แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมการแพทย์

๑. หลักการและเหตุผล

ตามที่ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

กรมการแพทย์ ได้กำหนดแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมการแพทย์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่องและป้องกันภัยคุกคามต่างๆ ปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาดังกล่าวได้อย่างถูกต้องและเหมาะสม นอกจากนี้ ยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่นๆ ที่เกี่ยวข้อง รวมถึงการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ด้วย

๒. วัตถุประสงค์

กรมการแพทย์ ได้กำหนดแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผลและปฏิบัติได้อย่างถูกต้องตามกฎหมายต่างๆ ที่เกี่ยวข้องได้กำหนดไว้

๒.๒ เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๔ นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้ง ต่อปี

๓. องค์ประกอบของนโยบาย

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมการแพทย์ จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งแนวปฏิบัติออกเป็นส่วนๆ ดังต่อไปนี้

ส่วนที่ ๑ แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Acceptable use Policy)

ส่วนที่ ๒ แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)

ส่วนที่ ๓ แนวปฏิบัติการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ ไฟล์วอลล์ (Firewall Policy)

ส่วนที่ ๔ แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail Policy)

ส่วนที่ ๕ แนวปฏิบัติการใช้งานอินเตอร์เน็ต (Internet Policy)

ส่วนที่ ๖ แนวปฏิบัติการควบคุมการเข้าถึง (Access Control Policy)

ส่วนที่ ๗ แนวปฏิบัติการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก (Intrusion Detection System : IDS and Intrusion Prevention System : IPS)

ส่วนที่ ๘ การกำหนดผู้รับผิดชอบ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมการแพทย์ แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมฯ เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรของกรมฯ ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมการแพทย์ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมฯ ซึ่งเจ้าหน้าที่ของกรมฯ และหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

๑. **หน่วยงาน หรือ องค์กร** หมายความว่า กรมการแพทย์

๒. **ระบบคอมพิวเตอร์** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๓. **ระบบเครือข่าย** หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

๔. **ความมั่นคงปลอดภัย** หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๕. **ระบบแลน (Local Area Network) และ ระบบอินทราเน็ต (Intranet)** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๖. **ระบบอินเทอร์เน็ต (Internet)** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

๗. **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

๘. **เครื่องคอมพิวเตอร์** หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

๙. **ข้อมูลคอมพิวเตอร์** หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๐. **สารสนเทศ (Information)** หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๑๑. **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมการแพทย์

๑๒. **ผู้ใช้บริการ หรือ ผู้ใช้งาน** หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างในสังกัดหน่วยงาน พนักงานราชการ และหมายรวมถึงบุคคลที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

๑๓. **ผู้ดูแลระบบ (System Administrator)** หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบเครือข่ายและคอมพิวเตอร์ไม่ว่าส่วนหนึ่งส่วนใด

๑๔. **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๑๕. **หน่วยงานภายนอก** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๖. **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร** หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

๑๖.๑ **พื้นที่ทำงาน** หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูและระบบ (System Administrator)

๑๖.๒ **พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย** หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

๑๖.๓ **พื้นที่ใช้งานระบบเครือข่ายไร้สาย** หมายความว่า พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

๑๗. **สินทรัพย์ หรือ ทรัพย์สิน** หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ หมายรวมถึงสิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

๑๘. **จดหมายอิเล็กทรอนิกส์ (e-mail)** หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

๑๙. **รหัสผ่าน (Password)** หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๒๐. **บัญชีผู้ใช้บริการ (Account)** หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

๒๑. **โปรแกรมประสงค์ร้าย (Malware)** หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ / หรือ ข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือ สปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Torjan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

๒๒. **ชื่อคอมพิวเตอร์ (Computer Name)** หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

๒๓. **สื่อบันทึกพกพา** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Disk หรือ Floppy Disk เป็นต้น

