ข้อควรปฏิบัติในการเตรียมความพร้อมรองรับการตรวจประเมิน
ระบบรักษาความมั่นคงปลอดภัยของข้อมูล ISO/IEC 27001 : 2013
สำหรับหน่วยงานภายในกรมวิทยาศาสตร์การแพทย์

ผู้ปฏิบัติงาน (User)

ควรปฏิบัติ	ไม่ควรปฏิบัติ
1. การดูแลเครื่องคอมพิวเตอร์ของราชการที่ใช้งานเฉพาะบุคคล (ทั้งคอมพิวเตอร์ตั้งโต๊ะ และคอมพิวเตอร์โน๊ตบุ๊ค)	
● ต้องตั้งรหัสผ่านของทุกเครื่อง ● จัดเรียงไฟล์ข้อมูลให้ง่ายต่อการค้นหา ● ทำการอัพเดทเวอร์ชั่นของระบบปฏิบัติการอย่างสม่ำเสมอ เพื่อป้องกันการถูกโจมตี ● ติดตั้งโปรแกรมป้องกันไวรัสที่กรมจัดหาให้และตรวจให้พร้อมใช้งานอยู่เสมอ ● ทำความสะอาดเครื่องคอมพิวเตอร์และส่วนประกอบเป็นประจำ ● ตรวจสอบเครื่องสำรองไฟฟ้าว่าสามารถทำงานได้ตามปกติ ● ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล ● ตั้งโปรแกรมให้ระบบล็อคอัตโนมัติเมื่อจอนิ่งนานเกิน 15 นาที	● ใช้ระบบเครือข่ายคอมพิวเตอร์ของกรมวิทยาศาสตร์การแพทย์ เปิดใช้งานโปรแกรมออนไลน์เพื่อความบันเทิง ทุกประเภท เช่น การดูหนัง ฟังเพลง เกมส์ ในระหว่างเวลาปฏิบัติราชการ ● ใช้สินทรัพย์ของหน่วยงานที่จัดเตรียมให้เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของกรม ● ใช้สินทรัพย์ของกรมเพื่อประโยชน์ทางการค้า ● กระทำการใดๆ เพื่อเป็นการดักข้อมูลไม่ว่าข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายระบบสารสนเทศของกรม โดยเด็ดขาด ไม่ว่าด้วยวิธีการใดก็ตาม ● เปลี่ยนแปลง แก้ไขโปรแกรมที่ติดตั้ง บนเครื่องคอมพิวเตอร์ของหน่วยงาน ● คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
2. กำหนดรหัสผ่านของเครื่องคอมพิวเตอร์ส่วนบุคคล	
● ประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ต้องประกอบด้วยการผสมกันระหว่างตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักขระพิเศษ (Special character) ● เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้	● กำหนดรหัสผ่านอย่างเป็นแบบแผนและง่ายต่อการคาดเดา เช่น “abcdef” “aaaaaa” “123456” “123456” ● กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่ ● ใช้รหัสผ่านร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

	● ใช้โปรแกรมช่วยในการจำรหัสผ่านอัตโนมัติ (Save password) ● จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
ควรปฏิบัติ	**ไม่ควรปฏิบัติ**
3. การยืนยันตัวตนหรือพิสูจน์ตัวตน (Authentication)	
● หากการยืนยันหรือพิสูจน์ตัวตนมีปัญหา ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที ● หากมีบุคคลในหน่วยงานลาออก หรือโยกย้ายหน่วยงาน ให้ทำหนังสือแจ้งมายังผู้ดูแลระบบ เป็นลายลักษณ์อักษร เพื่อยกเลิกสิทธิ์การใช้งาน ● หากต้องการ เพิ่ม/ลบ/แก้ไข รายชื่อผู้ใช้งานของระบบสารสนเทศ ให้หน่วยงานทำหนังสือแจ้งมายังผู้ดูแลระบบเป็นลายลักษณ์อักษร	● ใช้ชื่อและรหัสผ่าน (Username & Password) ของผู้อื่น เพื่อใช้สินทรัพย์หรือระบบสารสนเทศของกรม
4. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ชนิดพกพา (Mobile Device) ส่วนบุคคล (เช่น โน้ตบุค, โทรศัพท์มือถือ, External hard disk, flash drive ฯลฯ) มาใช้ร่วมกับระบบเครือข่ายคอมพิวเตอร์ของกรม	
● ต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ● นำเครื่องคอมพิวเตอร์ส่วนตัวมารับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน หรือได้รับอนุญาตจากหัวหน้าหน่วยงาน ● การนำอุปกรณ์สื่อบันทึกข้อมูลชนิดพกพา เช่น USB Flash Drive, External Harddisk มาใช้ในการปฏิบัติงานร่วมกับเครื่องคอมพิวเตอร์ลูกข่าย จะต้องทำการตรวจสอบไวรัสคอมพิวเตอร์ทุกครั้ง ● เมื่อจำเป็นต้องทำสำเนาข้อมูลสารสนเทศของกรม และนำออกไปใช้นอกกรม ต้องดูแล ป้องกัน ไม่ให้เกิดความเสียหายต่อระบบความปลอดภัยของข้อมูลสารสนเทศกรม ● หากทำการสำเนาข้อมูลเพื่อใช้ภายในหน่วยงาน เมื่อใช้งานเรียบร้อยแล้วให้ลบข้อมูลนั้นออกจากสื่อบันทึกข้อมูลแบบถาวร (Shift + delete) หรือ ฟอร์แมต (format) ทันที	● นำเครื่องคอมพิวเตอร์ส่วนตัวที่ยังไม่ผ่านการตรวจสอบจากผู้ดูแลระบบของหน่วยงาน หรือยังไม่ได้รับอนุญาต มาใช้งานในระบบเครือข่ายคอมพิวเตอร์ของกรม หากฝ่าฝืนต้องถูกดำเนินการตามระเบียบราชการ

