ประกาศกระทรวงสาธารณสุข
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน
ของกระทรวงสาธารณสุข พ.ศ. ๒๕๕๔

ด้วยปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทำให้ผู้ประกอบการตลอดจนองค์กร ภาครัฐ และภาคเอกชนที่มีการดำเนินงานใด ๆ ในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ขาดความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกรูปแบบ ประกอบกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตระหนักถึงความจำเป็นที่จะส่งเสริมและผลักดันให้ประเทศสามารถยกระดับการแข่งขันกับประเทศอื่น ๆ โดยการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย จึงเห็นความสำคัญที่จะนำกฎหมาย ข้อบังคับต่าง ๆ มาบังคับใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งในส่วนที่ต้องกระทำและในส่วนที่ต้องงดเว้นการกระทำ เพื่อช่วยให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล กระทรวงสาธารณสุข จึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของกระทรวงสาธารณสุข

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกระทรวงสาธารณสุข ว่าด้วยการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของกระทรวงสาธารณสุข พ.ศ. ๒๕๕๔

ข้อ ๒ ประกาศนี้จัดทำขึ้นเพื่อให้สอดคล้องกับระเบียบปฏิบัติด้านความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข และประกาศ กระทรวงสาธารณสุข เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงสาธารณสุข

ข้อ ๓ ประกาศนี้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๔ บรรดา ประกาศ ระเบียบและคำสั่งอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดกับระเบียบนี้ให้ใช้ระเบียบนี้แทน

ข้อ ๕ ประกาศนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ ลูกจ้าง และพนักงานราชการ ที่ปฏิบัติงานเกี่ยวข้องกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวข้องกับระบบสารสนเทศ ของกระทรวงสาธารณสุข

ส่วนที่ ๑
กล่าวทั่วไป

ข้อ ๑ ประกาศนี้จัดทำขึ้นเพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยระบบสารสนเทศของกระทรวงสาธารณสุข กำหนดข้อปฏิบัติและแนวทางการดำเนินการ เพื่อให้

สอดคล้องกับนโยบายและภารกิจของกระทรวงสาธารณสุข และเกิดความมั่นคงปลอดภัยมากที่สุด ประกอบด้วยนโยบาย ดังต่อไปนี้

(๑) นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy)
(๒) นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)
(๓) นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)
(๔) นโยบายความมั่นคงปลอดภัยของอีเมล์(E-mail Policy)
(๕) นโยบายความมั่นคงปลอดภัยของอินเตอร์เน็ต (Internet Security Policy)
(๖) นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access control Policy)
(๗) นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก
(๘) นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
(๙) นโยบายการรักษาความปลอดภัยฐานข้อมูล (Database Security)
(๑๐) นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)
(๑๑) นโยบายการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม (Physical and Environment Security)

ข้อ ๒ นิยามศัพท์ต่าง ๆ

๒.๑. “**กระทรวงสาธารณสุข**" หมายถึง ส่วนราชการ หน่วยงานเจ้าของทรัพย์สิน

๒.๒. "**ผู้ใช้งาน**" หมายถึง ข้าราชการ ลูกจ้าง และพนักงานราชการ ที่ปฏิบัติงานเกี่ยวข้องกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวข้องกับระบบสารสนเทศ ของกระทรวงสาธารณสุข

๒.๓. “**ผู้ดูแลระบบ**” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๒.๔. “**สิทธิผู้ใช้งาน**” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้ทรัพย์สิน

๒.๕. “**หน่วยงาน**” หมายถึง ราชการส่วนกลางและส่วนภูมิภาคในสังกัดกระทรวงสาธารณสุข และหน่วยงานที่มีฐานะเทียบเท่ากองที่กระทรวงสาธารณสุข กรม จัดตั้งขึ้น

๒.๖. “**ทรัพย์สินสารสนเทศ**” หมายถึง

(๑) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
(๒) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด
(๓) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๒.๗. **“ระบบสารสนเทศ”** (Information System) หมายความว่า ระบบข่าวสารของกระทรวงสาธารสุข ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสารมาช่วยในการสร้างสารสนเทศที่กระทรวงสาธารสุข สามารถนำมาใช้ในการวางแผน การบริหาร การพัฒนาและควบคุม ซึ่งมีองค์ประกอบดังนี้

๒.๗.๑. ระบบคอมพิวเตอร์ (Computer System)
๒.๗.๒. ระบบสื่อสาร (Communication System)
๒.๗.๓. สารสนเทศ (Information) ที่ดำเนินการในระบบคอมพิวเตอร์ และระบบสื่อสาร