๒๔. **ปุ่มกดง่าย (Shortcut)** หมายความว่า เครื่องมือที่ช่วยในการเรียกใช้โปรแกรมได้อย่างรวดเร็วและสามารถเข้าถึงโปรแกรมหรือแฟ้มข้อมูลที่ต้องการได้ทันที ซึ่งผู้ใช้สามารถลบหรือสร้างใหม่ได้

๒๕. **ไบออส(BIOS)** หมายความว่า ซอฟต์แวร์ขนาดเล็กซึ่งเก็บอยู่ในหน่วยความจำบนเมนบอร์ดของเครื่องคอมพิวเตอร์ ทำหน้าที่ควบคุมขั้นตอนการบู๊ตและการทำงานของอุปกรณ์พื้นฐานต่าง ๆ ที่ติดตั้งอยู่บนเมนบอร์ด

๒๖. **การตั้งค่าระบบ (Configuration)** หมายความว่า ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

๒๗. **เลขที่อยู่ไอพี (IP Address)** หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

๒๘. **เลขที่อยู่ไอพีสาธารณะ (Public IP Address)** หมายความว่า เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

๒๙. **แบนด์วิดท์ (Bandwidth)** หมายความว่า ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

๓๐. **ชื่อผู้ใช้ (Username)** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

๓๑. **ลงบันทึกเข้า (Login)** หมายความว่า กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้ระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

๓๒. **ลงบันทึกออก (Logout)** หมายความว่า กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

๓๓. **อัพเดท (Update)** หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่าง ๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

๓๔. **ช่องโหว่ (Vulnerability)** หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓๕. **ไฟล์ที่สามารถประมวลผลได้ (Executable File)** หมายความว่า ไฟล์โปรแกรมที่สามารถเรียกใช้งานได้ทันที เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe ในขณะที่ไฟล์ข้อมูลอื่น ๆ จะเป็นไฟล์ข้อมูลประกอบ

๓๖. **การเข้ารหัส (Encryption)** หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๓๗. **อุปกรณ์กระจายสัญญาณ (Access Point)** หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

๓๘. **SSID (Service Set Identifier)** หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๓๙. **WEP (Wire Equivalent Privacy)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

๔๐. **WPA (Wi-Fi Protected Access)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

๔๑. **Wireless LAN Client** หมายความว่า เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลน โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE ๘๐๒.๑๑

๔๒. **MAC Address (Media Access Control Address)** หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขที่จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๔๓. **ไฟร์วอลล์ (Firewall)** หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๔๔. **VPN (Virtual Private Network)** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๔๕. **Web Server** หมายความว่า เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บและมีหน้าที่ให้บริการเว็บเพจต่าง ๆ

๔๖. **ชื่อโดเมนย่อย (Sub Domain Name)** หมายความว่า ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่ม ต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ “ที่อยู่เว็บไซต์” แทนก็ได้

๔๗. **อุปกรณ์จัดเส้นทาง (Router)** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

๔๘. **อุปกรณ์กระจายสัญญาณข้อมูล (Switch)** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ – ส่งข้อมูล

๔๙. **การพิสูจน์ยืนยันตัวตน (Authentication)** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

๕๐. **แผนผังระบบเครือข่าย (Network Diagram)** หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

๕๑. **Command Line** หมายความว่า บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความ เพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

๕๒. **Firewall Log** หมายความว่า การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟล์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

๕๓. **เวลาอ้างอิงสากล (Stratum O)** หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ) เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๕๔. **ข้อมูลจราจรทางคอมพิวเตอร์ (Log)** หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลาและชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์

๕๕. **การเข้าถึงควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๕๖. **ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)** หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

๕๗. **เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๕๘. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ส่วนที่ ๑

แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Acceptable use Policy)

