดภัยคุกคามทางอินเตอร์เน็ตที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของกรมวิทยาศาสตร์การแพทย์

(3) **<u>หาก</u>**ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดภัยคุกคามทางอินเตอร์เน็ตหรือส่งออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดภัยคุกคามทางอินเตอร์เน็ตกับระบบเครือข่าย**<u>ทันที</u>** แล้วทำการแก้ไข**<u>ต่อไป</u>**

(4) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคาม หรือได้รับผลกระทบจากภัยคุกคามทางอินเตอร์เน็ต

(5) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางอินเตอร์เน็ต

(6) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางอินเตอร์เน็ต หรือถูกใช้เพื่อค้นหาข้อมูลใดๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

(7) ตรวจสอบหรือวิเคราะห์คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใดๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางอินเตอร์เน็ต และแจ้งผลการตรวจสอบแก่เจ้าของกรรมสิทธิ์หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์

หมวดที่ 3

นโยบายและมาตรการทางกายภาพ (Physical controls)

วัตถุประสงค์

1. เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การสร้างความเสียหาย และการแทรกแซงต่อข้อมูลของหน่วยงานและทรัพย์สินอื่นที่เกี่ยวข้อง

2. เพื่อให้มั่นใจว่าการเข้าถึงทางกายภาพต่อข้อมูลของหน่วยงานและทรัพย์สินอื่นที่เกี่ยวข้องจะเกิดขึ้นเฉพาะในกรณีที่ได้รับอนุญาตเท่านั้น

3.เพื่อป้องกันหรือบรรเทาผลกระทบที่เกิดจากเหตุการณ์ซึ่งมีสาเหตุมาจากภัยคุกคามทางกายภาพและสิ่งแวดล้อม

แนวปฏิบัติ

ส่วนที่ 1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

ข้อ 1. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ 2. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

(1) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตาม ความสำคัญแล้วแต่กรณี

(2) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก

(3) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(4) จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(5) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจากบริเวณดังกล่าว

(6) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

(7) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ 3. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(1) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

(2) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)

ส่วนที่ 2 การควบคุมการเข้าออกทางกายภาพ (Physical entry)

ข้อที่ 1. การควบคุมการเข้าออก อาคารสถานที่

(1) กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(2) การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitors)

(3) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

(4) ผู้มาติดต่อ/บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

(5) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(6) ดูแลผู้มาติดต่อในพื้นที่ที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(7) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(8) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(9) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(10) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(11) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น หรือจดบันทึกข้อมูลผู้เข้าออก เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

(12) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

ข้อ 2. มาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

(1) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor) แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร **“บันทึกการเข้าออกพื้นที่”**

(2) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร **“บันทึกการเข้าออกพื้นที่”** ให้ถูกต้องชัดเจน

(3) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มการขออนุญาตเข้าออกเป็นประจำทุกเดือน

ส่วนที่ 3 ระบบสาธารณูปโภคสนับสนุน (Supporting utilities)

ข้อ 1. ควรมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

ข้อ 2. ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยเดือนละ 1 ครั้ง เพื่อมั่นใจว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

ข้อ 3. ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่ายเมื่อมีการทำงานผิดปกติหรือหยุดการทำงาน

ข้อ 4. ระบบปรับสภาพอากาศ

(1) ผู้ดูแลห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่ายต้องรักษาอุณหภูมิของห้องให้อยู่ในช่วง 20 ^{O}C ถึง 25 ^{O}C และเฝ้าดูแลความชื้นสัมพัทธ์ระหว่าง 40% ถึง 55%

(2) หากพบความผิดปกติของอุณภูมิ ต้องมีการแจ้งเตือนในระบบเฝ้าระวังของกรมและแจ้งเตือนผ่านอีเมลของผู้ดูแลระบบ(SysAdmin)

ข้อ 5. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security) ควรปฏิบัติดังนี้

(1) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(2) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(3) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(4) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(5) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(6) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(7) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

(8) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับ สัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ 6. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(1) กำหนดให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(2) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(3) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(4) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและ

ปรับปรุงอุปกรณ์ดังกล่าว

(5) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(6) ตรวจสอบการแจ้งเตือนเมื่อถึงรอบการบำรุงรักษาของอุปกรณ์

(7) กำหนดและอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่เข้ามาบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ 7. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

(1) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

(2) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(3) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(4) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ 8. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

(1) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(2) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(3) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ 9. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

(1) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(2) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ส่วนที่ 4 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

ข้อ 1. พื้นที่ห้อง Server ต้องมีอุปกรณ์ป้องกันการเข้าถึง โดยไม่ได้รับอนุญาต หรือล๊อคประตู มีการบันทึกเหตุการณ์ในการเข้าห้อง Server โดยอุปกรณ์อิเล็กทรอนิกส์ หรือแบบฟอร์มบันทึก

ข้อ 2. ห้ามสูบบุหรี่ ภายในห้อง Data Center

ข้อ 3.ห้ามนำอาหารและเครื่องดื่ม เข้าไปในห้อง Data Center

ข้อ 4.ห้ามนำอุปกรณ์ที่บันทึกรูปภาพ วิดีทัศน์หรือเสียง และสื่อบันทึกชนิดเคลื่อนที่เข้าไปภายในห้อง Data Center เว้นแต่ได้รับอนุมัติจากผู้รับผิดชอบพื้นที่หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่เท่านั้น

ส่วนที่ 5 โต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์(Clear desk and clear screen)

ข้อ 1. พื้นที่โต๊ะทำงานต้องไม่วางเอกสารที่มีข้อมูลสำคัญ เช่น ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ ไว้ให้สามารถมองเห็นโดยง่าย

ข้อ 2. เมื่อไม่เมื่อไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง และปฏิบัติตามนโยบายในหมวดที่ 1 ส่วนที่ 6 ข้อที่ 18 อย่างเคร่งครัด

ข้อ 3. ผู้ใช้งานต้องจัดเรียงไฟล์ข้อมูลภายในเครื่องคอมพิวเตอร์ให้เป็นระเบียบจัดเก็ บ ในโฟลเดอร์ (Folder) และง่ายต่อการค้นหา

ข้อ 4. ก่อนการใช้งานสื่อบันทึกข้อมลูชนิดพกพาต่างๆ ต้องตรวจสอบเพื่อหาไวรัส โดยโปรแกรมป้องกันไวรัส และไม่อนุญาตให้ทำสำเนาข้อมูลที่เป็นความลับ มีความสำคัญออกไปใช้ภายนอกกรม กรณีใช้ภายในกรม เมื่อใช้งานเรียบร้อยแล้วต้องลบไฟล์บนสื่อบันทึกพกพาต่างๆ แบบถาวร (Shift+Delete) หรือ Format ทันที

หมวดที่ 4

นโยบายและมาตรการรทางเทคโนโลยี(Technological controls)

วัตถุประสงค์

1. เพื่อปกป้องข้อมูลจากความเสี่ยงที่เกิดจากการใช้งานอุปกรณ์ปลายทางของผู้ใช้

2. เพื่อป้องกันการนำฟังก์ชันที่ไม่ได้รับอนุญาตเข้าสู่ระบบ หลีกเลี่ยงการเปลี่ยนแปลงโดยไม่ตั้งใจหรือโดยประสงค์ร้าย และรักษาความลับของทรัพย์สินที่มีมูลค่า

3. เพื่อให้การพัฒนา หรือการจัดหาโปรแกรมประยุกต์มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ส่วนที่ 1 อุปกรณ์ปลายทางของผู้ใช้งาน (User end point devices)

การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ 1. แนวทางปฏิบัติการใช้งานทั่วไป

(1) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการเท่านั้น

(2) โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(3) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(4) การเคลื่อนย้ายเครื่องคอมพิวเตอร์ส่วนบุคคลไปติดตั้ง ณ สถานที่อื่นใดภายในกรม ต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมายหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับกรม

(5) ในการส่งซ่อมเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องได้รับความเห็นชอบจากผู้ดูแลระบบของหน่วยงานและได้รับอนุญาตจากหัวหน้าหน่วยงานก่อน โดยปฏิบัติให้สอดคล้องกับประกาศกรม เรื่อง นโยบายและแนวปฏิบัติการใช้งานคอมพิวเตอร์ที่ถูกต้องตามกฎหมาย

(6) ก่อนการใช้งานสื่อบันทึกข้อมลูชนิดพกพาต่างๆ ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส และไม่อนุญาตให้ทำสำเนาข้อมูลที่เป็นความลับมีความสำคัญออกไปใช้ภายนอกกรม กรณีใช้ภายในกรม เมื่อใช้งานเรียบร้อยแล้วต้องลบไฟล์บนสื่อบันทึกพกพาต่างๆ แบบถาวร (Shift+Delete) หรือ Format ทันที

(7) ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(8) ผู้ใช้งานต้องตรวจสอบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ และทำการตรวจสอบจัดเรียงข้อมูลภายในฮาร์ดดิสก์ (Defragment) ของเครื่องคอมพิวเตอร์อย่างน้อย เดือนละ 1 ครั้ง เพื่อเพิ่มประสิทธิภาพในการทำงาน

(9) ผู้ใช้งานต้องจัดเรียงไฟล์ข้อมูลภายในเครื่องคอมพิวเตอร์ให้เป็นระเบียบจัดเก็บ ในโฟลเดอร์ (Folder) และง่ายต่อการค้นหา

(10) ข้อมูลสำคัญหรือความลับที่พิมพ์ออกมาเป็นเอกสารจะต้องจัดเก็บให้มิดชิดให้ไม่สามารถเข้าถึงได้โดยผู้ไม่มีสิทธิเข้าถึง หรือทำลายเมื่อไม่ใช้งานแล้ว

(11) การส่งต่อข้อมูลสำคัญที่เป็นความลับต้องถูกปิดผนึก และประทับตราชั้น

(12) ความลับตามระเบียบงานสารบรรณเมื่อส่งให้ผู้รับจะต้องอยู่ในสภาพที่ปิดผนึกไม่ถูกฉีกขาด

(13) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น

(14) ผู้ใช้งาน ต้องตั้งค่าการใช้งานระบบปฏิบัติการให้อยู่ในโหมดประหยัดพลังงาน (Power saver mode) และให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่านก่อนเข้าใช้งานทุกครั้ง

(15) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งานหรือได้รับอนุญาตจากหัวหน้าหน่วยงาน หากมีการตรวจสอบพบความเสียหายต่อหน่วยงาน ถือว่าเป็นความผิด หัวหน้าหน่วยงานและผู้ใช้งานจะต้องรับผิดชอบร่วมกัน

ข้อ 2. การใช้รหัสผ่าน ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

ข้อ 3. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(1) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(2) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (Email) หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

(3) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่ กำหนดไว้

ข้อ 4. ติดตั้งโปรแกรมการป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention) ของกรมวิทยาศาสตร์การแพทย์

ข้อ 5. การสำรองข้อมูลและการกู้คืน

(1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(3) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บนฮาร์ดดิสก์ (Hard Disk) ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหากฮาร์ดดิสก์ (Hard Disk) เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

การใช้งานเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารชนิดพกพา (Mobile device)

ข้อ 6. แนวทางปฏิบัติการใช้งานทั่วไป

(1) เครื่องคอมพิวเตอร์แบบพกพาที่จัดหาโดยหน่วยงานราชการ เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการเท่านั้น

(2) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่มีลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรม

ต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(3) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(4) ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์แบบพกพาและรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(5) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(6) หลีกเลี่ยงการใช้ของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ ให้เป็นรอยขีดข่วนหรือทำให้จอของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(7) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(8) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(9) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(10) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้ แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

(11) ห้ามนำเครื่องคอมพิวเตอร์แบบพกพาส่วนตัวมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งานหรือได้รับอนุญาตจากหัวหน้าหน่วยงาน <u>หากมีการตรวจสอบพบความเสียหายต่อหน่วยงาน ถือว่าเป็นความผิดหัวหน้าหน่วยงานและผู้ใช้งานจะต้องรับผิดชอบร่วมกัน</u> รวมถึงการส่งข้อมูลผ่านทางผู้ให้บริการขนส่งที่น่าเชื่อถือ

(12) การนำอุปกรณ์สื่อบันทึกข้อมูลชนิดพกพา เช่น USB Flash Drive, External Hardisk มาใช้ในการปฏิบัติงานร่วมกับเครื่องคอมพิวเตอร์ลูกข่ายจะต้องทำการตรวจสอบไวรัสคอมพิวเตอร์ทุกครั้ง และผู้ใช้งานต้องไม่ทำการสำเนาข้อมูลที่เป็นความลับของกรมลงบนอุปกรณ์สื่อบันทึกข้อมูลชนิดพกพาทุกประเภทเพื่อนำออกไปใช้นอกกรม กรณีเป็นการดำเนินการภายในหน่วยงานเมื่อใช้งานเรียบร้อยแล้วให้ลบข้อมูลนั้นออกจากสื่อบันทึกข้อมูลแบบถาวร (Shift+delete) หรือ ฟอร์แมต (format) ทันที

(13) ไม่อนุญาตให้นำอุปกรณ์สื่อบันทึกข้อมูลชนิดพกพาทุกชนิด เช่น USB Flash Drive, External Hardisk มาใช้ในการปฏิบัติงานร่วมกับเครื่องคอมพิวเตอร์แม่ข่ายหากมีความจำเป็นจะต้องได้รับการอนุญาตจากผู้ดูแลระบบ (System Admin) ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานก่อนดำเนินการ และจะต้องทำการตรวจสอบไวรัสคอมพิวเตอร์ทุกครั้งและผู้ใช้งานต้องไม่ทำการสำเนาข้อมูลที่เป็นความลับของกรมลงบนอุปกรณ์สื่อบันทึกข้อมูลชนิดพกพาทุกประเภทเพื่อนำออกไปใช้นอกกรม กรณีเป็นการดำเนินการภายในหน่วยงานเมื่อใช้งานเรียบร้อยแล้วให้ลบข้อมูลนั้นออกจากสื่อบันทึกข้อมูลแบบถาวร (Shift+delete) หรือ ฟอร์แมต (format) ทันที

(14) การนำอุปกรณ์พกพาที่เป็นทรัพย์สินส่วนตัวเข้ามาใช้ร่วมกับระบบเครือข่ายคอมพิวเตอร์ไร้สายของกรม เช่น โน้ตบุ้ค โทรศัพท์มือถือ ต้องลงโปรแกรมป้องกันไวรัสคอมพิวเตอร์และต้องมีการลงชื่อเข้าใช้งานเพื่อยืนยันตัวบุคคลทุกครั้ง

(15) กรณีนำอุปกรณ์พกพาที่เป็นทรัพย์สินส่วนตัวเข้ามาใช้ร่วมกับระบบเครือข่ายคอมพิวเตอร์ชนิดใช้สายต้องดำเนินการตาม ส่วนที่ 5 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ 7. ความปลอดภัยทางด้านกายภาพ

(1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล๊อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(2) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อ 8. การควบคุมการเข้าถึงระบบปฏิบัติการ

(1) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(2) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในข้อที่ 14 “การใช้งานรหัสผ่าน”

(3) ผู้ใช้งานต้องตั้งการใช้งานระบบปฏิบัติการให้อยู่ในโหมดประหยัดพลังงาน (Power saver mode) และให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(4) ผู้ใช้งานต้องทำการออกจากระบบ (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ 9. การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

ข้อ 5. การสำรองข้อมูลและการกู้คืน

(1) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

(2) ผู้ใช้งานต้องเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

(3) แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(4) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