๒.๘. **“ระบบคอมพิวเตอร์”** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๒.๙. **“ระบบสื่อสาร”** (Communication System) หมายความว่า ระบบที่ประกอบด้วย ผู้รับ ผู้ส่ง และสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล (ตัวอักษร ตัวเลข ภาพ เสียง เป็นต้น) ทั้งระบบวงจรทางสาย เช่น สายเคเบิล (Cable) โคแอกเชียล (Coaxial Cable) วิทยาการเส้นใยนำแสง (Fiber Optic) และระบบไร้สาย เช่น ไมโครเวฟ (Microwave) ดาวเทียม (Satellite) รวมทั้งอุปกรณ์อื่น ๆ เช่น ฮับ (Hub) การสลับ (Switching) อุปกรณ์จัดเส้นทาง (Router)

๒.๑๐.**“สารสนเทศ”** (Information) หมายความว่า ข้อเท็จจริงที่ได้จากการสกัด ข้อมูลให้มีความหมาย โดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความหรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย เช่น รายงาน ตาราง แผนภูมิเป็นต้น และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๒.๑๑.**“ระบบเครือข่าย”** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

๒.๑๒. **“ระบบเทคโนโลยีสารสนเทศ”** หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

๒.๑๓.**“เครื่องคอมพิวเตอร์”** หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

๒.๑๔. **“ข้อมูลคอมพิวเตอร์”** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๒.๑๕. **“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ”** หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๒.๑๖.**“ความมั่นคงปลอดภัยด้านสารสนเทศ”** หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

๒.๑๗. **“ความเสี่ยง** (Risk)” หมายความว่า โอกาสของการเกิดภัยในรูปแบบที่เหมาะกับ

๒.๑๘. **“ประเมินความเสี่ยง”** (Risk Assessment) หมายความว่า กระบวนการวิเคราะห์ภัยและความอ่อนแอของระบบสารสนเทศ รวมทั้งผลกระทบจากการสูญเสียสารสนเทศ หรือการสูญเสียความสามารถในการรักษาความปลอดภัยของระบบสารสนเทศ การประเมินความเสี่ยง ใช้เป็นพื้นฐานในการกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสมให้ระบบสารสนเทศต่อไป

ข้อ ๓ นิยามศัพท์ต่าง ๆ ที่ไม่ได้กำหนดไว้ในระเบียบนี้ ให้ยึดถือตามระเบียบนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๒
แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy)

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กระทรวงสาธารณสุข เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกระทรวงสาธารณสุข ให้อยู่ระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC 27001 อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของกระทรวงสาธารณสุข

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ กระทรวงสาธารณสุข ประกอบด้วย ๘ หมวด โดยมีรายละเอียดดังต่อไปนี้

หมวด ๑ ว่าด้วยการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

ข้อ ๑. ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๒. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๓. ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

ข้อ ๔. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๖๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๕. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของกระทรวงสาธารณสุข และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดยล็อคก็ดี หรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

(๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
(๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง
(๓) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้
(๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง
(๖) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๕ นาที

หมวด ๒ ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

ข้อ ๖. ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) กระทรวงสาธารณสุขที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๗. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๘. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๙. ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

ข้อ ๑๐. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

ข้อ ๑๑. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่กระทรวงสาธารณสุขมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยบรรดารายการทรัพย์สิน (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบจะอยู่แนบท้ายเอกสารข้อบังคับนี้การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่กระทรวงสาธารณสุขมอบหมาย

ข้อ ๑๒. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของกระทรวงสาธารณสุขที่ได้รับมอบหมาย

ข้อ ๑๓. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๑๔. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊ค ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ ๑๕. ทรัพย์สินและระบบสารสนเทศต่างๆ ที่กระทรวงสาธารณสุข จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของกระทรวงสาธารณสุขเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่กระทรวงสาธารณสุขไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อกระทรวงสาธารณสุข

ข้อ ๑๖. ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๑๕ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด ๓ ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ ๑๗. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของกระทรวงสาธารณสุข หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๘. ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของกระทรวงสาธารณสุข ถือเป็นทรัพย์สินของกระทรวงสาธารณสุข ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๑๙. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของกระทรวงสาธารณสุข หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๐. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ ๒๑. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กระทรวงสาธารณสุข จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น

ยกเว้นในกรณีที่กระทรวงสาธารณสุข ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับกระทรวงสาธารณสุข ซึ่งกระทรวงสาธารณสุขอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด ๔ ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ ๒๒. มีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๒๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์(Bittorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๒๔. ห้ามเปิดหรือใช้งาน (Run) โปรแกรม ออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๒๕. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของกระทรวงสาธารณสุขที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของกระทรวงสาธารณสุข

ข้อ ๒๖. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของกระทรวงสาธารณสุขเพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกระทรวงสาธารณสุข

ข้อ ๒๗. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกระทรวงสาธารณสุขเพื่อประโยชน์ทางการค้า

ข้อ ๒๘. ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของกระทรวงสาธารณสุข โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ ๒๙. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของกระทรวงสาธารณสุข ต้องหยุดชะงัก

ข้อ ๓๐. ห้ามใช้ระบบสารสนเทศของกระทรวงสาธารณสุข เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๓๑. ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๒. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของกระทรวงสาธารณสุข โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด ๕ การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

ข้อ ๓๓. จัดให้มีการทำ และปรับปรุงนโยบายด้านความมั่นคงปลอดภัยอย่างสม่ำเสมออย่างน้อยปีละ ๒ ครั้ง

ข้อ ๓๔. แสดงเจตนารมณ์ หรือสื่อสารให้เจ้าหน้าที่ทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยขององค์กรโดยเคร่งครัด อย่างสม่ำเสมอ

ข้อ ๓๕. จัดให้มีการประชุมเกี่ยวกับการบริหารจัดการด้านความมั่นคงปลอดภัยอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง โดยกำหนดให้มีวาระการประชุมที่ต้องหารือกันอย่างน้อยดังนี้

(๑) การตรวจสอบการปฏิบัติตามนโยบายความมั่นคงฯ และผลการตรวจสอบ

(๒) แผนการดำเนินการเชิงป้องกัน/แก้ไข จากผลการตรวจสอบดังกล่าว

(๓) การปรับปรุงนโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป

(๔) การประเมินความเสี่ยงและแผนลดความเสี่ยง รวมทั้งจัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่เพียงพอต่อการจัดการดังกล่าว

ข้อ ๓๖. จัดให้มีการสร้างความตระหนักทางด้านความมั่นคงปลอดภัยเพื่อให้เจ้าหน้าที่ขององค์กรมีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้ในเบื้องต้น อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๓๗. จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศ ปีละ ๑ ครั้ง และจัดให้มีการทำแผนเพื่อลดความเสี่ยง หรือปัญหาที่พบ

ข้อ ๓๘. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัย โดยผู้ตรวจสอบภายในด้านสารสนเทศ ปีละ ๑ ครั้ง และจัดให้มีการทำแผนเพื่อปรับปรุง หรือแก้ไขปัญหาที่พบ

ข้อ ๓๙. จัดให้มีการแจ้งเวียนให้เจ้าหน้าที่ทั้งหมดได้ระมัดระวัง และดูแลทรัพย์สินขององค์กรที่ตนเองใช้งาน เพื่อป้องกันการสูญหาย อย่างน้อยปีละ 1 ครั้ง

ข้อ ๔๐. กำหนดนโยบายการใช้งานระบบเครือข่ายอย่างชัดเจนว่า บริการใดที่อนุญาตให้ใช้งาน และบริการใดไม่อนุญาตให้ใช้งาน เช่น การใช้งาน MSN ดูหนังฟังเพลงผ่านทางอินเตอร์เน็ต เป็นต้น รวมทั้งปรับปรุงนโยบายตามความจำเป็น นโยบายการใช้งานระบบเครือข่าย ขณะนี้ประกอบด้วย

(๑) ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

- การพนัน
- วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และ พระมหากษัตริย์
- ลามก อนาจาร
- อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม

(๒) ห้ามเล่นเกมส์ ดูภาพยนต์ หรือฟังเพลง ผ่านทางอินเทอร์เน็ตในเวลาทำงาน

หมวด ๖ ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

ข้อ ๔๑. กระทรวงสาธารณสุข ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่กระทรวงสาธารณสุข อนุญาตให้ใช้งานหรือที่กระทรวงสาธารณสุข มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และกระทรวงสาธารณสุขห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ กระทรวงสาธารณสุขถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๔๒. ซอฟต์แวร์ (Software) ที่กระทรวงสาธารณสุขได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด ๗ ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing MalWare)

ข้อ ๔๓. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่กระทรวงสาธารณสุข ได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๔๔. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๔๕. ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๔๖. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๔๗. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และ ต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๔๘. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆที่เป็นทรัพย์สินของกระทรวงสาธารณสุข หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๔๙. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของกระทรวงสาธารณสุข

หมวด ๘ ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

ข้อ ๕๐. บรรดากฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบ ของกระทรวงสาธารณสุข ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