๑. วัตถุประสงค์

ปัจจุบันระบบเครือข่ายคอมพิวเตอร์ เป็นสิ่งสำคัญสำหรับหน่วยงานที่เข้ามาช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็วการติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่าง ๆ ของหน่วยงานที่เชื่อมต่อในระบบอินเตอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์และการมีเว็บไซต์เป็นของหน่วยงาน สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสารต่าง ๆ เป็นต้น ทั้งนี้ระบบเครือข่ายดังกล่าว แม้จะมีประโยชน์และอำนวยความสะดวกก็ตาม แต่ในขณะเดียวกันก็มีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเครือข่ายคอมพิวเตอร์เปรียบเสมือนการเปิดประตูเพื่อติดต่อกับโลกภายนอกทำให้มีโอกาสถูกบุกรุกได้มากยิ่งขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการโจมตีทางระบบเครือข่ายเพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้น ผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแลบำรุงรักษาและการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

๒. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. กรมการแพทย์ จัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานประกอบด้วยเนื้อหา ดังต่อไปนี้

๑.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๑.๒ จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๑.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๒. กรมการแพทย์ จัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานประกอบด้วยเนื้อหา ดังต่อไปนี้

๒.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๒.๒ จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๒.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๓. ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) ดังนี้

๓.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๓.๒ ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของกรมการแพทย์

๓.๓ กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๔. ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วนคือ การควบคุมการเข้าถึงสารสนเทศและการปรับปรุงหรือทบทวนให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๕. ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและผ่านการฝึกอบรม หลักสูตร การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต มีรายละเอียด ดังนี้

๕.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๕.๒ การลงทะเบียนผู้ใช้งาน (User Registration) กำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๕.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) จัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๕.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) จัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๕.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) จัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

๖. ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยมีรายละเอียด ดังนี้

๖.๑ การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๖.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๖.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๗. ให้มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยมีรายละเอียด ดังนี้

๗.๑ การใช้งานบริการเครือข่าย กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๗.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User Authentication for External Connections) กำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

๗.๓ การระบุอุปกรณ์บนเครือข่าย(Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๗.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๗.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๗.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

๗.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๘. ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีรายละเอียด ดังนี้

๘.๑ การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๘.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๘.๓ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๘.๔ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

๘.๕ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

๙. ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยมีรายละเอียด ดังนี้

๙.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น

๙.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กรต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)

๙.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสาร

๙.๔ การควบคุมการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) กำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

๑๐. หน่วยงานมีระบบสารสนเทศในการจัดทำระบบสำรอง ตามแนวทางต่อไปนี้

๑๐.๑ พิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๑๐.๒ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๐.๓ มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๐.๔ มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

๑๐.๕ กำหนดความถี่ของการปฏิบัติในแต่ละข้อ มีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

๑๑. หน่วยงานจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยมีรายละเอียด ดังนี้

๑๑.๑ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑๑.๒ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วย เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

๑๒. กำหนดให้มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

๑๓. กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑๔. บทลงโทษและการบังคับใช้

๑๔.๑ กำหนดความผิด ที่เกิดขึ้นจากผู้ใช้งานที่มีเจตนาฝ่าฝืนนโยบายว่าด้วยความมั่นคงปลอดภัยสารสนเทศ กรมการแพทย์ ตามเอกสารฉบับนี้ แม้ว่าการฝ่าฝืนนั้นจะกระทำไม่บรรลุผลโดยสมบูรณ์

๑๔.๒ ความผิดเกี่ยวกับ นโยบายว่าด้วยความมั่นคงปลอดภัยสารสนเทศ กรมการแพทย์ ให้ลงโทษผู้กระทำผิดตามระเบียบ กฎหมายที่เกี่ยวข้อง

ส่วนที่ ๒

แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๒.๑ ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับอนุญาตจากผู้บังคับบัญชา โดยกรอกข้อมูลลงใน *"แบบฟอร์มการขึ้นทะเบียนคอมพิวเตอร์และการยืนยันตัวบุคคล"*

