



## ประกาศกรมควบคุมโรค

### เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมควบคุมโรค เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กรมควบคุมโรค และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ จึงเห็นสมควรกำหนดนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น

ฉะนั้นอาศัยอำนาจตามความในมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ อธิบดีกรมควบคุมโรค จึงออกประกาศไว้ ดังนี้

๑. ประกาศนี้เรียกว่า “ประกาศกรมควบคุมโรค เรื่อง นโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ”

๒. บรรดาประกาศและคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้ว ซึ่งขัด หรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

๓. ประกาศนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ ลูกจ้างประจำ พนักงานราชการ และลูกจ้างชั่วคราว สังกัดกรมควบคุมโรค ที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศของกรมควบคุมโรค และบุคคลภายนอกที่เข้ามาใช้บริการระบบสารสนเทศของกรมควบคุมโรค รวมถึงหน่วยงานภายนอก ที่ได้รับ อนุญาตให้ใช้งานระบบสารสนเทศของกรมควบคุมโรค

๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรค มีวัตถุประสงค์ ดังต่อไปนี้

๔.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานสารสนเทศ ของกรมควบคุมโรค ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานของกรมควบคุมโรค ได้รับทราบ และถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๔.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกรมควบคุมโรคตระหนักถึงความสำคัญของการรักษาความมั่นคงสารสนเทศ ในการใช้งานด้านสารสนเทศของกรมควบคุมโรค เพื่อปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบาย ปีละ ๑ ครั้ง

๕. นโยบาย...

๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรค กำหนดประเด็นสำคัญดังต่อไปนี้

๕.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๕.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๕.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๕.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่าย โดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่กระทรวงสาธารณสุขจัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งโซน (Zone) การใช้งาน เพื่อให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๕.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่เข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมมัลแวร์ประเภทต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

๕.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๕.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๕.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้ผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๒ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๖. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงจะกำหนดบทลงโทษแก่บุคลากรผู้ปฏิบัติงานนั้น โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๗. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรคตามแนบท้ายประกาศนี้

๘. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๓๑ มกราคม พ.ศ. ๒๕๖๖



(นายธเรศ กรัษนัยรวิวงศ์)  
อธิบดีกรมควบคุมโรค

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย  
ด้านสารสนเทศ ของกรมควบคุมโรค  
ประกาศ ณ วันที่ ๓๑ มกราคม ๒๕๖๖

## สารบัญ

ข้อ ๑ คำนิยาม	๑
หมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ	๓
ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)	๓
ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)	๖
ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Responsibilities)	๘
ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)	๑๐
ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)	๑๒
ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	๑๕
ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)	๑๗
ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing MalWare)	๑๙
ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)	๒๐
ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)	๒๑
ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)	๒๒
ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)	๒๓
ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)	๒๔
ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล	๒๕
ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา	๒๗
ส่วนที่ ๑๖ การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS )	๒๘
ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)	๒๙
ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)	๓๐
หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล	๓๑
ส่วนที่ ๑ การรักษาความปลอดภัยของฐานข้อมูล	๓๑
ส่วนที่ ๒ การสำรองข้อมูล	๓๓
หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	๓๕
ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง	๓๕

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ	๓๕
หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม	๓๘
หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ	๔๒
หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	๔๓
หมวดที่ ๘ การบริหารจัดการการใช้บริการจากหน่วยงานภายนอก	๔๕
แนวปฏิบัติ เมื่อเกิดฟิชซิง (Phishing) ที่เว็บไซต์เวอร์ของหน่วยงาน (ภาคผนวก ๑)	๔๗
แนวปฏิบัติ เมื่อเกิดมัลแวร์ ที่เว็บไซต์เวอร์ของหน่วยงาน (ภาคผนวก ๑)	๔๗

## แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมควบคุมโรค

ตามประกาศกรมควบคุมโรค เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรค กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรค เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมควบคุมโรคเป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อกรมควบคุมโรคนั้น

กรมควบคุมโรค จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

### ข้อ ๑ คำนิยาม

“หน่วยงาน” หมายถึง กรมควบคุมโรค รวมถึงหน่วยงานที่อยู่ภายใต้สังกัดกรมควบคุมโรค

“ผู้ใช้งาน” หมายถึง ข้าราชการ ลูกจ้าง และพนักงานราชการ ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

“ผู้บริหาร” หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ ผู้อำนวยการสำนัก/สถาบัน/ศูนย์/กอง หรือเทียบเท่า เป็นต้น

“ผู้บริหารระดับสูง” หมายถึง อธิบดี รองอธิบดี หรือเทียบเท่า ของกรมควบคุมโรค

“ผู้ดูแลระบบ” (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์

“สินทรัพย์” หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศ การสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย อาทิเช่น โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) อุปกรณ์ระบบเครือข่ายฮาร์ดแวร์และซอฟต์แวร์รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

“ระบบสารสนเทศ” หมายถึง ระบบพื้นฐานของการทำงานต่างๆ ในรูปแบบของการเก็บ (input) การประมวลผล (processing) เผยแพร่ (output) และมีส่วนจัดเก็บข้อมูล (storage)

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

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์

และทาง ภายนอก รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการ เข้าถึงโดยมิชอบเอาไว้

“**ความมั่นคงปลอดภัยด้านสารสนเทศ**” หมายถึง การดำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิดชอบ การห้ามปฏิเสธความรับผิดชอบ และความน่าเชื่อถือ

“**เหตุการณ์ด้านความมั่นคงปลอดภัย**” หมายถึง การเกิดเหตุการณ์ สภาพของบริการ หรือ เครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“**สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด**” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงาน ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม



## หมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

### วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจของหน่วยงานของรัฐ
๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

### แนวปฏิบัติ

#### ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบและธุรกรรม ตามความจำเป็นต่อการใช้งาน เท่านั้น

ข้อ ๒. บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูง หรือหัวหน้าหน่วยงานแล้วแต่กรณี เพื่อให้ความเห็นชอบและอนุญาตก่อน

ข้อ ๓. กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ โดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิ์ตามอนุญาตนั้น ดังนี้

(๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๒) กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

(๓) ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศและปฏิบัติงานตามหัวหน้าหน่วยงานมอบหมาย ดังนี้

(๓.๑) อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของหน่วยงานจะกระทำต่อเมื่อได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๓.๒) กำหนดสิทธิ์ของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิ์การเข้าถึงนั้นอย่างสม่ำเสมอ

(๓.๓) ทดสอบระบบการบันทึกและติดตามการใช้งานและตรวจตราการ ละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศของหน่วยงานอย่างสม่ำเสมอ

ข้อ ๔. จัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาเข้าถึง และช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจนโดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยกำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

(๑) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

(๒) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงมาก
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓) จัดแบ่งประเภทของข้อมูล

- ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลนโยบายข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุขเป็นข้อมูลที่เกี่ยวข้องกับการรักษาผู้ป่วย ประวัติผู้ป่วย ข้อมูลทางการแพทย์และข้อมูลสถานพยาบาล

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นในบังคับบัญชาในหน่วยงานนั้น
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้หรือได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิ์ที่ได้รับมอบหมายตามอำนาจหน้าที่

(๕) รูปแบบของเอกสารอิเล็กทรอนิกส์ให้ถือตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

ข้อ ๕. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบ

(๒) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้งานข้อมูลในแต่ละชั้นความลับ

(๓) กำหนดระยะเวลาการใช้งานและระดับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การกำหนดให้เปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดความสำคัญของข้อมูลแต่ละระดับ

(๕) การรับ-ส่งข้อมูลด้วย SSL, VPN หรือ XML Encryption ผ่านระบบเครือข่ายต้องเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์หน่วยงานออกนอกหน่วยงาน รวมถึงการบำรุงรักษาตรวจสอบให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