(5) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ต้องไม่เป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียหายจะไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ 2 การจำกัดการเข้าถึงซอร์สโค้ด (Access to source code)

ข้อ 1. จำกัดให้เฉพาะผู้ดูแลระบบที่ได้รับการมอบหมายจากหัวหน้าหน่วยงานเป็นผู้เข้าถึง ซอร์สโค้ด เท่านั้น

ข้อ 2. จำกัดการเข้าถึงซอร์สโค้ด (Source Code) ของระบบงาน หลีกเลี่ยงการติดตั้งซอร์สโค้ดของระบบงานบนเครื่องให้บริการ (ยกเว้นในกรณีที่ระบบงานต้องเรียกใช้โดยตรงในขณะที่ทำงาน)

ส่วนที่ 3 การป้องกันจากโปรแกรมไม่ประสงค์ดี (Protection against malware)

ข้อ 1. คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่หน่วยงานได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา ทดลอง โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ 2. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 3. ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ 4. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ 5. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ 6. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นสินทรัพย์ของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ 7. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของหน่วยงาน สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการดังนี้

(1) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(2) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญ ในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(3) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(4) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่ทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(5) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจ บนเครือข่ายคอมพิวเตอร์

ส่วนที่ 4. การบริหารจัดการการตั้งค่าระบบ(Configuration Management)

ข้อ 1. การปรับปรุงระบบปฏิบัติการ (Operating System Update)

(1) ติดตั้งระบบปฏิบัติการให้ตรงกับความต้องการใช้งาน

(2) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบและชื่อผู้ใช้งาน (User)

(3) กำหนดชื่อเครื่อง (Computer Name) และตั้งค่า IP Address ตามการใช้งาน

(4) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

(5) กรณีที่ระบบปฏิบัติการที่มี Service Patch Update ให้ตรวจสอบหรือปรับปรุงการกำหนดค่าต่างๆ โดยเฉพาะระดับความปลอดภัยของระบบปฏิบัติการ

ข้อ 2. การบริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management)

(1) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)

(2) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

(3) บันทึกบัญชีผู้ใช้งานและทบทวนสิทธิ์การเข้าใช้ระบบให้เป็นปัจจุบันและสอดคล้องกับหน้าที่ความรับผิดชอบ

ข้อ 3. ระบบรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการปรับปรุงการป้องกันไวรัส (System Security & Antivirus Update)

(1) ติดตั้งโปรแกรม Antivirus และปรับปรุงฐานข้อมูลไวรัส (virus definition) ให้ทันสมัยอยู่เสมอ และกำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม รวททั้งScan ตรวจหาไวรัสคอมพิวเตอร์เป็นประจำ

(2) ตรวจสอบประสิทธิภาพของระบบคอมพิวเตอร์ จากระบบรักษาความปลอดภัยที่ติดตั้ง

(3) ปรับปรุง / กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา

ข้อ 4. การดำเนินการบริหารจัดการฐานข้อมูล (Database Management Operation)

(1) ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่หน่วยงานใช้

(2) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูลให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง และมีประสิทธิภาพตามระบบฐานข้อมูลนั้นกำหนด

(3) สร้างรายชื่อผู้ดูแลระบบฐานข้อมูล (Database Administrator) ชื่อผู้ใช้งาน (User) อื่นและกำหนดสิทธิ์การเข้าใช้งาน

(4) ปรับปรุงและกำหนดค่าระบบให้เหมาะสมทันสมัยอยู่เสมอ เพื่อป้องกันการเกิดปัญหา

ข้อ 5. ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่างๆ กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

(1) ติดตั้งโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา

(2) กำหนดค่า services ต่างๆ ให้ทำงานร่วมกับระบบปฏิบัติการ อย่างถูกต้องและมีประสิทธิภาพ

(3) ติดตั้งฐานข้อมูล เชื่อมต่อระบบงาน และทดสอบการให้บริการ ตามที่ระบบงานกำหนด

(4) แจ้งผู้ใช้งาน หรือเจ้าของระบบงานให้สามารถเริ่มใช้งานได้โดยแจ้งรายชื่อ รหัสผ่าน และสิทธิ์การเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้

(5) กำหนดเกณฑ์การสำรอง สำเนา และทดสอบกู้คืน (Restore Test)

(6) บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้างหรือปรับปรุง

(7) กำหนดการจัดเก็บ Event Log ตามหลัก Security Baseline การใช้ระบบงานสารสนเทศสำหรับผู้ดูแลระบบ ซึ่งต้องสามารถค้นหาและตรวจสอบได้ ประกอบด้วย ชื่อผู้ใช้งาน หมายเลขไอพีแอดเดรส รายละเอียดการใช้งาน (ดู เพิ่ม แก้ไข ลบ พิมพ์ อัพโหลด ข้อมูลและไฟล์ต่างๆ) วันเวลาเดือนปีที่ดำเนินการ เป็นต้น

ส่วนที่ 5. การบันทึกข้อมูลล็อก (Logging)

ข้อ 1. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

ข้อ 2. ห้ามแก้ไขข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ 3. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ 4. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ 5. กำหนดการตั้งค่าอุปกรณ์เครือข่ายคอมพิวเตอร์ และเครื่องคอมพิวเตอร์แม่ข่ายไปที่ (Network Time Server : NTP) ของกรม โดยผู้ดูแลระบบต้องดำเนินการตั้งค่าให้ตรงกับสถาบันมาตรวิทยาแห่งชาติ และผู้ดูแลระบบตรวจสอบความแม่นยำเป็นประจำทุกเดือน

ส่วนที่ 6. การลบข้อมูล (Information deletion)

ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การตัด ฉีก หรือตัดด้วยเครื่องทำลายเอกสาร
Flash Drive	ให้ Format และใช้วิธีการขูดขีด ทุบหรือบดให้เสียหาย หรือใช้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน **DOD 5220.22 M** ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ
แผ่น CD/DVD	ใช้การตัด หรือตัดด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีการขูดขีด ทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ให้ Format และใช้วิธีการขูดขีด ทุบหรือบดให้เสียหาย หรือใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน **DOD 5220.22 M** ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ

ส่วนที่ 7 การจำกัดการเข้าถึงข้อมูล (Information access restriction)

ข้อ 1. กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

(1) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

(2) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

(2.1) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่ ดูข้อมูล สร้างข้อมูล แก้ไขข้อมูล ลบข้อมูล นำเข้าข้อมูล ส่งออกข้อมูล เป็นต้น

(2.2) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(2.3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(3) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูลตามการจัดแบ่งประเภทของข้อมูล ระดับความสำคัญของข้อมูล และระดับชั้นความลับ ตามหมวดที่ 1 โดยจัดแบ่งระดับชั้นการเข้าถึงดังนี้

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(4) การกำหนดจำนวนช่องทางที่สามารถเข้าถึงได้ ได้แก่ Intranet หรือ Internet หรือเครือข่าย GIN เป็นต้น

ข้อ 2. ข้อมูล ข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่นๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ 3. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. 2544 และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ 4. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใดๆ กับข้อมูลนั้นได้ตามสิทธิ์และจัดให้มีแฟ้มบันทึกเข้าออก (Log File) ได้แก่ ชื่อบัญชีผู้ใช้งาน ฟังก์ชันงาน หมายเลขไอพีแอดเดรส วันเดือนปีเวลาที่กระทำการ เป็นต้น) สำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ 5. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือบันทึกข้อความสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงานภายนอก ดังต่อไปนี้

(1) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่มีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

(2) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกันหรือแลกเปลี่ยนข้อมูล ได้แก่ วิธีการส่ง การรับ การแก้ไข การลบ เป็นต้น