- - - - - - - - - - - - - - - -

๒.๒ นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำ อุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๗ ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บัญชาการกระทรวงสาธารณสุขทราบทันที

ข้อ ๘ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

- - - - - - - - - - - - - - - -

๒.๓ นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

ข้อ ๑ กระทรวงสาธารณสุข มีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของไฟร์วอลล์ทั้งหมด

ข้อ ๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ ๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

ข้อ ๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

ข้อ ๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางกระทรวงสาธารณสุข อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากกระทรวงสาธารณสุข ก่อน

ข้อ ๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๒ กระทรวงสาธารณสุข มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มี ความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจาก กระทรวงสาธารณสุขก่อน

ข้อ ๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

- - - - - - - - - - - - - - - -

๒.๔ นโยบายความมั่นคงปลอดภัยของอีเมล์(E-mail Policy)

ข้อ ๑ ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่กระทรวงสาธารณสุข

ข้อ ๒ เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ ๓ ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๔ ควรเปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือน

ข้อ ๕ ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

ข้อ ๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๗ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลอีเมล์ที่องค์กรกำหนดไว้ ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่อีเมล์ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๘ ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๙ ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๙ ห้ามส่งอีเมล์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อ ๑๐ ห้ามส่งอีเมล์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๑ ให้ระบุชื่อของผู้ส่งในอีเมล์ทุกฉบับที่ส่งไป

ข้อ ๑๒ ให้ทำการสำรองข้อมูลอีเมล์ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าองค์กรจะทำการสำรองข้อมูลอีเมล์ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้นอีเมล์ที่เก่ามากๆ และจำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

- - - - - - - - - - - - - - - -

๒.๕ นโยบายความมั่นคงปลอดภัยของอินเตอร์เน็ต (Internet Security Policy)

ข้อ ๑ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๓ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๔ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ ๖ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

- - - - - - - - - - - - - - - -

๒.๖ นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access control Policy)

หมวด ๑ การควบคุมการเข้าถึงระบบสารสนเทศ

ข้อ ๑ กระทรวงสาธารณสุข กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บัญชาการสำนักงานกระทรวงสาธารณสุข

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

หมวด ๒ การบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของกระทรวงสาธารณสุข ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๓) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(๔) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๕) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

(๕) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

- - - - - - - - - - - - - - -

๒.๗ นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

ข้อ ๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในกระทรวงสาธารณสุข ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของกระทรวงสาธารณสุขและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๔ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๕ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

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

ข้อ ๗ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๙ เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๑๐ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

ข้อ ๑๑ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๓ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๔ กระทรวงสาธารณสุข มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๕ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของกระทรวงสาธารณสุข การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของกระทรวงสาธารณสุข จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

- - - - - - - - - - - - - - - -

๒.๘ นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

ข้อ ๑ กระทรวงสาธารณสุข กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

ข้อ ๒ ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บัญชาการกระทรวงสาธารณสุข และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

ข้อ ๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บัญชาการกระทรวงสาธารณสุข และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

ข้อ ๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

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

(๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

(๗) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๙) การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๗ กระทรวงสาธารณสุข กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

(๑) ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

(๒) ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

(๓) ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

(๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ ๘ กระทรวงสาธารณสุข กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

(๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บัญชาการกระทรวงสาธารณสุข

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๓) วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้บัญชาการกระทรวงสาธารณสุข

(๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(๕) การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

- ----------

๒.๙ นโยบายการรักษาความปลอดภัยฐานข้อมูล (Database Security)

ข้อ ๑ นโยบายนี้ความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันฐานข้อมูลจากการเข้าถึง การเปลี่ยนแปลงการโอนถ่ายข้อมูลหรือการกระทำใด ๆ โดยผู้ไม่เกี่ยวข้อง ตลอดจนการเตรียมระบบสำรองและการฟื้นฟูระบบ

ข้อ ๒ ข้อมูล ข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓ ข้อมูลที่เป็นความลับโดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ ๔ ส่วนราชการเจ้าของฐานข้อมูล ผู้มีสิทธิและอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้และโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ์และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ใน การตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างราชการให้จัดทำข้อตกลงการใช้

- ----------

๒.๑๐ นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)

ข้อ ๑ จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

ข้อ ๒ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

ข้อ ๓ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

ข้อ ๔ ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

- ----------

๒.๑๑ การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม (Physical and Environment Security)

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

ข้อ ๒. ห้องเครื่องคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

๒.๑. กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

๒.๒. ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก

๒.๓. จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายใน สถานที่ดังกล่าว

๒.๔. จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่าง หรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่อยู่