(๗) กำหนดเวลาการเข้าถึงระบบสารสนเทศ หากมีการบันทึกแก้ไขข้อมูลสารบบคดีอิเล็กทรอนิกส์ให้เรียกรายงานได้ในเวลาเช้าวันรุ่งขึ้นในอีกวันถัดไปเท่านั้น เนื่องจากระบบจะทำการประมวลผลตอนเที่ยงคืน

(๘) การกำหนดระยะเวลาการเชื่อมต่อ (Limitation of Connection Time) สำหรับการใช้งานระบบสารสนเทศบางระบบให้เป็นไปตามช่วงเวลาการทำงานที่หน่วยงานกำหนดส่วนระบบสารสนเทศที่มีความสำคัญสูงให้ทำการตัดระบบและหมดเวลาการใช้งานรวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีการใช้งานภายในช่วงระยะเวลา ๑๕ นาที

ข้อ ๖. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) ควบคุมการเข้าถึงสารสนเทศโดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิ์เกี่ยวข้องกับระบบสารสนเทศ

(๒) ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๗. การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงาน ดังนี้

(๑) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน ดังนี้ ระบบรักษาความปลอดภัย (Security) ระบบสำรองกระแสไฟฟ้า (UPS) เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบระบายอากาศ ระบบปรับอากาศและควบคุมความชื้น

(๒) ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าทำงานได้ปกติและลดความเสี่ยงจากความล้มเหลวในการทำงาน

(๓) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีจากระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (Data Center) เมื่อมีการทำงานเครื่องผิดปกติหรือหยุดการทำงาน

(๔) จัดวางอุปกรณ์ในพื้นที่ หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอกและให้แยกอุปกรณ์ที่มีความสำคัญเก็บไว้ที่พื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

(๕) ตรวจสอบสอดส่องดูแลสภาพแวดล้อมภายในห้องและตรวจสอบระดับอุณหภูมิความชื้นให้อยู่ระดับปกติเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในห้องศูนย์ข้อมูล (Data Center)

(๖) การเดินสายไฟสายสัญญาณเครือข่ายของหน่วยงานและสายเคเบิลอื่นที่จำเป็นต้องทำการวางผ่านเข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้นั้น ให้ร้อยท่อสายสัญญาณต่าง ๆ

เพื่อป้องกัน หนู นก กระรอก แมลงสาบ หรือสัตว์อื่นกัดสายไฟ ป้องกันการดักจับ สัญญาณ การตัดสายสัญญาณ อันจะทำให้เกิดความเสียหายต่อระบบเครือข่ายใช้งานไม่ได้

(๗) ต้องจัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง โดยสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน แล้วให้จัดเก็บสายสัญญาณต่าง ๆ ไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิทเพื่อป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง

## ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๗. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

- (๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ
- (๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน
- (๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ ๓)
- (๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งทีแสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ ๘. ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

ข้อ ๙. ผู้ดูแลระบบต้องการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก หรือสิ้นสุดการจ้างโดยปฏิบัติตามแนวทาง ดังนี้

- (๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน
- (๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่
- (๓) ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน
- (๔) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง และทบทวนสำหรับผู้ที่มีสิทธิในระดับสูงด้วยความถี่มากกว่าผู้ใช้งาน
- (๕) เมื่อเจ้าหน้าที่มีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก สิ้นสุดการจ้างงาน หรือเปลี่ยนหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้ถอดถอนสิทธิภายใน ๑ - ๒ วันทำการ

ข้อ ๑๐. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

- (๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- (๒) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

- (๓) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)
- (๔) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)
- (๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง
- (๖) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

ข้อ ๑๑. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธี การทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

- (๑) ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมเข้าถึงข้อมูลและประเภทชั้นความลับทั้งการเข้าถึง โดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภท ชั้นความลับหากข้อมูลมีความลับ
- (๒) เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูล ของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ ยังคงมีความเหมาะสม
- (๓) ผู้ดูแลข้อมูลระบบควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการ เข้าถึงข้อมูลโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนด รายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการ ตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับข้อมูล
- (๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ VPN
- (๕) มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญ ของข้อมูลตามที่ระบุไว้ในเอกสาร “การใช้งานรหัสผ่านผู้ใช้งาน”
- (๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจสอบให้ดำเนินการสำรองและลบ ข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น
- (๗) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของ ผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- (๘) หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใดบุคคลหนึ่ง ต้องเป็นผู้รับผิดชอบต่อการกระทำความผิด นั้นตามกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง

ข้อ ๑๒. ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อน ตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างกรมควบคุมโรคหรือหน่วยงานที่มาขอเชื่อมโยง

- (๑) กำหนดนโยบายและมาตรการเพื่อควบคุมป้องกัน และบริหารจัดการ การใช้ข้อมูลร่วมกัน
- (๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล
- (๓) พิจารณาวามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน
- (๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน
- (๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มี มาตรการป้องกันเพียงพอ

### ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๓. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

- (๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)
- (๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้อง ประกอบด้วย ตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)
- (๓) หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อหรือนามสกุลของตนเองหรือตรงกับคำในพจนานุกรม
- (๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้เพิ่มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่าย คอมพิวเตอร์
- (๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- (๖) ไม่จดหรือบันทึกที่รหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของ บุคคลอื่น
- (๗) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบ รหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย
- (๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๑๘๐ วัน หรือทุกครั้งที่มีการ แจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๑๔. การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบ การรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ โดยต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

ข้อ ๑๕. การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนด ให้เป็นความผิด ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๑๖. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศ ของ หน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล้าสมัย หรือเกิดจากความ ผิดพลาด ใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

- (๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
- (๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง
- (๓) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้
- (๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง
- (๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๑๐ นาที และต้องใส่รหัสผ่าน (Password) ให้ถูกต้อง จึงจะสามารถเปิดหน้าจอได้

ข้อ ๑๗. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของกรมควบคุมโรค หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๘. เอกสารที่เป็นความลับหรือมีระดับความสำคัญ ซึ่งพิมพ์ออกจากเครื่องพิมพ์ (Printer) ตลอดจนข้อมูลที่เป็นความลับในรูปอิเล็กทรอนิกส์ ผู้ใช้งานต้องปฏิบัติให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับทางราชการดังนี้

- (๑) จัดหมวดหมู่เอกสารที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก
- (๒) จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ
- (๓) การเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย ต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน หรือผู้ที่เป็นเจ้าของ
- (๔) ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน
- (๕) ทำลายเอกสารที่เป็นความลับ หรือมีระดับความสำคัญสูงเมื่อหมดความจำเป็นในการใช้งาน

ข้อ ๑๙. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของกรมควบคุมโรค และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งาน ต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๐. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้ของข้อมูล (Availability) ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๒๑. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กรมควบคุมโรคจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่กรมควบคุมโรคต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับกรมควบคุมโรค ซึ่งกรมควบคุมโรคอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๒. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่าย คอมพิวเตอร์แบบหนึ่งที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่าแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือ แฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม

(File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent) , อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๒๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เล่นเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๒๔. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของกรมควบคุมโรค

ข้อ ๒๕. ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกรมควบคุมโรค

ข้อ ๒๖. ห้ามใช้สินทรัพย์ของกรมควบคุมโรคเพื่อประโยชน์ทางการค้า

ข้อ ๒๗. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะ เป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายระบบสารสนเทศของกรมควบคุมโรค โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๒๘. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ ๒๙. ห้ามใช้ระบบสารสนเทศของกรมควบคุมโรค เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓๐. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะ เป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๑. ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของกรมควบคุมโรค โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

#### ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๓๒. ผู้ใช้งานต้องไม่เข้าไปในห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center ) หมายถึง สถานที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย, อุปกรณ์บริหารจัดการเครือข่ายและเครื่องระบบคอมพิวเตอร์เสมือนที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๓. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๔. ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๓๕. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ ๓๖. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัด อุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บ ข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้



ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
กระดาษ	- ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ หรือใช้วิธีการทุบหรือบดให้เสียหาย ตามขั้นตอนปฏิบัติการจัดระดับชั้นความลับ และการ จัดการสื่อบันทึกข้อมูล (Information Classification and Media Handling Procedure)
แผ่น CD/DVD	-ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร ตามขั้นตอนปฏิบัติการจัดระดับชั้นความลับ และการ จัดการสื่อบันทึกข้อมูล (Information Classification and Media Handling Procedure)
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- ทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบหรือใช้วิธีการทุบหรือบดให้เสียหาย ตามขั้นตอนปฏิบัติการจัดระดับชั้นความลับ และการ จัดการสื่อบันทึกข้อมูล (Information Classification and Media Handling Procedure)

ข้อ ๓๗. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบการรับหรือคืน สินทรัพย์ จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่หน่วยงานมอบหมาย

ข้อ ๓๘. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมาย

ข้อ ๓๙. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๔๐. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน้ตบุ๊ก ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

ข้อ ๔๑. ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่างๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อกรมควบคุมโรค

ข้อ ๔๒. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๔๒ ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

## ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๔๓. มาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

- (๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor) แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”
- (๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการ ปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ ในแบบฟอร์มการขออนุญาตเข้าออกให้ถูกต้องชัดเจน
- (๓) ผู้ดูแลระบบต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกแบบฟอร์มการขออนุญาตเข้า-ออก เป็นประจำทุกเดือน

ข้อ ๔๔. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ระบบ เครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

ข้อ ๔๕. การขออนุญาตใช้งานพื้นที่เครื่องแม่ข่ายเสมือน โดยใช้ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ โดยแจ้งผ่านระบบอิเล็กทรอนิกส์ (DDC SERVICE) และได้รับการอนุญาตจากหัวหน้ากลุ่มงานฯ และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบ และผู้ใช้งานอื่น ๆ

ข้อ ๔๖. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์กระจายสัญญาณ (Access point) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๗. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

- (๑) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น
- (๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
- (๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้
- (๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมี ความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย
- (๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้า ใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ
- (๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้อง มีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการ พิสูจน์ยืนยันตัวตน (Authentication) ด้วยการเข้ารหัสผ่าน เพื่อตรวจสอบความ ถูกต้องของผู้ใช้งานก่อนทุกครั้ง

- (๓) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายใน ของระบบเครือข่ายภายในของหน่วยงาน
- (๔) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- (๕) การระบุอุปกรณ์บนเครือข่าย
  - ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
  - อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่กำหนด โดยผู้ดูแลระบบเครือข่าย
  - ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
  - กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ที่สามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้ หรือไม่ สามารถเชื่อมต่อได้
  - อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
  - การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้ อุปกรณ์

(๑๐) กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่าย เมื่อเว้นว่างจากการใช้งานเป็นเวลานาน

ข้อ ๔๘. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๔๙. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบ ให้ติดตั้งก่อนดำเนินการ

ข้อ ๕๐. กำหนดให้มีการจัดเก็บซอร์สโค้ด ไบรารี และเอกสารสำหรับซอฟต์แวร์ของระบบงาน ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ ๕๑. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ข้อ ๕๒. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบตามแนวทางปฏิบัติ ดังต่อไปนี้

- (๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่าย และ เครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็น ลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้าหน่วยงาน
- (๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

- (ก) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน
- (ข) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ
- (ค) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกล ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๕๓. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

- (๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต
- (๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอกเพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อ ๕๔. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ ๕๕. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ ๕๖. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคล ที่ใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบ เครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ข้อ ๕๗. IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ใหบุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ข้อ ๕๘. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

## ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๕๙. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๖๐. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

- (๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
- (๒) หลังจากระบบติดตั้งเสร็จ ต้องมีระบบบริหารจัดการรหัสผ่าน ที่สามารถทำงานเชิงโต้ตอบหรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการเปลี่ยนรหัสผ่านของผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที
- (๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
- (๔) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง
- (๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน
- (๖) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
- (๗) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน
- (๘) ซอฟต์แวร์ที่กรมควบคุมโรคใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว
- (๙) ซอฟต์แวร์ที่กรมควบคุมโรคจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น
- (๑๐) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกรมควบคุมโรค เพื่อประโยชน์ทางการค้า
- (๑๑) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพ ไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครื่องคอมพิวเตอร์
- (๑๒) ห้ามผู้ใช้งานของหน่วยงานควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๖๑. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง โดยปฏิบัติตามแนวทางที่กำหนดไว้ในข้อ ๑๑

ข้อ ๖๒. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการ ใช้งานโปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิด สามารถทำให้ผู้ใช้หลักเสี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้

เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

- (๑) การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับการอนุมัติจากผู้ดูแลระบบและต้องมีการพิสูจน์ ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน
- (๒) โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์
- (๓) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน
- (๔) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้
- (๕) ต้องยกเลิกหรือลบทั้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

ข้อ ๖๓. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session time-out)

- (๑) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งาน เป็นเวลา ๓๐ นาทีเป็นอย่างน้อย ต้องยุติการใช้งานระบบสารสนเทศ (Session Time-out) นั้น
- (๒) ระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นตามความเหมาะสม หรือเป็นเวลา ๑๐ นาที

ข้อ ๖๔. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

- (๑) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศ หรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัย ดังนี้
  - กำหนดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับระบบสารสนเทศ หรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูงเพื่อให้ผู้ใช้งาน สามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้ได้ ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง
  - กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุและพิสูจน์ตัวตน เพื่อเข้าใช้งานใหม่ทุกครั้ง
- (๒) กำหนดให้ระบบสารสนเทศ ที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ ภายใน ๓๐ นาที

## ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ข้อ ๖๕. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การ ลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๖๖. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) ระบบทรัพยากรบุคคล(DIPS) ระบบบริหารงานโครงการ (Estimate) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าว อย่างสม่ำเสมอ

ข้อ ๖๗. ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงาน ระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกิน ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ ๖๘. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

- (๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบ ลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- (๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
- (๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- (๔) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้อง ได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้ รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๖๙. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลาย ข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

- (๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน
- (๒) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล
- (๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- (๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น
- (๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