(3) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

(4) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ

(5) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่นๆ กับข้อมูลนั้น

(6) กำหนดสิทธิ์การเข้าถึงข้อมูล

(7) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

(8) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่นๆ ที่มีความสำคัญ ได้แก่ กุญแจที่ใช้ในการเข้ารหัส (CA : Certificate Authority) จากหน่วยที่ได้การรับรอง เป็นต้น

ส่วนที่ 8 การคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ

โดยที่การดำเนินการของกรมวิทยาศาสตร์การแพทย์ ซึ่งมีอำนาจหน้าที่ ตรวจวิเคราะห์ทางห้องปฏิบัติการเพื่อควบคุมคุณภาพ ประสิทธิภาพและมาตรฐานให้เป็นไปตามกฎหมายและสนับสนุนป้องกันและควบคุมโรค จำเป็นต้องมีการจัดเก็บข้อมูลส่วนบุคคลของบุคคลผู้ติดต่อราชการและบางกรณีมีความจำเป็นต้องดำเนินการทางอิเล็กทรอนิกส์ เพื่อให้สามารถบริการประชาชนได้อย่างมีประสิทธิภาพ

ดังนั้น เพื่อให้มีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการของกรมวิทยาศาสตร์การแพทย์ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงมีแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ดังนี้

ข้อ 1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

กรมวิทยาศาสตร์การแพทย์จะจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการไว้เท่าที่จำเป็น และเป็นการจัดเก็บข้อมูลจากเจ้าของข้อมูลโดยตรง ภายใต้อำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของกรมวิทยาศาสตร์การแพทย์ตามที่กฎหมายกำหนด หรือรับรองตามมาตรา ๒๔ แห่งพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ.๒๕๔๐ เท่านั้น ในกรณีที่กรมวิทยาศาสตร์การแพทย์ประสงค์ใช้ข้อมูลส่วนบุคคลของผู้ใช้บริการเพื่อวัตถุประสงค์อื่น กรมวิทยาศาสตร์การแพทย์จะแจ้งความประสงค์ให้ผู้ใช้บริการทราบและขอความยินยอมจากผู้ใช้บริการก่อน เว้นแต่เป็นกรณีที่กฎหมายกำหนด หรือในกรณี อื่น ๆ ตามที่กำหนดไว้ในนโยบายฉบับนี้

ข้อ 2. คุณภาพของข้อมูลส่วนบุคคล

กรมวิทยาศาสตร์การแพทย์มีการรวมรวมและจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการ ทั้งทางด้านเอกสาร และธุรกรรมทางอิเล็กทรอนิกส์โดยข้อมูลที่จัดเก็บ กรมวิทยาศาสตร์การแพทย์จะให้ความสำคัญถึงความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

ข้อ 3. การระบุวัตถุประสงค์ ในการรวบรวมและจัดเก็บข้อมูล

กรมวิทยาศาสตร์การแพทย์ มีการรวบรวม จัดเก็บ ใช้ ข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยมีวัตถุประสงค์เพื่อให้บริการ ด้านการตรวจวิเคราะห์ การขึ้นทะเบียนครอบครองเชื้อโรคและพิษจากสัตว์ การรับเรื่องร้องเรียน เป็นต้น ทั้งนี้ หากภายหลังกรมวิทยาศาสตร์การแพทย์มีการเปลี่ยนแปลงวัตถุประสงค์ในการรวบรวมและจัดเก็บข้อมูลส่วนบุคคล กรมวิทยาศาสตร์การแพทย์จะแจ้งให้ผู้ใช้บริการทราบและขอความยินยอม นอกจากนี้ กรมวิทยาศาสตร์การแพทย์ได้กำหนดให้มีการบันทึกการแก้ไขเพิ่มเติมไว้เป็นหลักฐานด้วย

ข้อ 4. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

กรมวิทยาศาสตร์การแพทย์จะไม่เปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์นอกเหนือจากวัตถุประสงค์ในการรวบรวมและจัดเก็บข้อมูล เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูล หรือตามคำสั่งศาล หรือเป็นกรณีเปิดเผยตามที่กฎหมายกำหนดให้กระทำได้และกำหนดให้ ผู้รับจ้าง (outsource) ต้องเก็บรักษาความลับและความปลอดภัยของข้อมูลของผู้ใช้บริการโดยห้ามนำข้อมูลไปใช้นอกเหนือจากที่กำหนดให้ดำเนินการ

ข้อ 5. การรักษาความมั่นคงปลอดภัย

กรมวิทยาศาสตร์การแพทย์มีมาตรการในการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลของผู้ใช้บริการทั้งด้านเอกสารและธรุกรรมทางอิเล็กทรอนิกส์ เพื่อป้องกันมิให้ข้อมูลสูญหาย การเข้าถึง การใช้ข้อมูล การทำลายข้อมูล และการนำข้อมูลไปใช้โดยมิชอบ รวมถึงการเปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยเป็นไปตามประกาศกรมวิทยาศาสตร์การแพทย์ เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ 6. การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล

กรมวิทยาศาสตร์การแพทย์มีการดำนเนินการตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล โดยจะเปิดเผยและเผยแพร่ผ่านทางเว็บไซต์ https://pdpa.dmsc.moph.go.th/

ทั้งนี้ กรมวิทยาศาสตร์การแพทย์มีช่องทางให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจดูความมีอยู่ ลักษณะของข้อมูลส่วนบุคคล วัตถุประสงค์ของการนำข้อมูลไปใช้ ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคลได้ที่ E-mail : dpo@dmsc.mail.go.th หรือ ณ กรมวิทยาศาสตร์การแพทย์ เลขที่ ๘๘/๗ ซอยบำราศนราดูร ถ.ติวานนท์ ต.ตลาดขวัญ อ.เมือง จ.นนทบุรี ๑๑๐๐๐ โทร ๐ ๒๙๕๑ ๑๐๐๐ และศูนย์วิทยาศาสตร์การแพทย์ทั้ง ๑๕ แห่ง

ข้อ 7. การมีส่วนร่วมของเจ้าของข้อมูล

กรมวิทยาศาสตร์การแพทย์จะเปิดเผยรายละเอียดข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลต่อเมื่อได้รับคำร้องขอจากเจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท หรือผู้แทนโดยชอบธรรม ผู้พิทักษ์ตามกฎหมาย ผู้อนุบาล โดยยื่นคำร้องขอและวัตถุประสงค์ของการนำไปใช้ ได้ที่ E-mail : dpo@dmsc.mail.go.th หรือ ณ กรมวิทยาศาสตร์การแพทย์ เลขที่ ๘๘/๗ ซอยบำราศนราดูร ถ.ติวานนท์ ต.ตลาดขวัญ อ.เมือง จ.นนทบุรี ๑๑๐๐๐ โทร ๐ ๒๙๕๑ ๑๐๐๐ และศูนย์วิทยาศาสตร์การแพทย์ทั้ง ๑๕ แห่ง

ทั้งนี้กรมวิทยาศาสตร์การแพทย์จะดำเนินการให้แล้วเสร็จภายใน ๓๐ วัน นับแต่วันที่ได้รับคำร้องในกรณีที่เจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท หรือผู้แทนโดยชอบธรรม ผู้พิทักษ์ตามกฎหมาย ผู้อนุบาล มีการคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใด ๆ เช่น การแจ้งปรับปรุงแก้ไขข้อมูลส่วนบุคคล หรือลบข้อมูลส่วนบุคคล เป็นต้น หลังจากกรมวิทยาศาสตร์การแพทย์ได้ตรวจสอบหลักฐานที่เชื่อถือได้ซึ่งเจ้าของข้อมูลได้แสดงต่อกรมวิทยาศาสตร์การแพทย์แล้ว จะบันทึกคำคัดค้านเพื่อเก็บไว้เป็นหลักฐานด้วย ทั้งนี้ กรณีที่กรมวิทยาศาสตร์การแพทย์ปฏิเสธการให้ข้อมูลส่วนบุคคลใด ๆ กรมการขนส่งทางบก จะจัดทำคำชี้แจ้งให้เจ้าของข้อมูลทราบ