๒.๕. หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจากบริเวณดังกล่าว

๒.๖. ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

๒.๗. จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากร สารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๓. การรักษาความปลอดภัยทางด้านกายภาพของระบบ เพื่อประโยชน์ให้ติดตั้งอุปกรณ์ รักษาความปลอดภัย ณ สถานที่ตั้งระบบให้บริการ ด้วยเทคโนโลยีที่เหมาะสมและทันสมัย

ข้อ ๔. ให้เจ้าหน้าที่ของกระทรวงสาธารณสุขซึ่งได้รับมอบหมาย หรือได้รับอนุญาตเท่านั้น เป็นผู้มีสิทธิ์เข้าถึง หรือเข้า-ออกบริเวณพื้นที่ ที่เป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะ

ข้อ ๕. ต้องกำหนดให้มีการป้องกันรักษาความปลอดภัยเครื่องคอมพิวเตอร์และอุปกรณ์ ประกอบที่สามารถเคลื่อนย้ายได้ และหรืออยู่นอกพื้นที่ควบคุม เมื่อถูกนำไปใช้งานนอกสถานที่ ต้องกำหนดการปฏิบัติในการใช้งาน การยืม/คืน และอื่นๆ ให้สอดคล้องกับระเบียบว่าด้วยการรักษาความปลอดภัยอย่างรัดกุม

ข้อ ๖. ระบบไฟฟ้าและระบบปรับอากาศ จะต้องมีความปลอดภัยและเหมาะสม โดยจัดให้ มีระบบไฟฟ้าสำรองเพื่อใช้งานเมื่อไฟฟ้าขัดข้อง และระบบปรับอากาศสำรองเพื่อควบคุมและรักษาอุณหภูมิและความชื้นของห้องให้คงที่

ข้อ ๗. ต้องมีการป้องกันรักษาความปลอดภัยระบบสายไฟและเคเบิล โดยเดินสายไฟฟ้า หรือสายเคเบิลผ่านช่องทางพิเศษที่จัดไว้ ซึ่งต้องเป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย

ข้อ ๘. ต้องมีมาตรการป้องกันอัคคีภัยและภัยธรรมชาติ โดยจัดเตรียมอุปกรณ์การดับเพลิงสำหรับระบบคอมพิวเตอร์ อุปกรณ์ป้องกันภัยธรรมชาติ ให้พร้อมใช้งานได้ตลอดเวลา มีมาตรการป้องกันภัยธรรมชาติ ตลอดจนจัดเตรียมสถานที่ วัสดุ อุปกรณ์ ที่จำเป็นสำหรับการฟื้นฟูระบบ และสถานที่เก็บรักษาสำรองข้อมูลที่ปลอดภัย

๘.๑. การป้องกันอัคคีภัย บริเวณพื้นที่ซึ่งติดตั้งและจัดวางอุปกรณ์ จะต้องมีการติดตั้งระบบดับเพลิง ซึ่งมีคุณสมบัติพิเศษในการดับเพลิงได้อย่างรวดเร็วและมีประสิทธิภาพ โดยไม่ก่อให้เกิดความเสียหายกับอุปกรณ์ประเภทไฟฟ้า อิเล็กทรอนิกส์ หรือคอมพิวเตอร์

๘.๒. การเก็บรักษาสื่อที่ใช้เก็บข้อมูล (Media Storage) สื่อแม่เหล็ก หรือสื่ออื่นๆ ซึ่งใช้ในการเก็บข้อมูลและสำรองข้อมูล จะต้องถูกจัดเก็บไว้อย่างปลอดภัยและมีระบบสำรองข้อมูลที่มีประสิทธิภาพ

๘.๓. การทำลายสิ่งที่ไม่ใช้ สื่อแม่เหล็ก หรือสื่ออื่นซึ่งใช้ในการบันทึก หรือเก็บ ข้อมูลที่ไม่ใช้อีกต่อไป ต้องดำเนินการเพื่อไม่ให้มีการนำสื่อข้างต้นกลับมาใช้หรือเรียกค้นข้อมูลได้อีก การทำลายสื่อแม่เหล็ก หมายรวมถึง การเขียนข้อมูลใหม่ทับ (Overwrite) การทำลายด้วยสนามแม่เหล็ก (Degauss) หรือการทำลายทิ้ง (Destruct) ก็ได้

ข้อ ๙. ต้องมีแผนและนโยบายเตรียมรับสถานการณ์ฉุกเฉินต่างๆ เช่น แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) แผนบริหารความเสี่ยงของฐานข้อมูล