- (๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ ออก นอกหน่วยงาน เช่น บำรุงรักษา ตรวจสอบ ให้ดำเนินการสำรองและลบ ข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น
  - (๗) ต้องสำรองข้อมูลและระบบ และทดสอบการกู้คืนข้อมูลและระบบอย่างสม่ำเสมอ โดยกำหนดความถี่ในการดำเนินงานอย่างชัดเจนในแต่ละระบบ
  - (๘) ไม่เก็บข้อมูลสำคัญขององค์กรไว้บนอุปกรณ์แบบพกพา เว้นแต่มีความจำเป็น และข้อมูลดังกล่าวจะต้องมีการเข้ารหัสข้อมูลที่เป็นมาตรฐาน
  - (๙) ข้อมูลที่มีชั้นความลับที่ต้องส่งออกไปนอกองค์กร โดยถูกจัดเก็บไว้บนอุปกรณ์แบบพกพาหรือถูกส่งผ่านระบบเครือข่ายไร้สาย ต้องผ่านการอนุมัติจากเจ้าของระบบงานและธุรกรรม และทำการเข้ารหัสข้อมูลและระบบเครือข่ายไร้สายก่อนเท่านั้น
  - (๑๐) การเคลื่อนย้ายข้อมูลที่มีชั้นความลับ ต้องกระทำโดยบุคคลที่เข้าของระบบงาน และธุรกรรมกำหนด และจะต้องทำลายข้อมูลดังกล่าวทันทีเมื่อไม่มีการใช้งานแล้ว
- ข้อ ๗๐. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้
- (๑) ระบบที่ไวต่อการรบกวน โดยมีผลกระทบและมีความสำคัญสูง ได้แก่ ระบบข้อมูลผู้ป่วยที่เป็นข้อมูลที่เกี่ยวข้องกับการรักษาพยาบาลและข้อมูลทางการแพทย์ ระบบบุคลากรที่เป็นข้อมูลส่วนบุคคลของเจ้าหน้าที่ภายในกรมควบคุมโรค
  - (๒) ต้องมีการควบคุมสภาพแวดล้อมของระบบที่ไวต่อการรบกวนโดยเฉพาะ
    - (๒.๑) มีห้องปฏิบัติการแยกเป็นสัดส่วน และต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว
    - (๒.๒) ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่นและกำหนดสิทธิ์ในการเข้าถึงข้อมูล
  - (๓) ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร
- ข้อ ๗๑. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้
- (๑) ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์
  - (๒) รมั้ดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป
  - (๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที
  - (๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย
  - (๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น



## ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing MalWare)

ข้อ ๗๒. กรมควบคุมโรคได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐาน ละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๗๓. ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ ๗๔. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่หน่วยงานได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้า หน่วยงาน กรณีที่ติดตั้งโปรแกรมไวรัสคอมพิวเตอร์ (Antivirus) ด้วยตนเอง ผู้ดูแลระบบจะไม่รับผิดชอบต่อการเกิดข้อผิดพลาดใดๆ โดยถือเป็นความรับผิดชอบส่วนบุคคล

ข้อ ๗๕. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบ ไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๗๖. ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๗๗. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๗๘. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๗๙. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็น สิทธิ์ของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๘๐. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สิทธิ์ของหน่วยงาน สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการดังนี้

- (๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูล บุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น
- (๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์ และลำดับความสำคัญ ในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น
- (๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่น ในลักษณะเช่นเดียวกับหนอนคอมพิวเตอร์หรือไวรัสคอมพิวเตอร์
- (๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้าง เว็บเพจ บนเครือข่ายคอมพิวเตอร์

ข้อ ๘๑. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์ โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนา โดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้ง ก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้อง ดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

(๖) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องลงนามในสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ก่อนดำเนินการ

(๗) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องถือปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมควบคุมโรค

#### ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๘๒. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัส (Virus)และการใช้งานไฟร์วอลล์ (Firewall) ตามที่หน่วยงานกำหนด

ข้อ ๘๓. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

ข้อ ๘๔. ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้อง มีการตรวจสอบ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ ๘๕. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคง ปลอดภัยของหน่วยงาน

ข้อ ๘๖. ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการ ต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ ๘๗. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุง สิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

## ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ ๘๘. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๘๙. ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน และกำหนดให้ซ่อน SSID (Service Set Identifier) โดยเฉพาะระบบงานที่เป็นชั้นความลับ ดังกล่าวด้วย

ข้อ ๙๐. ผู้ดูแลระบบจะต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) หรือ ที่ดีกว่า ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าโดยไม่ให้แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๙๑. ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และหรือบัญชีผู้ใช้ใช้งาน โดยอนุญาตเฉพาะผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สายตามที่กำหนดไว้เท่านั้น

ข้อ ๙๒. ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๙๓. ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่าย ไร้สาย

ข้อ ๙๔. ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนระบบเครือข่ายไร้สาย

ข้อ ๙๕. ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ความผิดปกติของเครื่องต่อการใช้งานในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อ ๙๖. ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้เกิดบุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สาย ในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

ข้อ ๙๗. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรมควบคุมโรค จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการอนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ ๙๘. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

## ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๙๙. หน่วยงานมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

ข้อ ๑๐๐. การกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

ข้อ ๑๐๑. ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดย Firewall

ข้อ ๑๐๒. ผู้ใช้งานอินเทอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

ข้อ ๑๐๓. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการสำรองข้อมูลการตั้งค่าทุกครั้งก่อนการเปลี่ยนแปลง ค่าต่าง ๆ บน Firewall

ข้อ ๑๐๔. การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๑๐๕. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้า-ออก อุปกรณ์ Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(FortiAnalyzer) โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๐๖. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิด Antivirus และ Application Control เพื่อควบคุมการใช้งานระบบเครือข่ายและความมั่นคงปลอดภัยระบบเครือข่าย ในกรณีที่ต้องใช้งานเกินกว่ามาตรฐานการเชื่อมต่ออินเทอร์เน็ตที่กำหนด จะต้องได้รับความยินยอมจากหน่วยงานก่อน

ข้อ ๑๐๗. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายชื่อเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงาน โดยต้องระบุข้อมูล ดังนี้

(๑) หมายเลข Port ที่ต้องการขอให้เปิด

(๒) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

(๓) วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้น ๆ

ข้อ ๑๐๘. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ Firewall เป็นประจำทุกเดือนและทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ ๑๐๙. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ภายในหน่วยงานที่มีลักษณะที่เป็นอินเทอร์เน็ต จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๑๐. หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดหรือเสี่ยงต่อความปลอดภัยของระบบเครือข่ายส่วนรวม หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๑๑๑. การเชื่อมต่อในลักษณะของการเข้าถึงจากภายนอก มายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน Data center จะต้องบันทึกการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานก่อน

ข้อ ๑๑๒. ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ข้อ ๑๑๓. ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งาน อย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

## ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

ข้อ ๑๑๔. ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องทำการกรอกข้อมูล ขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-Mail) ผ่านระบบบริการออนไลน์ (DDC SERVICE)

ข้อ ๑๑๕. รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ “•” ในการพิมพ์แต่ละตัวอักษร

ข้อ ๑๑๖. เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ให้เปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ ๑๑๗. ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ เช่น ไม่เกิน ๓ ครั้ง

ข้อ ๑๑๘. ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๑๑๙. เปลี่ยนรหัสผ่าน (Password) ทุก ๖ เดือน

ข้อ ๑๒๐. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่าน หรือรับ หรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-Mail) ของตน

ข้อ ๑๒๑. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๑๒๒. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่หน่วยงานกำหนดไว้ให้ใช้ความ ระมัดระวังในการระบุชื่อที่อยู่ จดหมายอิเล็กทรอนิกส์ (E-Mail) ของผู้รับ ให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๑๒๓. ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นจดหมายขยะ (SpamMail)

ข้อ ๑๒๔. ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๑๒๕. ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

ข้อ ๑๒๖. ห้ามส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๒๗. ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ (E-Mail) ทุกฉบับที่ส่งไป

ข้อ ๑๒๘. ให้ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ (E-Mail) ตามความจำเป็น (แม้ว่าหน่วยงานจะ ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้นจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่เก่ามาก ๆ และ มีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

ข้อ ๑๒๙. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .COM เป็นต้น

ข้อ ๑๓๐. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๓๑. ผู้ใช้งานต้องไม่ใช่ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมหรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมาย อิเล็กทรอนิกส์

ข้อ ๑๓๒. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุดและควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๑๓๓. ข้อควรระวังผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อ ๑๓๔. ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในระบบราชการตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

### ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ ๑๓๕. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem หรือ Home Router หรือ Router Wi-Fi หรือ Switch ที่ไม่ได้รับอนุญาต ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ ๑๓๖. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่อ อินเทอร์เน็ต ผ่านเว็บเบราว์เซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ ๑๓๗. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๑๓๘. ห้ามใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อกระทำการต่อไปนี้

- (๑) หาประโยชน์ในเชิงธุรกิจส่วนตัว
- (๒) เพื่อความบันเทิง ได้แก่ การเล่นเกม ดูภาพยนตร์ ฟังเพลง
- (๓) กระทำการที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ และชื่อเสียงขององค์กร เช่น การเผยแพร่ข้อมูลที่อาจก่อความเสียหายต่อองค์กร หรือข้อมูลสำคัญที่เป็นความลับขององค์กร
- (๔) กระทำผิดกฎหมาย เช่น
  - นำเข้าหรือเผยแพร่ ข้อมูลหรือชุดโปรแกรมที่ละเมิดลิขสิทธิ์
  - แพร่กระจายโปรแกรมไม่ประสงค์ดี (Malware) เช่น ไวรัสคอมพิวเตอร์
  - กระทำการที่ไม่เหมาะสมขัดต่อศีลธรรม เช่น การเล่นเกมออนไลน์ การนำเข้าหรือเผยแพร่สื่อลามก อนาจาร
  - กระทำการที่ส่งผลร้าย กระทบกับความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เช่น การก่อการร้าย

- กระทำการข่มขู่ คุกคาม หรือละเมิดสิทธิ์ของผู้อื่นให้ได้รับความเสียหาย เช่น การนำเข้าหรือเผยแพร่ภาพ เสียง สื่อผสมภาพและเสียง (Multimedia) ของผู้อื่น ทั้งที่เป็นข้อมูลจริง หรือข้อมูลเท็จอันเกิดจากการสร้าง ตัดต่อ แต่งเติม หรือ ดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่ทำให้ผู้อื่นนั้นเสีย ชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
- กระทำการเป็นภัยต่อสังคม เช่น การนำเข้าหรือเผยแพร่ ข้อมูลที่มีลักษณะอันเป็นเท็จเพื่อสร้างความสับสนวุ่นวาย หรือเพื่อการหลอกลวงให้เกิดความเสียหายต่าง ๆ

ข้อ ๑๓๙. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๑๔๐. ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๑๔๑. ในการใช้งานระบบเครือข่ายอินเทอร์เน็ตไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๑๔๒. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่ควรเสนอความคิดเห็น หรือใช้ข้อความที่ยั่ว ุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

ข้อ ๑๔๓. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

ข้อ ๑๔๔. หลังจากสิ้นสุดการใช้งานระบบอินเทอร์เน็ต (Internet) ให้ทำการออกจากระบบ (logout) และปิดเว็บเบราว์เซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๑๔๕. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ/หรือกฎหมาย ระเบียบ วิธีปฏิบัติทางคอมพิวเตอร์ อื่นๆ ที่เกี่ยวข้อง อย่างเคร่งครัด

#### ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ ๑๔๖. แนวทางปฏิบัติการใช้งานทั่วไป

- (๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ในราชการ
- (๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอก โปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือ นำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- (๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน
- (๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการ โดยเจ้าหน้าที่ของหน่วยงาน หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และ อุปกรณ์ที่ได้ทำสัญญากับกรมควบคุมโรคเท่านั้น

- (๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
- (๖) ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์
- (๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวัน เสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง
- (๘) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งาน ที่เครื่องคอมพิวเตอร์
- (๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่าย ของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อน การใช้งาน

ข้อ ๑๔๗. การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทาง “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน” ที่ระบุไว้ในเอกสารส่วนที่ ๓

ข้อ ๑๔๘. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

- (๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์
- (๒) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน
- (๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ ๑๔๙. การสำรองข้อมูลและการกู้คืน

- (๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึก อื่น ๆ เช่น CD, DVD, External Hard Disk, flash Drive เป็นต้น
- (๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้ อย่างสม่ำเสมอ
- (๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน



## ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

### ข้อ ๑๕๐. แนวทางปฏิบัติการใช้งานทั่วไป

- (๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ
- (๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- (๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- (๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม
- (๕) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับ เครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระแทกกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
- (๖) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
- (๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์
- (๘) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบาที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- (๙) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะเวลาหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
- (๑๐) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

### ข้อ ๑๕๑. ความปลอดภัยทางด้านกายภาพ

- (๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
- (๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

### ข้อ ๑๕๒. การควบคุมการเข้าถึงระบบปฏิบัติการ

- (๑) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา
- (๒) ผู้ใช้งานต้องกำหนดรหัสผ่านอย่างน้อย ๘ ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

- (ก) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่านใหม่อีกครั้ง
- (ค) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอ เป็นเวลานาน

ข้อ ๑๕๓. การใช้รหัสผ่านให้ผู้ใช้งานกำหนดรหัสผ่านอย่างน้อย ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

ข้อ ๑๕๔. การสำรองข้อมูลและการกู้คืน

- (๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล
- (๒) ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล
- (๓) แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ
- (๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้วต้องทำลายไม่ให้นำไปใช้งานได้
- (๕) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

## ส่วนที่ ๑๖ การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS )

ข้อ ๑๕๕. IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่ายพร้อมทั้งบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๑๕๖. IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูล ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๑๕๗. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๑๕๘. ระบบทั้งหมดใน DMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๑๕๙. โฮสต์(Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๑๖๐. ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

ข้อ ๑๖๑. ระบบ IDS/IPS ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งานกิจกรรม และบันทึก ปริมาณข้อมูลเข้าใช้งานเครือข่าย เป็นประจำทุกวัน โดยผู้ดูแลระบบ

ข้อ ๑๖๒. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่าย ของระบบสารสนเทศตามปกติ

ข้อ ๑๖๓. เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน  
ข้อ ๑๖๔. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้หัวหน้าหน่วยงานทราบทันทีที่ตรวจพบ

ข้อ ๑๖๕. พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกรู้จักพบ จะต้องมีการรายงานให้หัวหน้าหน่วยงานทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๖๖. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๖๗. ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มัลแวร์ที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๖๘. หน่วยงานมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๖๙. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของกรมควบคุมโรค การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบ สารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อ ข้อมูล และทรัพยากรระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

## ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อ ๑๗๐. การปรับปรุงระบบปฏิบัติการ (Operating System Update)

- (๑) ตรวจสอบเครื่องแม่ข่าย เครื่องแม่ข่ายเสมือนและอุปกรณ์ระบบ
- (๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน
- (๓) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน (User)
- (๔) กำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name) / IP Address
- (๕) ปรับปรุง / กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่มีระบบปฏิบัติการที่มี Service Patch Update)
- (๖) ติดตั้งโปรแกรม Antivirus ต้องเป็น/ปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

ข้อ ๑๗๑. การบริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการทำงานของระบบ (User Account Management)

- (๑) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)
- (๒) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)
- (๓) บันทึกบัญชีผู้ใช้งานและสิทธิ์การเข้าใช้ระบบ

ข้อ ๑๗๒. การปรับปรุงการรักษาความปลอดภัย / Anti Virus (System Security & Antivirus Update)

- (๑) ติดตามแผนผังการทำงานของคอมพิวเตอร์การเข้าใช้ระบบ
- (๒) Performance ของระบบหรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

- (ก) ปรับปรุง / กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา
- (ข) ปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นปัจจุบัน
- (ค) ดำเนินการ Scan ตรวจสอบไวรัสคอมพิวเตอร์เป็นประจำ