๒.๒ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๓ ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สายลงในแบบฟอร์ม

๒.๔ ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (default) มาจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

๒.๕ ผู้ดูแลระบบควรเปลี่ยนค่าชื่อ login และรหัสผ่าน สำหรับการตั้งค่าการทำงานของอุปกรณ์ ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๒.๖ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ Access Point เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

๒.๗ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address และชื่อผู้ใช้รหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

ส่วนที่ ๓

แนวปฏิบัติการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟล์วอลล์ (Firewall Policy)

๑. วัตถุประสงค์

เหตุผลหลักที่มีการใช้ไฟร์วอลล์ (Firewall) ก็เพื่อให้ผู้ใช้ที่อยู่ภายในองค์กรสามารถใช้บริการเครือข่ายภายในได้เต็มที่และใช้บริการเครือข่ายภายนอก เช่น อินเตอร์เน็ตได้ ในขณะที่ไฟร์วอลล์จะป้องกันไม่ให้ผู้ใช้ภายนอกเข้ามาใช้บริการเครือข่ายที่อยู่ข้างใน ไฟร์วอลล์สามารถควบคุมการใช้เครือข่ายได้ โดยอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่านได้ซึ่งแพ็กเก็ตที่อนุญาตให้ผ่านหรือไม่นี้จะขึ้นอยู่กับนโยบายการรักษาความปลอดภัย (Security Policy) ของเครือข่าย ไฟร์วอล์เป็นระบบที่บังคับใช้นโยบายการรักษาความปลอดภัยระหว่างเครือข่าย โดยหลักการแล้วไฟร์วอลล์จะทำงานอยู่ ๒ กลไก คือ การอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่าน ถ้าเครือข่ายองค์กรนั้นมีการเชื่อมต่อโดยตรงกับอินเตอร์เน็ตโดยที่ไม่มีไฟร์วอลล์เป็นการเปิดช่องโหว่ให้เครือข่ายสามารถถูกโจมตีหรือบุกรุกได้อย่างง่ายดาย ตัวอย่างเช่น เครือข่ายมีโฮสต์หรือเซิรฟ์เวอร์เป็นร้อย ๆ เครื่อง ถ้าผู้บุกรุกเครือข่ายสามารถบุกรุกเข้าเครื่องใดเครื่องหนึ่งได้ ต่อไปนี้ก็ไม่เป็นการยากที่จะบุกรุกเข้าไปยังเครื่องอื่นๆ การติดตั้งไฟร์วอลล์จะเป็นการป้องกันผู้บุกรุกได้ในระดับหนึ่ง

๒. แนวปฏิบัติการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall) ของกรมการแพทย์ มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๒.๑ ผู้ดูแลระบบต้องเฝ้าระวังและบริหารจัดการระบบรักษาความปลอดภัย (Firewall)

๒.๒ ผู้ดูแลระบบต้องกำหนดนโยบาย (Policy) การใช้งานไฟร์วอลล์

๒.๓ ผู้ดูแลระบบต้องจัดให้มีระบบตรวจสอบตัวตนจริง และสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น การกำหนดรหัสผ่าน (Password) ให้ยากแก่การคาดเดา เป็นต้น

๒.๔ ผู้ดูแลระบบต้องกำหนดค่า (Configuration) หรือกำหนดนโยบาย (Policy) เพื่อกลั่นกรองข้อมูลที่มาทางเว็บไซต์ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรมการแพทย์ ป้องกันผู้บุกรุก ไวรัส รวมทั้ง malicious code ต่างๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์

๒.๕ ผู้ดูแลระบบต้องกำหนดขั้นตอนหรือวิธีปฏิบัติ ในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติต้องดำเนินการแก้ไข รวมทั้งมีการรายงานผู้บังคับบัญชาโดยทันที

๒.๖ การเปิดใช้บริการ (Service) ต้องได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันเพิ่มเติม