และสารสนเทศ แผนการเคลื่อนย้าย แผนการทำลายระบบสารสนเทศในเวลาฉุกเฉิน และนโยบายความมั่นคง ปลอดภัยของระบบสารสนเทศ

ข้อ ๑๐. จัดให้มีเวร - ยามรักษาการณ์ และพิทักษ์รักษาระบบสารสนเทศ และมีการประชุมชี้แจงเจ้าหน้าที่รักษาการณ์ให้ทราบถึงขั้นตอนการตรวจการณ์ การพิสูจน์ทราบ และการเข้าขัดขวางในพื้นที่รับผิดชอบอย่างสม่ำเสมอ และให้มีการกำกับดูแลอย่างเข้มงวด

ส่วนที่ 3
การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

ข้อ ๑. ความมุ่งหมาย เพื่อให้เป็นแนวทางปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยต่อระบบสารสนเทศของกระทรวงสาธารณสุข และลดความเสียหายที่เกิดขึ้นจากการกระทำที่ฝ่าฝืน หรือละเลยให้เหลือน้อยที่สุด พร้อมทั้งตรวจสอบค้นหาสาเหตุผลเสียหายเพื่อปรับปรุงมาตรการป้องกันการละเมิดที่จะเกิดขึ้นซ้ำอีกกับกำหนดวิธีดำเนินการต่อผู้ละเมิดการรักษาความปลอดภัย

ข้อ ๒. การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

๒.๑. เมื่อตรวจพบหรือสงสัยว่ามีการละเมิดการรักษาความปลอดภัยระบบสารสนเทศหรือมีสิ่งผิดปกติเกิดขึ้นในระบบสารสนเทศ ให้รีบรายงานผู้บังคับบัญชา หรือเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของส่วนราชการทราบโดยเร็วที่สุด

๒.๒. เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของส่วนราชการดำเนินการดังนี้ต่อไปนี้

๒.๒.๑. รายงานขั้นต้นต่อผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของผู้บริหารหน่วยงานหากพบว่าเป็นการละเมิดต่อสารสนเทศที่มีชั้นความลับ

๒.๒.๒. ลดความเสียหายเบื้องต้น โดยการระงับใช้แก้ไข หรือยกเลิกระบบสารสนเทศที่สงสัยว่าถูกละเมิดนั้น หากเป็นสารสนเทศที่มีชั้นความลับจะต้องยกเลิกชั้นความลับโดยทันทีและแจ้งให้เจ้าของเรื่องสารสารเทศที่มีชั้นความลับนั้นทราบด้วย

๒.๒.๓. สำรวจความเสียหายที่เกิดจากการละเมิด ตรวจสอบสาเหตุ และจุดอ่อนหรือข้อบกพร่องที่ก่อให้เกิดการละเมิด ให้มีผู้แทนจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารศึกษาร่วมในการตรวจสอบสาเหตุด้วย

๒.๒.๔. รายงานเหตุการณ์ที่เกิดขึ้น ให้ผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกระทรวงสาธารณสุขทราบ พร้อมทั้งแนวทางป้องกันมิให้เกิดการละเมิดซ้ำ

๒.๒.๕. ในกรณีที่ระบบรหัส ประมวลลับที่ใช้ในระบบสารสนเทศสูญหาย หรือสงสัยว่ามี ผู้ไม่มีอำนาจหน้าที่ทราบระบบรหัส ประมวลลับ ให้ระงับใช้ยกเลิกหรือเปลี่ยน แปลงรหัสประมวลลับนั้นโดยทันที แล้วรายงานให้ผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกระทรวงสาธารณสุขทราบโดยเร็วที่สุด

ข้อ ๓. ความรับผิดชอบของผู้อำนวยการรักษาความปลอดภัยระบบสารสนเทศของกระทรวงสาธารณสุข

๓.๑. แจ้งให้ส่วนราชการเจ้าของสารสนเทศร่วม ทราบโดยเร็วที่สุด

๓.๒. ตั้งคณะกรรมการร่วมกับส่วนราชการที่มีการละเมิดต่อสารสนเทศ สืบสวนสอบหาตัวผู้รับผิดชอบและผู้กระทำผิดโดยเร็วที่สุด

๓.๓. แจ้งให้ส่วนราชการต้นสังกัดลงโทษผู้รับผิดชอบและผู้กระทำผิดต่อการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ ตามกรณีที่ก่อให้เกิดความเสียหายต่อระบบหรือส่งตัวผู้กระทำผิดไปดำเนินการตามกฎหมายต่อไป