ข้อ ๑๗๓. ติดตั้ง / ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

- (๑) ติดตั้งระบบจัดการฐานข้อมูลตามความต้องการของระบบงานที่หน่วยงานใช้
- (๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง และมีประสิทธิภาพ ตามระบบฐานข้อมูลนั้นกำหนดของระบบฐานข้อมูล
- (๓) สร้าง และกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้งานอื่น และสิทธิ์การใช้
- (๔) ปรับปรุง / กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่ เสมอ

ข้อ ๑๗๔. ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่าง ๆ / กำหนดค่าระบบของโปรแกรม และกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

- (๑) ติดตั้งโปรแกรมระบบงานตามความต้องการหรือการพัฒนา
- (๒) กำหนดค่า หรือโปรแกรม หรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการเป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ
- (๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงานและทำการทดสอบการให้บริการตามระบบงานนั้นกำหนด
- (๔) แจ้งผู้ใช้งานหรือเจ้าของระบบงานให้สามารถเริ่มใช้งานได้โดยแจ้งรายชื่อรหัสผ่าน และสิทธิ์การเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้
- (๕) กำหนดเกณฑ์การสำรองข้อมูล / สำเนา / ทดสอบกู้คืน (Restore Test)
- (๖) บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้าง / ปรับปรุง

#### ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ ๑๗๕. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

ข้อ ๑๗๖. ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ ๑๗๗. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๑๗๘. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึก เหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

## หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

### วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง
๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย
๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนัก ถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

### แนวปฏิบัติ

#### ส่วนที่ ๑ การรักษาความปลอดภัยของฐานข้อมูล

ข้อ ๑. กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

ข้อ ๑. จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

ข้อ ๒. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

(๒.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว (read only)
- สร้างข้อมูล
- บ้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๒.๒) กำหนดเกณฑ์การระงับสิทธิ์การมอบอำนาจให้เป็นไปตามการบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๒.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาต เป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓. ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๓.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ระบบบริหารจัดการเชิงยุทธศาสตร์ (Estimate) ระบบสารสนเทศทรัพยากรบุคคลระดับกรม (DPIS) ข้อมูลงบประมาณการเงินและบัญชี (GFMS) เป็นต้น
- ข้อมูลสารสนเทศด้านข้อมูลโรคและภัยสุขภาพ เช่น ข้อมูลPink form ข้อมูลโรคเอดส์ ข้อมูลด้านโรคไม่ติดต่อ ข้อมูลโรคติดต่อ นำโดยแมลง เป็นต้น

(๓.๒) จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด ความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด ความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด ความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๓.๕) การกำหนดเวลาที่ได้เข้าถึง

(๓.๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ ๒. ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกัน ผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวดที่ ๑ ข้อ ๑๒.

ข้อ ๔. หน่วยงานเจ้าของฐานข้อมูลผู้มีสิทธิ์และอำนาจในสายงานเป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้า-ออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูล จากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับ หน่วยงานภายนอก ดังต่อไปนี้

- (๑) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง
- (๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกัน หรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น
- (๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล
- (๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูล เพื่อเป็นการป้องกันการปฏิเสธ

- (๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น
- (๖) กำหนดสิทธิ์การเข้าถึงข้อมูล
- (๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์
- (๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส ( Key Encryption) เป็นต้น

## ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๖. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพ พร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ ๗. ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ ๘. ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙. ต้องกำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- (๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- (๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล
- (๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา/ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- (๔) ตรวจสอบการตั้งค่า (Configuration) ต่าง ๆ ของระบบการสำรองข้อมูล
- (๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
- (๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้เกิดผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน
- (๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- (๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- (๙) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- (๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น
- (๑๑) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูล (Encryption) กับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ ๑๐. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการ ทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

- (๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
- (๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
- (๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
- (๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
- (๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
- (๖) การสร้างความตระหนัก หรือให้ความรู้กับเจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ ๑๑. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้ อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒. ต้องมีการกำหนดหน้าที่ และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อ ๑๓. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผน เตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ข้อ ๑๔. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง



## หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

### วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นได้กับระบบสารสนเทศ
๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

### แนวปฏิบัติ

#### ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัย สารสนเทศ โดยมีแนวทางการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

- ข้อ ๑. จัดลำดับความสำคัญของความเสี่ยง
- ข้อ ๒. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง
- ข้อ ๓. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง
- ข้อ ๔. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้
- ข้อ ๕. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
- ข้อ ๖. มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

- (๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
- (๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี
- (๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหาร จัดการความมั่นคงปลอดภัย
- (๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบรวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ
- (๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนี้จากการเข้าถึงโดยไม่ได้รับอนุญาต

#### ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ได้กำหนดแนวทางการดำเนินงานเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

- (๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้าน สารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human error ลดน้อยลง
- (๒) จัดทำหนังสือแจ้งเวียนหน่วยงานทั้งส่วนกลางและส่วนภูมิภาค เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse), และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

- (๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก
- (๒) ติดตั้งซอฟต์แวร์ Anti virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำให้ความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

- (๑) ติดตั้งอุปกรณ์สำรองระบบไฟฟ้า เช่น เครื่องสำรองไฟฟ้า(UPS) , เครื่องกำเนิดไฟฟ้า (Generator) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย
- (๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟ เกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ
- (๓) ติดตั้งอุปกรณ์ดับเพลิงอัตโนมัติ สำหรับห้องควบคุมระบบคอมพิวเตอร์ เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรง ที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

- (๑) เผื่อระวางภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยา ตลอดเวลา
- (๒) อุปกรณ์สำรองข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย
- (๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรกเกอร์เครื่องปรับอากาศ เพื่อป้องกัน เครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า
- (๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายไว้ในที่สูง
- (๕) กรณีน้ำลดลงเรียบร้อยแล้ว ให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่า สามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่าย สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย
- (๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งาน ของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่า สามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่าย ได้หรือไม่
- (๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูล ได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

## หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

### วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งาน หรือ เข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งาน ระบบเทคโนโลยีสารสนเทศของหน่วยงาน

### แนวปฏิบัติ

ข้อ ๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

- (๑) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี
- (๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออกของบุคคลเป็นจำนวนมาก
- (๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ในสถานที่ดังกล่าว
- (๔) จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่
- (๕) หากจำเป็นต้องใช้เครื่องพิมพ์ เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว
- (๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เว้นแต่ได้รับอนุญาต
- (๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศติดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

- (๑) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้ รับผิดชอบ รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้
- (๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้ง จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔. การควบคุมการเข้า-ออกอาคารสถานที่

- (๑) กำหนดสิทธิ์ผู้ใช้งานที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มิสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

- (๒) การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอกหรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตร ประชาชน ใบอนุญาตเข้าช้ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและ รับบแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)
- (๓) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)
- (๔) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน
- (๕) บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน
- (๖) จัดเก็บบันทึกการเข้า - ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น Data Center เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น
- (๗) ควบคุมดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต
- (๘) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และ ต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว
- (๙) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ
- (๑๐) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่เสมอ
- (๑๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต
- (๑๒) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การสแกนนิ้วมือ เป็นต้น เพื่อควบคุมการเข้า- ออกในพื้นที่หรือบริเวณที่มีความสำคัญ
- (๑๓) จัดให้มีการกำกับและควบคุม เพื่อเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานใน พื้นที่หรือบริเวณที่มีความสำคัญ
- (๑๔) จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

- (๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้
  - ระบบสำรองกระแสไฟฟ้า (UPS)
  - เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
  - ระบบระบายอากาศ (Ventilation System)
  - ระบบปรับอากาศ และควบคุมความชื้น (Air Conditioner)
- (๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๒ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ
- (๓) การติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีจากระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ (Cabling Security)