● ต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะทิ้ง หรือส่งอุปกรณ์ที่มีข้อมูลสารสนเทศของกรมวิทยาศาสตร์การแพทย์ไปซ่อม	

ควรปฏิบัติ	ไม่ควรปฏิบัติ
5. การควบคุมทรัพย์สินสารสนเทศ (Clear desk and clear screen policy) เพื่อควบคุมทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล แฟ้มข้อมูล เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง ระบบสารสนเทศ และข้อมูลสารสนเทศ	
● ลงชื่อออกจากระบบทันที เมื่อไม่อยู่หน้าจอหรือต้องไปทำภารกิจอื่น ● จัดเก็บเอกสาร ข้อมูลในการทำงาน ข้อมูลสำคัญหรือลับ หรือสื่อบันทึกข้อมูล ไว้ในสถานที่ที่มีความปลอดภัยภายหลังจากใช้งานเสร็จ เช่น เก็บไว้ในตู้ที่ล็อคกุญแจได้ เป็นต้น ● นำเอกสารสำคัญหรือเอกสารที่เป็นความลับ ออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ หากมีการพิมพ์ผิดต้องทำลายเอกสารนั้น ด้วยเครื่องทำลายเอกสารหรือฉีกเป็นชิ้นเล็กๆ ● หากจำเป็นต้องนำทรัพย์สินของทางราชการไปใช้นอกสถานที่ ต้องปฏิบัติตาม ประกาศกรมวิทยาศาสตร์-การแพทย์ เรื่อง ข้อปฏิบัติในการยืมทรัพย์สินของกรมวิทยาศาสตร์การแพทย์ ● ก่อนคืนทรัพย์สินทุกครั้ง ผู้ยืมต้องลบข้อมูลที่เป็นความลับออกจากตัวเครื่องก่อนเสมอ	● ลบ ทำลาย สำเนาข้อมูลที่มีความสำคัญของกรมวิทยาศาสตร์การแพทย์ ก่อนได้รับอนุญาตจากหัวหน้าหน่วยงาน ● ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊คของหน่วยงาน ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้น ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน
6. ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)	

● ปฏิบัติตามข้อกำหนด และระเบียบความปลอดภัยเทคโนโลยีสารสนเทศของกรม อย่างเคร่งครัด ● การมอบชื่อผู้ใช้และรหัสผ่านให้บุคคลอื่นเข้าใช้งาน หากมีการกระทำผิดใดๆ ที่เกิดจากการใช้บัญชีนั้น ท่านต้องรับผิดชอบต่อการกระทำความผิดที่เกิดจากการเข้าใช้งานนั้นตามกฎหมาย ● ข้อมูลของทางราชการและข้อมูลของลูกค้าถือเป็นความลับ การเผยแพร่โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลทั้งตั้งใจและไม่ตั้งใจ ถือว่ามีความผิดตามกฎหมาย ● ผู้ใช้งานต้องดูแลรักษาไว้ซึ่งความลับ ความถูกต้องของข้อมูล และป้องกันความเสี่ยงต่อการเข้าถึง โดยผู้ซึ่งไม่มีสิทธิ์ ● กรมวิทยาศาสตร์การแพทย์ ถือว่าข้อมูลส่วนตัวของผู้ใช้เป็นความลับ จะไม่เปิดเผยต่อบุคคลอื่นโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล เว้นแต่การตรวจสอบข้อมูลตามกฎหมาย ที่สามารถตรวจสอบข้อมูลได้โดยไม่ต้องแจ้งผู้ใช้ทราบ	● นำอุปกรณ์ต่อพ่วง เข้ามาติดตั้งเพิ่มเติมในระบบเครือข่ายคอมพิวเตอร์ของกรมวิทยาศาสตร์การแพทย์โดยไม่ได้รับความเห็นชอบจากผู้ดูแลระบบ ● กระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