ข้อ 8. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูลส่วนบุคคล

กรมวิทยาศาสตร์การแพทย์กำหนดให้เจ้าหน้าที่ทุกคนที่จัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการ ต้องให้ความสำคัญและรับผิดชอบในการจัดเก็บและคุ้มครองข้อมูลส่วนบุคคลที่ตนจัดเก็บตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้อย่างเคร่งครัด

ส่วนที่ 9 การสำรองข้อมูล (Information backup)

ข้อ 1. พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ 2. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ 3. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง รวมทั้งจัดทำและทบทวนแผนป้องกันและแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

ข้อ 4. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้นโดยให้มีวิธีการสำรองข้อมูล ดังนี้

(2) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(3) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

(4) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

(5) ตรวจสอบค่าการตั้งค่า (Configuration) ต่างๆ ของระบบการสำรองข้อมูล

(6) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(7) ควรจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

(8) ควรดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(9) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(10) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(11) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น

(12) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ 5. ต้องจัดทำแผนบริหารความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศของกรม เพื่อให้สามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง โดย

(1) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(2) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว โรคระบาด การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(3) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(4) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(5)มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(6)มีการสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ 6. ทบทวนและปรับปรุงแผนบริหารความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ กรมวิทยาศาสตร์การแพทย์ กระทรวงสาธารณสุข ให้มีความเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจอย่างน้อยปีละ 1 ครั้ง

ข้อ 7. ต้องซ้อมแผนบริหารความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ส่วนที่ 10 ความมั่นคงปลอดภัยของเครือข่าย (Networks security)

ข้อ 1. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของหน่วยงาน ต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงานและได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับการมอบหมาย

ข้อ 2. การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ ต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงานและได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับการมอบหมาย โดยต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่นๆ

ข้อ 3. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 4. ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(1) จำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(2) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(3) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(4) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware) ด้วย

(5) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

(6) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเตอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(7) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายของหน่วยงาน

(8) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(9) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบ ต้องบันทึกบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์เชื่อมต่อจากเครือข่ายภายนอก ต้องกำหนดสิทธิ์การเข้าใช้งาน และระยะเวลาในการเชื่อมต่อ ภายหลังจากได้รับเอกสารอนุญาตจากหัวหน้าหน่วยงาน
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ 5. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ 6. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุญาตจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

ข้อ 7. กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบรารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบงาน ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ 8. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550 และแก้ไขเพิ่มเติม พ.ศ. 2560

ข้อ 9. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

(1) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงาน ต้องขออนุญาตจากหัวหน้าหน่วยงาน เป็นลายลักษณ์อักษร หรือสมัครใช้งานจากระบบที่กรมจัดไว้ให้ก่อนการใช้งาน

(2) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(3) วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

(4) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(5) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ 10. หน่วยงาน ควรติดตั้งระบบตรวจสอบการบุกรุก**(Intrusion Detection System / Intrusion Prevention System: IDS/IPS)** และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ

และข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ 11. หน่วยงาน ควรติดตั้ง IDS/IPS ให้ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงาน และระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเตอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ 12. ระบบทั้งหมดใน DMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ 13. โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ 14. ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

ข้อ 15. ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำโดยผู้ดูแลระบบ

ข้อ 16. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ ไฟร์วอลล์ (Firewall) ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ 17. เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ 18. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ต้องมีการรายงานให้หัวหน้าหน่วยงานทราบทันทีที่ตรวจพบพฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ต้องมีการรายงานให้หัวหน้าหน่วยงานทราบ ภายใน 1 ชั่วโมงที่ตรวจพบ

ข้อ 19. การตรวจสอบการบุกรุกทั้งหมด ต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

ข้อ 20. ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ 21. หน่วยงานมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องแจ้งผู้ใช้งานล่วงหน้า

ข้อ 22. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของกรม โดยการพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ข้อ 23. หน่วยงานต้องมีการตั้งค่าระบบในการการคัดกรองเว็บ (Web filtering) ไม่พึงประสงค์ อันตราย อันจะก่อให้เกิดความเสื่อมเสีย หรือเสียหายต่อระบบของกรม

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ 24. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานของระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ 25. ผู้ดูแลระบบต้องทำการเปลี่ยนค่าอุปกรณ์เครือข่ายที่มาจากโรงงานให้เป็นค่าที่ได้รับจัดสรรจากกรม

ข้อ 26. ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WPA (Wi-Fi Protected

Access) หรือ WPA2 (Wi-Fi Protected Access2) เป็นอย่างน้อย ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)

ข้อ 27. ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) หรือกำหนดชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย

ข้อ 28. ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ 29. ผู้ดูแลระบบ ควรแยกการใช้งานระหว่างเครือข่ายภายในและภายนอก เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายจากเครือข่ายไร้สาย

ข้อ 30. ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยในระบบเครือข่ายไร้สาย หากตรวจสอบแล้วพบการใช้งานระบบเครือข่ายไร้สายมีความผิดปกติ ผู้ดูแลระบบต้องรายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อ 31. ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของกรม

ข้อ 32. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรม ต้องลงทะเบียนอุปกรณ์กับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นลายลักษณ์อักษรหรือตามระบบที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจัดเตรียมไว้ให้

ข้อ 33. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมถึงทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ 34. หน่วยงานมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าขอไฟร์วอลล์ (Firewall) ทั้งหมด และการกำหนดค่าเริ่มต้นของไฟร์วอลล์ (Firewall) ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny) ทุกบริการ (Services) รวมไปถึงเส้นทางเชื่อมต่ออินเตอร์เน็ต และเว็บไซต์ ที่ไม่อนุญาต (web filtering) ตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์ (Firewall)

ข้อ 35. ผู้ใช้งานอินเตอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

ข้อ 36. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต ต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่างๆ ของไฟร์วอลล์ (Firewall)

ข้อ 37. การเข้าถึงอุปกรณ์ไฟร์วอลล์ (Firewall) ต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น

ข้อ 38. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ (Firewall) ต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

ข้อ 39. การกำหนดนโยบายในการให้บริการอินเตอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะดำเนินการเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือจากที่กำหนด ต้องทำหนังสือขออนุญาตจากหัวหน้าหน่วยงานและได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมายก่อนทุกครั้ง

ข้อ 40. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

ข้อ 41. ต้องสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์ (Firewall) เป็นประจำทุกสัปดาห์ หรือทุกครั้งก่อนที่มีการเปลี่ยนแปลงค่า

ข้อ 42. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ ภายในหน่วยงาน ที่มีลักษณะที่เป็นอินทราเน็ต (Intranet) ต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเตอร์เน็ต เว้นแต่มีความจำเป็นโดยต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานและได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ 43. ผู้ดูแลระบบมีสิทธิ์ระงับหรือปิดกั้น (Block) การใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมละเมิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข ทั้งนี้ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ (Firewall) จะถูกระงับการใช้งานอินเตอร์เน็ตทันที

ข้อ 44. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายภายใน ต้องขออนุญาตพร้อมระบุเหตุผลเป็นลายลักษณ์อักษร และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานและได้รับการอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมายก่อน

ส่วนที่ 11 การแบ่งแยกเครือข่าย (Segregation in networks)

ข้อ 1. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(1) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(2) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

(3) Dmz zone แบ่งแยกเครือข่ายส่วนของเครื่องคอมพิวเตอร์แม่ข่าย เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

ข้อ 2. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่างๆ เช่น IP Address อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้อง ให้รับทราบทุกครั้ง เป็นลายลักษณ์อักษร