- (๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้
- (๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย
- (๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน
- (๔) ทำป้ายชื่อสำหรับสายสัญญาณ (Label) และบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น
- (๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง
- (๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก
- (๗) พิจารณาใช้งานสายไฟเบอร์ออปติกแทนสายสัญญาณสื่อสารแบบเดิม สำหรับระบบสารสนเทศที่สำคัญ
- (๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

- (๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต
- (๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามผู้ผลิตแนะนำ
- (๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง
- (๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- (๕) กำกับและควบคุมการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน
- (๖) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับ อนุญาต

ข้อ ๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

- (๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน
- (๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน
- (๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน
- (๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย
- (๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็น หลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

- (๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์
- (๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้ในที่สาธารณะ
- (๓) เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

- (๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว
- (๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกัน ไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

## หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

### วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

### แนวปฏิบัติ

#### ข้อ ๑. ระบบป้องกันผู้บุกรุก

- (๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำ การตรวจสอบมีดังต่อไปนี้
  - มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
  - ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
  - ระดับความรุนแรงมากน้อยเพียงใด
  - หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

#### ข้อ ๒. ระบบไฟร์วอลล์

- (๑) ดำเนินการตรวจสอบระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง
- (๒) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้
  - Package ที่ไฟร์วอลล์ได้ทำการ Block
  - ลักษณะของ Package ที่ถูก Block
  - Package ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก
- (๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศ ให้แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ ๓. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

- (๑) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบ ป้องกัน ภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้
  - มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
  - มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
  - มีการส่งมัลแวร์จากเครือข่ายภายในกรมควบคุมโรคไปยังภายนอกหรือไม่
- (๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจาย อยู่ในเครือข่ายของกรมควบคุมโรค
- (๓) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที



## หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

### วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของกรมควบคุมโรค
๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย
๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

### แนวปฏิบัติ

๑. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง
๒. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรม โดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน
๓. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนา มีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดรวมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้
๔. ตีตประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ
๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน
๖. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร
๗. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน
๘. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบของกรมควบคุมโรค และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

## หมวดที่ ๗ หน้าที่และความรับผิดชอบ

### วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

### แนวปฏิบัติ

ข้อ ๑. **ระดับนโยบาย** ผู้รับผิดชอบ ได้แก่

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCO/CIO)
  - ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค หรือเทียบเท่าระดับผู้อำนวยการ
- (๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ
- (๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตาม นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒. **ระดับบริหาร** ผู้รับผิดชอบ ได้แก่ หัวหน้ากลุ่มงาน หรือผู้ที่ได้รับมอบหมายให้เทียบเท่า

- (๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและ เทคโนโลยีสารสนเทศ
- (๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบ ฐานข้อมูล

ข้อ ๓. **ระดับปฏิบัติ** ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการกรมควบคุมโรค เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่พนักงานคอมพิวเตอร์

- (๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- (๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ
- (๓) รับผิดชอบกำกับ ควบคุมการรักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
- (๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด
- (๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต
- (๖) รับผิดชอบในการรักษาความปลอดภัยระบบอินเทอร์เน็ต
- (๗) ปฏิบัติตามแนวปฏิบัติที่เกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ของกระทรวงสาธารณสุขประกาศไว้
- (๘) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรค

## หมวดที่ ๘ การบริหารจัดการการใช้บริการจากหน่วยงานภายนอก

### วัตถุประสงค์

เพื่อให้หน่วยงานภายนอก ได้ปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรค ทำให้ระบบสารสนเทศดำเนินไปได้อย่างต่อเนื่องและมีประสิทธิภาพ

### แนวปฏิบัติ

ข้อ ๑. ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูลและระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

ข้อ ๒. การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของหน่วยงานจากหน่วยงานภายนอกต้องมีการขออนุญาตอย่างเป็นทางการ และได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

ข้อ ๓. การบริการ และการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตาม นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่าง ๆ ของกรมควบคุมโรค

ข้อ ๔. ผู้ดูแลระบบต้องให้สิทธิ์การเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น

ข้อ ๕. ต้องมีการทำสัญญาการรักษาความลับขององค์กร ระหว่างหน่วยงานและหน่วยงานภายนอก ที่เข้ามาปฏิบัติงานก่อนเปิดให้ใช้บริการระบบเสมอ

ข้อ ๖. ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน และวิธีการดำเนินงาน เป็นอย่างน้อยเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการให้เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และเป็นไปตามขอบเขตที่ได้กำหนดไว้

ข้อ ๗. สัญญาระหว่างหน่วยงาน และ หน่วยงานภายนอก ในการให้บริการต้องระบุถึงหัวข้อต่าง ๆ ดังต่อไปนี้ เป็นอย่างน้อย

- รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ
- ระดับการให้บริการ (Service Level)
- หน้าที่และความรับผิดชอบขององค์กรและหน่วยงานภายนอก ในการให้บริการในครั้งนั้น
- ระยะเวลาในการให้บริการ และการตรวจรับงานบริการในครั้งนั้น
- ราคา และเงื่อนไขการชำระเงิน
- ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อหรือพัฒนาขึ้น (ถ้ามี)
- การรักษาความลับของข้อมูลที่ได้รับจากการให้บริการแก่องค์กร

# ภาคผนวก

## แนวปฏิบัติ เมื่อเกิดฟิชซิง (Phishing) ที่เว็บไซต์เวอร์ของหน่วยงาน (ภาคผนวก ๑)

### วัตถุประสงค์

เพื่อกำหนดมาตรการในการแก้ไขปัญหาการเกิดฟิชซิง (Phishing) ให้สามารถดำเนินการได้อย่างรวดเร็ว ไม่ให้เกิดความเสียหาย และส่งผลกระทบต่อหน่วยงานทั้งภายในและภายนอกที่ใช้งานระบบสารสนเทศ

### แนวปฏิบัติ

ข้อ ๑. เมื่อผู้ดูแลระบบเครือข่ายของหน่วยงานได้รับแจ้งหรือตรวจพบว่าเว็บไซต์เวอร์ของหน่วยงานใด ๆ เป็นช่องทางให้ผู้ไม่หวังดีทำฟิชซิง (Phishing) ผู้ดูแลระบบของกรมควบคุมโรคจะดำเนินการ ดังนี้

- (๑) ดำเนินการบล็อก IP Address ของเว็บไซต์เวอร์ที่โดนฟิชซิงนั้น หรือแจ้งผู้ให้บริการเส้นทางเครือข่ายของหน่วยงานดำเนินการโดยเร่งด่วน
- (๒) แจ้งผู้ดูแลเว็บไซต์เวอร์ของหน่วยงานที่ถูกทำฟิชซิงทาง E-Mail หรือทางโทรศัพท์ เพื่อให้ดำเนินการแก้ไขปัญหา

ข้อ ๒. เมื่อหน่วยงานดำเนินการแก้ไขปัญหาเรียบร้อยแล้ว ให้ประสานไปยังเมื่อผู้ดูแลระบบเครือข่ายของกรมควบคุมโรค หรือผู้ให้บริการเส้นทางเครือข่ายของหน่วยงาน เพื่อปลดบล็อก IP Address

ข้อ ๓. ผู้ดูแลเว็บไซต์เวอร์ของหน่วยงานต้องตรวจสอบเว็บไซต์เวอร์และเว็บไซต์ภายในหน่วยงานของตนเอง รวมทั้งติดตั้งโปรแกรมปรับปรุงช่องโหว่ (Patch) อย่างสม่ำเสมอ เพื่อป้องกันผู้ที่ไม่หวังดีในการเข้ามาทำฟิชซิง