๓.๔. สั่งให้แก้ไขข้อบกพร่อง และป้องกันมิให้เกิดเหตุการณ์ซ้ำขึ้นอีก

ข้อ ๔. เพื่อให้การดำเนินมาตรการรักษาความปลอดภัยเกี่ยวกับระบบสารสนเทศตามประกาศนี้เป็นไปด้วยความเรียบร้อยและรวดเร็ว จึงอธิบายศัพท์เฉพาะบางคำที่ปรากฏอยู่ในระเบียบนี้เพิ่มเติม รวมทั้งคำศัพท์คอมพิวเตอร์ซึ่งมีความหมายใกล้เคียงกัน ดังนี้

๔.๑. ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ (ผนวก ๑)

๔.๒. ศัพท์คอมพิวเตอร์ที่เกี่ยวข้อง (ผนวก ๒)

ประกาศ ณ วันที่ ๒๓ เมษายน พ.ศ. ๒๕๕๓

ผนวก ๑

ผู้ดูแลรักษาความปลอดภัยระบบสารสนเทศของส่วนราชการ

๑. ผู้บริหารระบบ (System Administrator) มีความรู้ด้านฮาร์ดแวร์ ซอฟต์แวร์ระบบเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๑.๑ บริหารและดูแลอุปกรณ์คอมพิวเตอร์ซึ่งเป็นแม่ข่ายบริการแก่หน่วยงานต่าง ๆ

๑.๒ ควบคุมและตรวจสอบการใช้งานระบบ

๑.๓ ตรวจสอบ ควบคุม ดูแล การบำรุงรักษาระบบ

๑.๔ รักษาความปลอดภัยระบบ เช่น รักษาความลับ ความคงสภาพและความพร้อมใช้งาน

๒. ผู้จัดการฐานข้อมูล (Database Manager) มีความรู้ด้านการจัดการฐานข้อมูล ระบบคอมพิวเตอร์เป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๒.๑ ควบคุมดูแลฐานข้อมูล เช่น การรวบรวม การเพิ่ม การเปลี่ยนแปลง การลบ การจัดโครงสร้าง การใช้งาน การเก็บ และการเรียกดู

๒.๒ เลือก ตัดตอน และกำหนดรูปแบบข้อมูลที่เก็บในแฟ้มข้อมูล

๒.๓ รักษาความปลอดภัยฐานข้อมูล เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานให้ฐานข้อมูล

๒.๔ ตรวจสอบฐานข้อมูล และวิเคราะห์ข้อมูล

๒.๕ ควบคุม และบริการการใช้งานฐานข้อมูล

๓. ผู้จัดการเครือข่าย (Network Manager) มีความรู้ด้านฮาร์ดแวร์ การสื่อสารข้อมูล และอุปกรณ์ในระบบเครือข่ายเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๓.๑ กำหนดเลขที่อยู่ไอพี (IP Adress) ให้คอมพิวเตอร์ในเครือข่ายของส่วนราชการโดยประสานกับส่วนราชการ หรือผู้บริหารระบบเครือข่ายคอมพิวเตอร์ของกระทรวงสาธารณสุข

๓.๒ กำหนดบัญชีผู้ใช้ (Account) และรหัสผ่าน (Password) ของผู้ใช้ภายในเครือข่ายที่รับผิดชอบ

๓.๓ ดูแลการใช้เครือข่ายคอมพิวเตอร์ภายในส่วนราชการ

๓.๔ ดูแลโครงสร้างพื้นฐานและอุปกรณ์ที่เกี่ยวกับระบบเครือข่าย เช่น โทรศัพท์โมเด็ม ฮับ เป็นต้น

๓.๕ รักษาความปลอดภัยระบบเครือข่าย เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานให้ระบบเครือข่าย

๔. ผู้เขียนโปรแกรม (Programmer) มีความรู้เรื่องระบบคอมพิวเตอร์ การเขียนโปรแกรมคอมพิวเตอร์และฐานข้อมูลเป็นอย่างน้อย และรับมอบหมายให้ปฏิบัติหน้าที่ดังนี้

๔.๑ เขียนและพัฒนาโปรแกรมที่ได้รับมอบหมาย

๔.๒ จัดหาข้อมูลเพื่อทดสอบโปรแกรม

๔.๓ ดูแลบำรุงรักษาโปรแกรมที่พัฒนา

๔.๔ รักษาความปลอดภัยโปรแกรม เช่น รักษาความลับ ความคงสภาพ และความพร้อมใช้งานให้โปรแกรม

ผนวก ๒

คำศัพท์คอมพิวเตอร์ที่เกี่ยวข้อง

๑. “พื้นที่ใช้งานระบบสารสนเทศ (Information System Workspaces)” หมายความว่า พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ หรือ เตรียมข้อมูล เก็บอุปกรณ์คอมพิวเตอร์ พื้นที่ที่เป็นห้องทำงานของบุคลากรทางคอมพิวเตอร์ รวมทั้ง เครื่องคอมพิวเตอร์ส่วนบุคคลที่ติดตั้งประจำโต๊ะทำงาน