7. บทลงโทษตามแนวทางการจัดการความปลอดภัยด้านสารสนเทศของกรม

- **<u>โทษขั้นต้น</u>** ว่ากล่าวตักเตือนด้วยวาจา และ/หรือ ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่าย เป็นเวลา ๑๕ วัน
- **<u>โทษขั้นกลาง</u>** ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่าย เป็นเวลา ๒ เดือน
- **<u>โทษขั้นสูง</u>** ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่าย เป็นเวลา ๖ เดือน
- **<u>โทษขั้นร้ายแรง</u>** ระงับสิทธิการใช้เครื่องคอมพิวเตอร์และเครือข่าย เป็นเวลา ๑ ปี และ/หรือ หากละเมิด ฝ่าฝืนก่อให้เกิดความเสียหาย ต่อผู้อื่น หรือต่อทรัพย์สินทั้งของทางราชการอย่างร้ายแรง จะต้องรับโทษตามระเบียบส่วนราชการ หรือรับโทษ ตามกฎหมายโดยลำดับต่อไป

** **<u>ผู้ฝ่าฝืนขั้นต้น</u>** เกิดจากการฝ่าฝืนระเบียบโดยเล็กน้อยจากความไม่ตั้งใจ หรือโดยบังเอิญ เช่น เปิดให้ใช้แฟ้มข้อมูลร่วม(Share File/Folder) หรือการใช้อุปกรณ์ร่วม (Share CD) โดยลืมกำหนดรหัสผ่าน (password) และ/หรือไม่ทำการยกเลิกการเปิดใช้แฟ้มข้อมูลร่วมกัน หลังจากการใช้งานเสร็จสิ้น เป็นต้น

** **<u>ผู้ฝ่าฝืนขั้นรุนแรง</u>** เกิดจากการละเมิดกฎ และสร้างความเสียหายให้แก่ระบบเครือข่ายกรม เช่น

1. นำ โปรแกรมคอมพิวเตอร์ หรือข้อมูลที่มีไวรัสคอมพิวเตอร์ มาติดตั้งใช้งานในเครือข่ายของกรมวิทยาศาสตร์การแพทย์ ทำ ให้เกิดการแพร่กระจายในเครือข่าย

๒. ทำการติดตั้งเลขหมาย IP หรือนำ เลขหมาย IP ของกรมไปใช้ โดยไม่ได้รับอนุญาต ทำให้ความเสียหายแก่เครือข่าย

๓. ทำ การ Download ไฟล์ที่มีขนาดใหญ่ เกินกว่า ๑ MB. โดยไม่จำเป็น และในระหว่างเวลาราชการซึ่งมีการใช้เครือข่ายอย่างหนาแน่น

๔. ใช้ จดหมายอิเลคทรอนิคส์ (e-Mail) ของกรม ส่ง mail แบบกระจาย ถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำ เป็น หรือ การใช้ข้อความที่ไม่สุภาพส่งไปถึงบุคคลอื่น

๕. ใช้ ระบบ Internet ของกรมในการ ฟังเพลง Online หรือ เล่นเกมส์ Online หรือ สนทนา Online VDO (Chat) ในเวลาราชการ

๖. ล่วงละเมิด บุกรุกหรือรันโปรแกรมจนเป็นเหตุให้ระบบของเซิร์ฟเวอร์ได้รับความเสียหาย

๗. สร้างความเสียหายแก่โปรแกรมหรือข้อมูลหรือฮาร์ดแวร์ระบบ

๘. การเข้าถึงระบบโดยปราศจากความยินยอมหรือการอนุญาตของผู้ดูแลระบบพยายามขโมยรหัสผ่าน (Password) หรือข้อมูล หรือพยายามเจาะทะลุระบบรักษาความปลอดภัยของทั้งเครือข่ายภายในและภายนอกกรม