ข้อ 3. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ 4. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง และต้องมีการตั้งค่า Web filtering คัดกรองเว็บไซต์ที่มีเนื้อหาอันตรายขัดต่อศีลธรรม รวมไปถึง ซอฟต์แวร์ที่เป็นอันตรายต่อข้อมูลของกรม

ข้อ 5. IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ข้อ 6. การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่ 12. การใช้การเข้ารหัสข้อมูล (Use of cryptography)

กำหนดนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้ในกรม และต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจ (Key) ที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูล (Encrypt) ที่กำหนด

ข้อ 1. นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls) ต้องมีนโยบายการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง ที่สอดคล้องกับนโยบายของกรม

ข้อ 2. การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management) นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจ (Key) ต้องมีการจัดทำและปฏิบัติตามตลอดอายุการใช้งาน ควรมีการกำหนดมาตรการในการจัดเก็บที่เป็นข้อมูลความลับ ได้แก่ การสร้างกุญแจรหัสลับ การจัดเก็บและดูแลรักษากุญแจรหัสลับ การนำกุญแจรหัสลับไปใช้ การกำหนดอายุของกุญแจรหัสลับ ตลอดจนการทำลายกุญแจรหัสลับเมื่อไม่ได้ใช้งาน

แนวปฏิบัติการเข้ารหัสข้อมูล (Cryptographic)

ข้อ 1. มาตรการการเข้ารหัสข้อมูล (policy on the Use of Cryptographic Controls)

(1) การแปลงรูปแบบของข้อมูลที่รับเข้ามาไม่ว่าขนาดเท่าใดก็ตาม ให้อยู่ในอีกรูปแบบหนึ่งที่มีขนาดคงที่ และไม่สามารถถอดรหัสข้อมูลได้ (Decrypt) ทำได้เพียงตรวจสอบว่าข้อมูลที่ส่งแต่ละครั้งเหมือนกันหรือไม่ ความปลอดภัยจึงค่อนข้างสูง เช่น การเก็บรหัสผ่านผู้ใช้งานในฐานข้อมูล ได้แก่ การใช้ฟังก์ชั่น MD5 หรือ SHA1 เป็นต้น

(2) อัลกอริทึมที่เรียกใช้ต้องรองรับซอฟต์แวร์ประยุกต์ที่นำไปใช้งานได้ เช่น PGP (Pretty Good Privacy), SSL (Secure Socket Layer), TLS (Transport Layer Security) เป็นต้น

(3) ความยาวของคีย์ (Key) ในการเข้ารหัสต้องไม่น้อยกว่า 48 บิต (bit) สำหรับการเข้ารหัสแบบสมมาตร (Symmetric) และแบบไม่สมมาตร (Asymmetric) ต้องมีความยาวไม่น้อยกว่าตามที่ตกลงกันไว้

(4) เจ้าของข้อมูลต้องมีการทบทวนมาตรฐานของคีย์ (Key) ที่เข้ารหัสทุกๆ ปีเพื่อให้สอดคล้องกับความปลอดภัยและประสิทธิภาพของเครื่องคอมพิวเตอร์ลูกข่าย

(5) กรณีที่ไม่ทราบหรือต้องการทราบข้อมูลเกี่ยวกับการเข้ารหัสเพิ่มเติมให้ติดต่อหน่วยงานที่รับผิดชอบ

ข้อ 2. การบริหารจัดการกุญแจ (Key Management)

(1) ข้อมูลที่มีการเข้ารหัส (Encrypt) ต้องจัดให้มีกระบวนการในการบริหารจัดการกุญแจ (Key Management) ที่มีประสิทธิภาพโดยการดำเนินการ เช่น การสร้าง การจัดเก็บ การจัดส่งและการเปลี่ยน ควรกระทำอย่างปลอดภัยและมีการควบคุมที่เหมาะสม

(1.1) กรณีที่กุญแจ (Key) มีการกำหนดวันหมดอายุ ดำเนินการ ดังนี้

1. ผู้ใช้งานดำเนินการร้องขอมายังศูนย์เทคโนโลยีสารสนเทศ
2. ผู้ดูแลระบบกำหนดกุญแจ (Key) ซึ่งเป็นการเข้ารหัสข้อมูลแบบมาตรฐานการเข้ารหัสลับขั้นสูง (Advanced Encryption Standard : AES) โดยกำหนดวันที่และระยะเวลาในการใช้กุญแจ (Key)
3. กุญแจ (Key) จะถูกเปลี่ยนทุกครั้งที่ใช้งาน ไม่สามารถทำซ้ำได้

(1.2) กรณีที่กุญแจ (Key) ไม่กำหนดวันหมดอายุ ดำเนินการดังนี้

1. ผู้ใช้งานดำเนินการร้องขอผ่านระบบอัตโนมัติเพียงครั้งเดียว

2. ระบบอัตโนมัติกำหนดกุญแจ (Key) ให้กับผู้ร้องขอ โดยการแปลงรูปแบบของข้อมูลที่รับไม่ว่าขนาดใดก็ตาม ให้อยู่ในอีกรูปแบบหนึ่งที่มีขนาดคงที่ และไม่สามารถถอดรหัสข้อมูลได้ (Decrypt) เช่น การเก็บรหัสผ่านผู้ใช้งานในฐานข้อมูล ได้แก่ การใช้ฟังกชัน MD5 หรือ SHA1 เป็นต้น

3. ผู้ใช้งานสามารถใช้งานได้ตลอดไม่มีวันหมดอายุ เนื่องจากมีผลต่อความสามารถในการพิมพ์รายงานบนระบบงาน

(2) กุญแจส่วนตัว (Private key) ที่ใช้ในการเข้ารหัสข้อมูลต้องถูกจัดเก็บให้เป็นความลับและ มั่นคงปลอดภัย

(3) การส่งกุญแจ (Key) ถึงผู้รับ ต้องส่งผ่านในช่องทางที่มีความมั่นคงปลอดภัย

(4) กุญแจ (Key) ต้องได้รับการเพิกถอนทันที เมื่อทราบว่ามีความเสี่ยงที่จะก่อให้เกิดการล่วงละเมิดทางด้านความมั่นคงปลอดภัย เช่น กุญแจส่วนตัว (Private key) รั่วไหลไปยังบุคคลอื่น เป็นต้น

(5) การเพิกถอนการใช้งานกุญแจ (Key) ต้องแจ้งให้ผู้รับผิดชอบและผู้ใช้งานทราบ รวมถึงต้องแจ้งเหตุผลการเพิกถอน วันที่และเวลาที่กุญแจ (Key) ถูกเพิกถอน

(6) การจัดเก็บกุญแจ (Archive) เมื่อไม่มีการใช้งานเป็นระยะเวลานาน ต้องมีวิธีการเก็บด้วยวิธีที่มีความปลอดภัยด้วยการเข้ารหัส (Encrypt)

(7) การทำลายกุญแจ (Key) ต้องทำด้วยความระมัดระวัง โดยใช้วิธีการทำลายกุญแจอย่างปลอดภัยและถาวร (Secure Deletion) และตรวจสอบว่าจะไม่มีการนำกลับมาใช้งานซ้ำอีก

(8) การกระทำใด ๆ ที่เกี่ยวข้องกับกุญแจ (Key) ต้องมีการจัดเก็บข้อมูลการดำเนินการย้อนหลัง (Log) สม่ำเสมอ เพื่อให้สามารถตรวจสอบการทำงานได้ในภายหลัง

ส่วนที่ 13 หลักการวิศวกรรมระบบสารสนเทศอย่างมั่นคงปลอดภัย

(Secure System Engineering Principles)

ทฤษฎีด้านวิศวกรรมระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure System Engineering Principles) กำหนดขึ้นเพื่อให้ระบบสารสนเทศมีระดับการรักษาความมั่นคงปลอดภัยที่เหมาะสมและสามารถตอบสนองต่อความต้องการขององค์กรได้ โดยทฤษฎีดังกล่าวต้องนำไปใช้งานร่วมกับวงจร การพัฒนาระบบสารสนเทศ ซึ่งประเด็นพื้นฐานที่ต้องได้รับการพิจารณาในระหว่างการออกแบบสร้าง หรือพัฒนาระบบสารสนเทศ ได้แก่