๒. “เครือข่ายระบบสารสนเทศ” หมายความว่า การติดต่อสื่อสารหรือการส่ง ข้อมูลระหว่างระบบสารสนเทศของกองบัญชาการศึกษา สำนักงานตำรวจแห่งชาติ เช่น ระบบอินทราเน็ต(Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

๓. “สารสนเทศที่กำหนดชั้นความลับ” หมายความว่า สารสนเทศในรูปข้อมูล หรือ ข่าวสารที่บันทึกไว้ในแบบใด ๆ ที่กำหนดชั้นความลับตามความสำคัญของเนื้อหาจำกัดการเข้าถึง และหรือจำกัดให้ทราบเท่าที่จำเป็น และให้รวมถึงจานบันทึก ประมวลลับ รหัส และรหัสผ่านที่กำลังใช้อยู่หรือเตรียมจะใช้ตลอดจนวัสดุหรือเอกสารทุกอย่างที่บันทึกเรื่องดังกล่าว

๔. “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิด การฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๕. “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๖. “ภัย” (Threat) หมายความว่า อันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศ โดยคน(Person) สิ่งต่าง ๆ (Thing) หรือ เหตุการณ์(Event) ทั้งเจตนาและไม่เจตนา อันเป็นเหตุทำให้ข้อมูลข่าวสารของระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลาย ปฏิเสธการทำงาน หรือ การกระทำอื่น ๆ ตามความต้องการของภัยนั้น

๗. “ความอ่อนแอ” (Vulnerability) หมายความว่า จุดอ่อน หรือข้อบกพร่องใด ๆ ก็ตามของระบบสารสนเทศที่ภัยในรูปแบบที่เหมาะกัน สามารถนำไปใช้ประโยชน์เพื่อก่อให้เกิดอันตรายต่อระบบสารสนเทศนั้น ๆ ได้ความอ่อนแอที่มีอยู่ของระบบสารสนเทศ และความรุนแรงที่เกิดจากภัยนั้น ซึ่งภัยประเภทเดียวกันอาจมีระดับความเสี่ยงไม่เท่ากันในแต่ละพื้นที่ใช้งานระบบสารสนเทศ ฯ ความเสี่ยงเป็นสิ่งที่ใช้ตัดสินว่า ณ พื้นที่ใช้งานระบบสารสนเทศ ฯ แต่ละแห่งควรจัดเตรียมระบบการรักษาความปลอดภัยให้หนาแน่น เพียงใด

๘. “บัญชีผู้ใช้” (Account) ความหมาย เป็นสัญลักษณ์หรือชุดของตัวอักษรเรียงติดต่อกัน มีลักษณะเป็นหนึ่งเดียว (Unique) ไม่ซ้ำกันเพื่อเป็นการระบุตัว (Identification) เจ้าของบัญชีหรือกลุ่มคนที่สามารถเข้าถึงระบบได้ บัญชีผู้ใช้เป็นเครื่องมือรักษาความปลอดภัยที่ใช้ควบคู่กับรหัสผ่าน (Password)

๙. “แฟ้มลงบันทึกเข้าออก” (Log File) ความหมาย เป็นการบันทึกการปฏิบัติทั้งหมดของอุปกรณ์ที่เกี่ยวข้องกับการประมวลผลข้อมูล (Data Processing Equipment) จะบันทึกงานทุกงานหรือการดำเนินการ (Run) ตามลำดับที่เกิดขึ้นเวลาเริ่มต้นและสิ้นสุดของแต่ละงาน รวมทั้งกิจกรรมที่ทำ ทั้งนี้เพื่อนำมาตรวจสอบความถูกต้องของการใช้งานได้ในภายหลัง

เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีและระบบสารสนเทศของ สธ. ให้อยู่ในระดับมาตรฐานสากล สธ. ได้อนุมัตินโยบายความมั่นคงความปลอดภัยระบบสารสนเทศ โดยได้กำหนดแนวทางไว้เป็นกรอบและแผน และเพื่อให้การดำเนินการตามนโยบายความปลอดภัยของระบบสารสนเทศ สธ. เป็นไปด้วยความเรียบร้อย จึงขอให้ ข้าราชการตำรวจทุกนายในสังกัด สธ. ทราบและปฏิบัติตามแนวนโยบายความปลอดภัยระบบสารสนเทศ สธ. ต่อไป