๙. การสร้างโฮมเพ็จส่วนตัวที่แสดงออกในลักษณะที่ขัดต่อกฎหมาย กฎระเบียบ และศีลธรรม

๑๐. นำ ข้อมูลที่ไม่เหมาะสมใส่ไว้ในโฮมเพจ อาทิเช่น

- ข้อความไม่สุภาพ, ข้อมูลที่ขัดต่อพระราชบัญญัติลิขสิทธิ์และทรัพย์สินทางปัญญา
- นำเสนอภาพลามกอนาจาร ภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของไทย
- ลงโฆษณาหรือข้อมูลทางด้านการค้า, ล่วงละเมิดสิทธิของผู้อื่น

๑๑. ก่อความวุ่นวายที่ขัดต่อกฎระเบียบนี้ หรือสร้างความเดือดร้อน รบกวนการทำงานของผู้ใช้อื่นในระบบเครือข่ายกรม

๑2. ละเมิดกฎระเบียบขั้นต้น ซ้ำมากกว่า ๑ ครั้งโดยเจตนา

ผู้ดูแลระบบ (Admin)

1. ควบคุมการเข้าถึงห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่ายตามแบบฟอร์ม 0600 FM 0105 แก้ไขครั้งที่ 00 แบบฟอร์มเข้าใช้งานพื้นที่ควบคุมเครื่องคอมพิวเตอร์แม่ข่ายกรมวิทยาศาสตร์การแพทย์
2. ผู้ไม่มีหน้าที่ที่ได้รับมอบหมายโดยตรงในการเข้าห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย ต้องลงนามในแบบฟอร์ม ดังนี้
   - 0600 FM 0105 แก้ไขครั้งที่ 00
     แบบฟอร์มเข้าใช้งานพื้นที่ควบคุมเครื่องคอมพิวเตอร์แม่ข่ายกรมวิทยาศาสตร์การแพทย์
   - 0600 FM 0119 แก้ไขครั้งที่ 02
     แบบฟอร์ม การรักษาความเป็นกลาง ความลับ และการไม่มีผลประโยชน์ทับซ้อน ทุกครั้ง
3. ตรวจสอบ ปรับปรุง ระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย (update path) ให้เป็นเวอร์ชั่นปัจจุบันเสมอ
4. หากพบความผิดปกติของระบบเครือข่ายคอมพิวเตอร์ ให้บันทึกเหตุการณ์ในแบบฟอร์ม 0600 FM 0104 แก้ไขครั้งที่ 00 แบบฟอร์มประวัติการตรวจพบ/การแก้ไขอาการผิดปกติของระบบเครือข่ายคอมพิวเตอร์ กรมวิทยาศาสตร์การแพทย์

5. กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงาน
6. กำหนดให้มีการยืนยันตัวตนก่อนเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน
7. กำหนดให้มีการลงทะเบียนคอมพิวเตอร์ และอุปกรณ์เคลื่อนที่ ส่วนบุคคล ที่จะนำมาใช้ในระบบเครือข่ายคอมพิวเตอร์ และระบบอินเตอร์เน็ตของหน่วยงาน
8. จัดเก็บ log file เพื่อให้สามารถทวนสอบการใช้งานได้เมื่อจำเป็น
9. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับการขอใช้บริการระบบเทคโนโลยีสารสนเทศ และจัดเก็บข้อมูลให้เป็นระบบ
10. สำรองข้อมูลที่สำคัญ และซ้อมการกู้คืนระบบอย่างน้อยปี ละ 1 ครั้ง
11. ทำการประเมินความเสี่ยงข้อมูลสารสนเทศ และระบบ ต่างๆ ตาม 0600 WM 0019 แนวทางการจัดการความเสี่ยงในระบบบริหารคุณภาพ แก้ไขครั้งที่ 04
12. หน่วยงานที่มีระบบเป็นของตนเอง เช่น ศูนย์วิทยาศาสตร์การแพทย์ 15 แห่ง ศูนย์ปฏิบัติการตรวจคัดกรองทารกแรกเกิดแห่งชาติ สำนักยาและวัตถุเสพติด เป็นต้น ต้องทำการวิเคราะห์และจัดทำแผนบริหารความต่อเนื่องฯ ให้สอดคล้องกับแผนระดับกรม