(1) มาตรการรักษาความมั่นคงปลอดภัยของระบบต้องได้รับการออกแบบให้สอดคล้องกับข้อกำหนดของแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ ตลอดจนขั้นตอนปฏิบัติงาน มาตรฐาน หรือแนวปฏิบัติด้านความมั่นคงปลอดภัยที่เกี่ยวข้องขององค์กร

(2) พิจารณาและกำหนดมาตรการด้านความมั่นคงปลอดภัย ตั้งแต่ขั้นตอนการระบุความต้องการในการพัฒนาระบบสารสนเทศ (Requirements Development Phase) และถือเป็นส่วนหนึ่งของการออกแบบระบบในภาพรวม

(3) กรณีมีการปรับเปลี่ยนความต้องการของระบบ ต้องพิจารณาปรับเปลี่ยนหรือเพิ่มเติมมาตรการด้านความมั่นคงปลอดภัยให้มีความสอดคล้องกับความต้องการที่เปลี่ยนแปลงไปเสมอ

(4) มาตรการด้านความมั่นคงปลอดภัยที่เลือกใช้ต้องมีระดับความเข้มงวดที่เหมาะสมกับความเสี่ยง ค่าใช้จ่าย วัตถุประสงค์ทางธุรกิจ และประสิทธิผลของการใช้งานระบบสารสนเทศ โดยมาตรการที่ใช้ต้องสามารถลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

(5) ระบบต้องได้รับการออกแบบให้มีความซับซ้อนน้อยที่สุด เพื่อลดองค์ประกอบที่ไม่จำเป็น ข้อผิดพลาดที่อาจเกิดขึ้น และโอกาสในการถูกโจมตีโดยผู้ไม่ประสงค์ดี

(6) วางมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้หลายชั้น (Layered Security) โดยครอบคลุมทั้ง Physical และ Logical ทั้งในระดับระบบปฏิบัติการ ฐานข้อมูลแอพลิเคชันและระบบเครือข่าย

(7) ระบบต้องได้รับการออกแบบให้มีความสามารถในการป้องกันภัยคุกคาม (เช่น เมื่อ มาตรการรักษาความมั่นคงปลอดภัยทำงานผิดพลาดหรือถูกข้ามผ่าน ระบบต้องจำกัดหรือปฏิเสธการเข้าใช้งาน ไม่ยอมให้เข้าใช้งานได้) และมีความสามารถในการฟื้นสภาพ (Recoverability) (โดยอัตโนมัติหรือโดยการสร้าง กระบวนการกู้คืน) ภายในระยะเวลาที่เหมาะสม

(8) มีการสร้างมาตรการด้านความมั่นคงปลอดภัยเพื่อปกป้องในส่วนของการรักษาความลับของข้อมูล การรักษาความถูกต้อง ครบถ้วนของข้อมูล และความพร้อมใช้ของข้อมูลทั้งในระหว่างการประมวลผลการแลกเปลี่ยนและการจัดเก็บ

(9) กำหนดให้ผู้ใช้งานมีบัญชีผู้ใช้งานไม่ซ้ำกัน (Unique Identification)

(10) ต้องมีการออกแบบมาตรการรักษาความมั่นคงปลอดภัยเชิงป้องกันการโจมตีต่างๆ (Attack) โดยพิจารณาในมุมมองของผู้ไม่ประสงค์ดี หรือผู้ที่พยายามข้ามผ่านมาตรการรักษาความมั่นคงปลอดภัยที่มีอยู่และต้องสร้างมาตรการรักษาความมั่นคงปลอดภัยในกรณีที่จำเป็นต้องใช้งานระบบในสภาพแวดล้อมที่ไม่พึงประสงค์ (เช่น การใช้งานระบบในระหว่างเกิดเหตุฉุกเฉินหรือภัยพิบัติ)

(11) ออกแบบสิทธิในการใช้ระบบโดยอาศัยหลักการสิทธิที่น้อยที่สุด (Least Privilege) ตามหน้าที่การทำงานและ/หรือความจำเป็นในการใช้งาน

(12) ออกแบบระบบให้มีกลไกในการตรวจสอบการใช้งาน (Audit Mechanism) สำหรับฟังก์ชัน การทำงานที่สำคัญเพื่อตรวจจับการใช้งานระบบโดยไม่ได้รับอนุญาตและเพื่อใช้สนับสนุนการตรวจสอบ เหตุการณ์ผิดปกติต่างๆ

ส่วนที่ 14 การพัฒนาซอฟต์แวร์ (Software development)

ข้อ 1. โดยหน่วยงานภายนอก (Outsourced software development)

(1) ผู้รับจ่างพัฒนาซอฟตแวร ต่องใชซอฟตแวรที่มีลิขสิทธิ์ถูกต่องตามกฎหมายหากใชซอฟตแวรจากเจาของลิขสิทธิ์อื่น ผูรับจางตองไดรับอนุญาตที่ถูกตอง

(2) ผู้รับจ้างพัฒนาซอฟตแวร ต่องสงมอบเอกสารรับรองวาหนวยงานมีสิทธิใชซอฟตแวรที่เกิดจากการจางพัฒนาทั้งหมดและอนุญาตใหใชสิทธิในซอฟตแวรตามที่ตกลงกันไว้ในสัญญา

(3) ผู้รับจ้างพัฒนาซอฟต์แวร์ ต้องให้ความสำคัญเรื่อง Secure Coding ตั้งแต่การออกแบบ และพัฒนา รวมทั้งตรวจสอบแล้วว่าจะไม่สามารถถูกโจมตี หรือ ถูกเจาะด้วยเครื่องมือหรือภัยคุกคามที่เป็นที่รู้จักได้ง่าย

(4) ต้องแยกระบบในการทดสอบออกจากระบบงานจริง เพื่อป้องกันการเข้าถึงข้อมูลหรือเปลี่ยนแปลงต่อระบบที่ให้บริการจริงจากผู้ที่ไม่ได้รับอนุญาตและต้องติดตามสภาพการใช้งาน การวิเคราะห์ขีดความสามารถของทรัพยากรสารสนเทศอย่างสม่ำเสมอปีละ 1 ครั้ง และให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่างๆ ก่อนดำเนินการติดตั้งทุกครั้ง

(5) การยอมรับระบบใหม่ต้องจัดให้มีเกณฑ์ในการยอมรับ และจัดให้มีการทดสอบระบบใหม่ก่อนที่จะตรวจรับระบบนั้นอย่างเป็นลายลักษณ์อักษร

(6) การพัฒนาระบบที่มีความจำเป็นต้องส่งข้อมูลส่วนบุคคลออกสู่หน่วยงานภายนอกจำเป็นต้องทำการปิดบังข้อมูลบางส่วนหรือบาง Field ใน Database (Data Masking)

ข้อ 2. โดยหน่วยงานภายใน (In-house software development)

(1) จัดให้มีการควบคุมกำกับโครงการพัฒนาซอฟต์แวร์โดยผ่านหัวหน้างาน

(2) พัฒนาซอฟต์แวร์ตามหลักมาตรฐาน วงจรการพัฒนาระบบ (System Development Life Cycle : SDLC) อย่างปลอดภัย (Secure SDLC)

(3) กำหนดวัตถุประสงค์ด้านการรักษาความลับของข้อมูล ทุกครั้งใน คุณลักษณะเฉพาะหรือสัญญา

(4) ระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด

(5) ตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะพัฒนา

(6) ควบคุมเวอร์ชั่นของซอฟต์แวร์ (Software Version Control) ในขณะพัฒนา และหากมีการเปลี่ยนแปลงเกิดขึ้น ต้องควบคุมให้พร้อมนำไปใช้งานต่อได้