๒.๗ ผู้ดูแลระบบต้องเปิดใช้งานไฟร์วอลล์ตลอดเวลา

๒.๘ ผู้ดูแลระบบต้องออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์

๒.๙ ผู้ดูแลระบบต้องกำหนดให้มีการควบคุมการใช้งาน โดยการจัดให้มีบัญชีผู้ใช้งาน

๒.๑๐ ผู้ดูแลระบบการใช้งานต้องบันทึกชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเป็นการตรวจสอบผู้ใช้ก่อนเข้าใช้งานระบบ (Authentication) และควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไข เปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง

๒.๑๑ ผู้ดูแลระบบต้องติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของซอฟต์แวร์ระบบ (System Software) เช่น ระบบปฏิบัติการ DBMS Web Server เป็นต้น อย่างสม่ำเสมอ

๒.๑๒ ผู้ดูแลระบบต้องทดสอบซอฟต์แวร์ระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิ์ภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังการแก้ไขหรือบำรุงรักษา

๒.๑๓ ผู้บังคับบัญชาต้องกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ อย่างชัดเจน

๒.๑๔ ผู้ขอใช้งานต้องยอมรับและปฏิบัติตามนโยบายด้านความปลอดภัยอย่างเคร่งครัด

๒.๑๕ วัตถุประสงค์ในการขอใช้งานจะต้องไม่ขัดต่อนโยบาย ประกาศ ระเบียบต่าง ๆ ของกรมพัฒนาที่ดินและต่อกฎหมายที่เกี่ยวข้อง

๒.๑๖ ผู้ขอใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษร ต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุข้อมูลดังนี้

๒.๑๖.๑ หมายเลข Port ที่ต้องการขอให้เปิด

๒.๑๖.๒ หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๒.๑๖.๓ วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้น ๆ

๒.๑๖.๔ วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

๒.๑๗ ในการขอใช้งานหากพบว่าการขัดต่อนโยบาย ประกาศ ระเบียบของกรมการแพทย์ หรือกฎหมาย หรืออาจทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะไม่อนุญาตให้ใช้งาน

๒.๑๘ ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบายประกาศระเบียบ ของกรมการแพทย์ หรือกฎหมาย หรืออาจจะทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของกรมฯ ทางศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จะยกเลิกการให้บริการทันที

๒.๑๙ ผู้ดูแลระบบต้องกำหนดแนวทางปฏิบัติในการใช้งาน software utility เช่น personal firewall password cracker เป็นต้น และตรวจสอบการใช้งาน software utility อย่างสม่ำเสมอ

ส่วนที่ ๔

แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมาอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

๒.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมฯ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

๒.๒ ผู้ใช้รายใหม่ที่ต้องการขอลงทะเบียนบัญชีชื่อผู้ใช้ ต้องทำการกรอกแบบฟอร์มการใช้ระบบจดหมายอิเล็กทรอนิกส์ และยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน

๒.๓ ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมฯ

๒.๔ ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์

๒.๕ ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรมฯ

๒.๖ ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๒.๗ ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของกรมฯ เพื่อการทำงานของกรมฯ เท่านั้น

๒.๘ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๒.๙ ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

๒.๑๐ ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๒.๑๑ ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของกรมฯ ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

๒.๑๒ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒.๑๓ ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๒.๑๔ ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๒.๑๕ ผู้ใช้ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

๒.๑๖ ผู้ใช้ควรทำการสำรองข้อมูลในจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอเลือกสำรองจดหมายอิเล็กทรอนิกส์ที่มีความสำคัญมาก โดยอาจทำการส่งต่อไปยังจดหมายอิเล็กทรอนิกส์แอดเดรสอื่น หรือทำการสำรองไว้ที่เมล์เซิร์ฟเวอร์ของกรมฯ