## แนวปฏิบัติ เมื่อเกิดมัลแวร์ ที่เว็บไซต์เวอร์ของหน่วยงาน (ภาคผนวก ๑)

### วัตถุประสงค์

เพื่อกำหนดมาตรการในการแก้ไขปัญหาและสามารถดำเนินการป้องกันได้อย่างรวดเร็ว ไม่ให้เกิดความเสียหาย และส่งผลกระทบต่อหน่วยงานทั้งภายในและภายนอกที่ใช้งานระบบสารสนเทศ ดังนี้

### แนวปฏิบัติ จากมัลแวร์เรียกค่าไถ่ Ransomware

ข้อ ๑. สำหรับผู้ใช้งาน

๑. ทำการ Update ระบบปฏิบัติการ (OS) Windows
๒. ทำการติดตั้งและ Update โปรแกรม Antivirus ให้เป็นเวอร์ชันปัจจุบัน
๓. หลีกเลี่ยงติดตั้งโปรแกรม หรือ Application ที่ไม่น่าเชื่อถือ
๔. ไม่เข้า Web Site ที่ไม่น่าเชื่อถือ
๕. ไม่เปิด E-mail ที่มีไฟล์แนบที่ไม่รู้แหล่งที่มา
๖. ทำการ Backup ข้อมูลในเครื่องคอมพิวเตอร์เป็นประจำ
๗. มีการตระหนักรู้ด้านความมั่นคงปลอดภัยระบบสารสนเทศพื้นฐาน
๘. เมื่อติดมัลแวร์เรียกค่าไถ่ (Ransomware) หรือตกเป็นเหยื่อ ให้ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์กับระบบเครือข่ายคอมพิวเตอร์ขององค์กรและเครือข่ายอินเทอร์เน็ต โดยแจ้งผู้ดูแลด้านเทคโนโลยีสารสนเทศหรือ IT ระบบทราบทันที

- ข้อ ๒. เมื่อผู้ดูแลระบบเครือข่ายของหน่วยงาน ได้รับแจ้งหรือตรวจพบว่าเว็บเซิร์ฟเวอร์ (Web Server ) ของหน่วยงานใด ๆ ติดมัลแวร์เรียกค่าไถ่ ผู้ดูแลระบบของกรมควบคุมโรค มีขั้นตอนปฏิบัติงาน ดังนี้
๑. ตัดการเชื่อมต่อเครื่องแม่ข่ายกับระบบเครือข่าย Web Server
  ๒. ทำการ Restore ระบบ
  ๓. ทำการ Update Patch ให้เป็นปัจจุบัน
  ๔. ใช้ Software Anti-Virus และ Anti-Malware ที่ถูกต้องตามลิขสิทธิ์ และ ทำการ Full Scan
  ๕. ทำการปิด System restore ชั่วคราว
  ๖. ตรวจสอบ Host File เพื่อตรวจสอบความผิดปกติของค่าที่กำหนดไว้
  ๗. ตรวจสอบ Account ของผู้มีสิทธิ์ใช้งาน หากพบ Account แปลกปลอมให้ทำการลบออกจากระบบ
  ๘. เปลี่ยน Password ใช้งาน โดยกำหนดความยาวอย่างน้อย ๘ ตัวอักษรประกอบด้วย ตัวพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ เช่น . @ \* & % \$ !
  ๙. ตรวจสอบ Port ของเครื่องแม่ข่าย (Server) และเปิดใช้งานเฉพาะ Port ที่ใช้งานเท่านั้น
  ๑๐. แจ้งหน่วยงานที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ (Thaicert) ทางระบบไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) : report@thaicert.or.th

#### การป้องกันการติดมัลแวร์เรียกค่าไถ่ Ransomware

- ๒.๑.๑ ใช้ Microsoft Applocker เพื่อทำการblock การรันไฟล์มัลแวร์เรียกค่าไถ่ (เช่น ไฟล์ .exe, .js, .vbs) จากไดเรกทอรีที่เก็บไฟล์มัลแวร์ รายละเอียดเพิ่มเติมเกี่ยวกับApplocker ดูได้จากเว็บไซต์ของ Microsoft  
([https://technet.microsoft.com/enus/library/dd๗๕๙๑๑๗\(v=ws.๑๑\).aspx](https://technet.microsoft.com/enus/library/dd๗๕๙๑๑๗(v=ws.๑๑).aspx))
- ๒.๑.๒ กำหนดสิทธิ์การเข้าถึง File และการทำงานของโปรแกรม
- ๒.๑.๓ ทำการติดตั้งและ Update โปรแกรม Anti-virus หรือ Anti - Malware ให้เป็นเวอร์ชันปัจจุบัน
- ๒.๑.๔ ทำการ Update patch ระบบปฏิบัติการให้เป็นปัจจุบัน
- ๒.๑.๕ ใช้ software ที่ถูกต้องตามลิขสิทธิ์

#### แนวปฏิบัติ จากมัลแวร์ Cryptojacking

ข้อ ๑. สำหรับผู้ใช้งาน

๑. ทำการ Update ระบบปฏิบัติการ (OS) Windows
๒. ทำการติดตั้งและ Update โปรแกรม Antivirus ให้เป็นเวอร์ชันปัจจุบัน
๓. ไม่เข้า Web Site ที่ไม่น่าเชื่อถือ
๔. ไม่เปิด E-mail ที่มีไฟล์แนบที่ไม่รู้แหล่งที่มา
๕. ไม่ดาวน์โหลดไฟล์จาก Web site ที่ไม่น่าเชื่อถือ
๖. ทำการ Backup ข้อมูลในเครื่องคอมพิวเตอร์เป็นประจำ
๗. มีการตระหนักรู้ด้านความมั่นคงปลอดภัยระบบสารสนเทศพื้นฐาน

๘. เมื่อติดมัลแวร์ Cryptocurrency Mining ให้ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์กับระบบเครือข่ายคอมพิวเตอร์ขององค์กรและเครือข่ายอินเทอร์เน็ต โดยแจ้งผู้ดูแลด้านเทคโนโลยีสารสนเทศหรือ IT ระบบทราบทันที

ข้อ ๒. เมื่อผู้ดูแลระบบเครือข่ายของหน่วยงาน ได้รับแจ้งหรือตรวจพบว่าเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่ายของหน่วยงานใด ๆ ติดมัลแวร์ Cryptojacking ผู้ดูแลระบบของกรมควบคุมโรค มีขั้นตอนปฏิบัติงาน ดังนี้

๑. ทำการตัดการเชื่อมต่อเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่ายกับระบบเครือข่าย
๒. ทำการ Restore ระบบ หรือเครื่องคอมพิวเตอร์ที่มีการติดมัลแวร์ Cryptojacking
๓. ทำการ Update Patch ให้เป็นปัจจุบัน
๔. ใช้ Software Anti-Virus และ Anti-Malware ที่ถูกต้องตามลิขสิทธิ์ และ ทำการ Full Scan
๕. ทำการปิด System restore ชั่วคราว
๖. ตรวจสอบความผิดปกติของ File หรือ Application ที่กำหนดไว้
๗. ตรวจสอบ Account ของผู้มีสิทธิ์ใช้งาน หากพบ Account แปลกปลอมให้ทำการลบออกจากระบบ
๘. กำหนดให้มีการ Login ใช้งานระบบ โดยผ่านการ VPN และตรวจสอบ Port ของเครื่องแม่ข่าย (Server) และเปิดใช้งานเฉพาะ Port ที่ใช้งานเท่านั้น
๙. เปลี่ยน Password ใช้งานโดยกำหนดความยาวอย่างน้อย ๘ ตัวอักษรประกอบด้วย ตัวพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ เช่น .@ \* & % \$ !