(7) ต้องให้ความสำคัญเรื่อง Secure Coding ตั้งแต่การออกแบบ และพัฒนา รวมทั้งตรวจสอบแล้วว่าจะไม่สามารถถูกโจมตี หรือ ถูกเจาะด้วยเครื่องมือหรือภัยคุกคามที่เป็นที่รู้จักได้ง่าย

(8) ควรแยกระบบ การพัฒนา การทดสอบ และการให้บริการ ออกจากกัน

ส่วนที่ 15 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้รับจ้างภายนอก (Outsource)

ข้อ 1. ผู้รับผิดชอบโครงการหรืองานที่มีการจ้าง ผู้รับจ้างภายนอก (Outsource) ต้องกำหนดในคุณลักษณะเฉพาะของงาน (TOR) สัญญาจ้าง ให้ผู้รับจ้างภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศในโครงการ ต้องตระหนักถึงความมั่นคงปลอดภัยของระบบสารสนเทศตามมาตรฐาน ISO/IEC 27001 รวมไปถึงการสื่อสารข้อมูลในโครงการที่มีผลต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศจะต้องไม่ถูกสื่อสารไปยังผู้ที่ไม่มีสิทธิเข้าถึง ควรสื่อสารเท่าที่จำเป็น และต้องรักษาความลับของกรม รวมทั้งต้องกำหนดให้ผู้รับจ้างภายนอก (Outsource) ดำเนินการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ตามรูปแบบที่กรมกำหนดบนเว็บไซต์ https://pdpa.dmsc.moph.go.th

ข้อ 2. ผู้รับผิดชอบโครงการหรืองานที่มีการจ้างผู้รับจ้างภายนอก (Outsource) ต้องเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งาน ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงาน

ข้อ 3. ผู้รับผิดชอบโครงการหรืองานที่มีการจ้าง ผู้รับจ้างภายนอก (Outsource) ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงาน และต้องขออนุญาตผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ก่อนปฏิบัติงาน

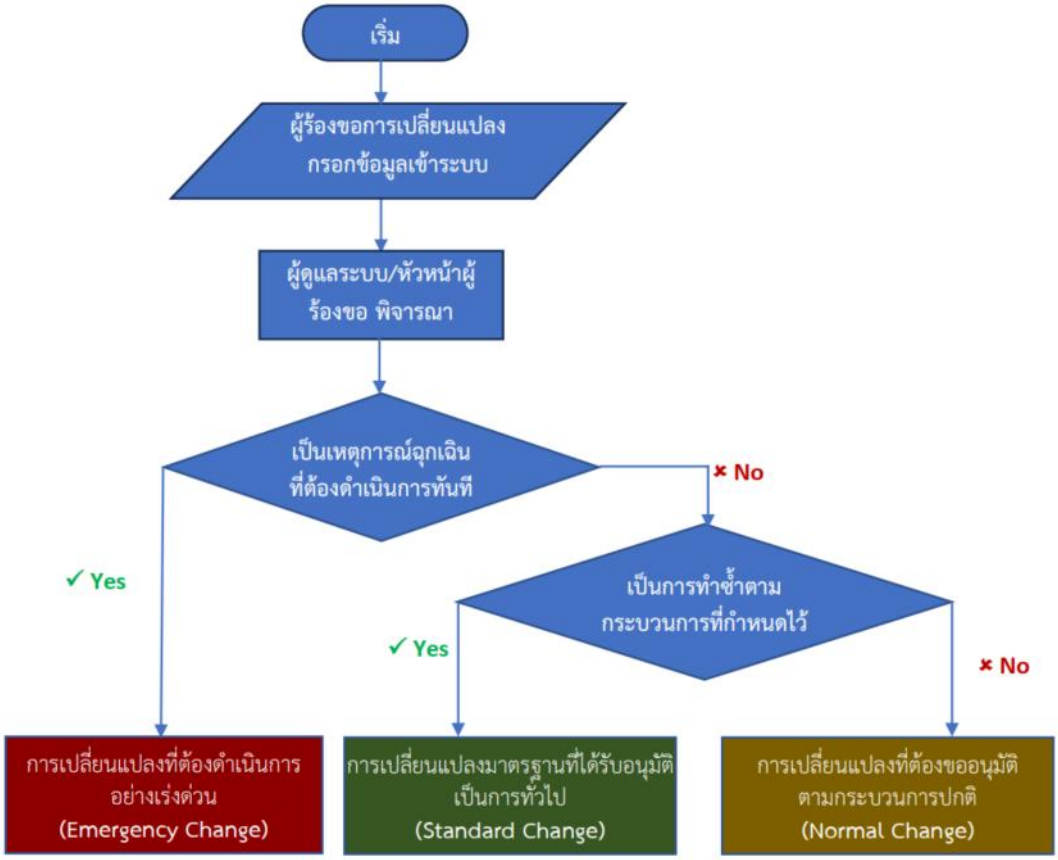
ข้อ 4. ผู้รับผิดชอบโครงการหรืองานที่มีการจ้าง ผู้รับจ้างภายนอก (Outsource) ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร

ข้อ 5. ผู้รับผิดชอบโครงการหรืองานที่มีการจ้าง ผู้รับจ้างภายนอก (outsource) หากต้องเข้าปฏิบัติงานภายในกรม ต้องอยู่ในการดูแลของเจ้าหน้าที่ของกรมตลอดระยะเวลาการปฏิบัติงาน

ส่วนที่ 16 การบริหารจัดการการเปลี่ยนแปลง (change management)

ดำเนินการตามแนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมวิทยาศาสตร์การแพทย์ เรื่องการจัดทำกระบวนการจัดการเปลี่ยนแปลง

แผนผังวิธีการพิจารณาประเภทการเปลี่ยนแปลง



โดยการควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศให้ดำเนินการดังนี้

ข้อ 1. การเปลี่ยนแปลงอุปกรณ์ระบบเครือข่ายและการสื่อสาร ให้ดำเนินการ ดังนี้

- ผู้เกี่ยวข้องต้องดำเนินการแจ้งผู้บังคับบัญชาเป็นลายลักษณ์อักษร
- ผู้เกี่ยวข้องต้องวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลงนั้นๆ
- ผู้เกี่ยวข้องต้องรายงานผลการเปลี่ยนแปลงและผลกระทบต่อผู้บังคับบัญชาเมื่อสิ้นสุดการดำเนินการ

ข้อ 2. การควบคุมการเปลี่ยนแปลง

2.1 กรณีไม่ทราบการเปลี่ยนแปลงมาก่อน ให้ดำเนินการตามแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP)

2.2 กรณีทราบการเปลี่ยนแปลงก่อนล่วงหน้าไม่กี่วัน ให้ดำเนินการ ดังนี้

- สื่อสารไปยังผู้ได้รับผลกระทบ ผ่านช่องทาง Group Line
- ผู้ดูแลระบบดำเนินการเตรียมการเฝ้าระวังต่อการเปลี่ยนแปลงที่จะเกิดขึ้น

2.3 กรณีทราบการเปลี่ยนแปลงก่อนล่วงหน้าเป็นระยะเวลานาน ให้ดำเนินการ จัดทำแผนรองรับการเปลี่ยนแปลง

ข้อ 3. พิจารณาความเหมาะสมของทรัพยากรเป็นประจำสม่ำเสมอ โดยหน่วยงานแจ้งความประสงค์ขอสนับสนุนทรัพยากรมายังศูนย์เทคโนโลยีสารสนเทศ และเลขาคณะกรรมการบริหารและพัฒนาระบบสารสนเทศจะนำเรื่องเข้าที่ประชุมคณะกรรมการบริหารและพัฒนาระบบสารสนเทศ เพื่อพิจารณาความเหมาะสม เป็นประจำทุกเดือน