๒.๑๗ ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ ควรให้ความรู้เกี่ยวกับการรักษาความปลอดภัยในจดหมายอิเล็กทรอนิกส์แก่ผู้ใช้งานจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ การให้ความรู้ถือเป็นการป้องกันเบื้องต้นเพื่อมิให้ผู้ใช้งานตกเป็นเหยื่อของผู้ไม่หวังดี และเป็นการป้องกันไม่ให้เกิดปัญหา ในกรณีที่ทำผิดพลาดแม้เพียงครั้งเดียว อาจส่งผลกระทบทำให้ระบบไม่สามารถทำงานได้

๒.๑๘ ในการใช้จดหมายอิเล็กทรอนิกส์ในการติดต่อสื่อสารนั้น ผู้ใช้ควรให้เกียรติกับผู้รับปลายทางเหมือนการสนทนาด้วยวาจา ควรตรวจสอบตัวสะกดไวยากรณ์ อ่านทวนเนื้อหาก่อนส่ง ใช้ข้อความที่กระชับเข้าถึงประเด็นอย่างรวดเร็ว แต่ข้อความต้องไม่สั้นเกินจนดูแล้วห้วน และให้ตระหนักอยู่เสมอว่าข้อความใด ๆ ที่ส่งผ่านเครือข่ายอินเทอร์เน็ตนั้นเป็นข้อความที่สามารถมองเห็นและอ่านได้โดยผู้อื่น ดังนั้นการส่งข้อความที่เป็นความลับจะต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อเข้ารหัสข้อมูลนั้นก่อนส่งออกไป

๒.๑๙ ผู้ใช้ต้องไม่ทำการเปลี่ยนแปลง หรือแก้ไขข้อความจดหมายอิเล็กทรอนิกส์ต้นฉบับที่ได้รับมาและต้องการส่งต่อไป หากจดหมายอิเล็กทรอนิกส์นั้นถูกส่งถึงผู้รับเป็นการส่วนตัวต้องขออนุญาต ผู้ส่งก่อนที่จะส่งต่อจดหมายอิเล็กทรอนิกส์นั้นไปจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคลควรได้รับการเข้ารหัสอย่างปลอดภัย (Encryption)

๒.๒๐ ผู้ใช้ควรใส่ชื่อหัวข้อเรื่องใน Subject ของจดหมายอิเล็กทรอนิกส์ เพื่อแสดงถึงเรื่องของจดหมายอิเล็กทรอนิกส์ที่ต้องการหารือหรือแจ้งให้ทราบ และควรส่งจดหมายอิเล็กทรอนิกส์

ตอบกลับสั้น ๆ หากไม่มีเวลาพอเพื่อให้ผู้ส่งได้รับทราบว่าผู้รับได้รับจดหมายอิเล็กทรอนิกส์นั้นแล้ว และจะตอบกลับอย่างสมบูรณ์ในภายหลัง

๒.๒๑ ผู้ใช้ไม่ควรส่งต่อจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่ไม่สมควรทำบนเครือข่ายอินเทอร์เน็ต หากได้รับจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ และมีข้อความขอให้ส่งต่อจดหมายอิเล็กทรอนิกส์นั้นให้ติดต่อหรือแจ้งผู้ดูแลระบบโดยทันที

๒.๒๒ ผู้ใช้ไม่ควรส่งจดหมายอิเล็กทรอนิกส์ที่เกี่ยวกับการล่วงละเมิดหรือข่มขู่ หรือมีเนื้อหาข้อความที่ขัดต่อกฎหมายและศีลธรรม และใช้จดหมายอิเล็กทรอนิกส์เป็นเครื่องมือในการกระจายข่าวสาร เว้นแต่เป็นการประกาศที่เหมาะสม

๒.๒๓ ผู้ใช้ควรพิจารณาใช้ “BCC” (blind carbon copy - สำเนาโดยที่ผู้รับไม่ทราบ) ในการส่งจดหมายอิเล็กทรอนิกส์ถึงผู้รับเป็นจำนวนมาก เพื่อไม่ให้รายชื่อผู้รับทั้งหมดปรากฏในลักษณะที่ยาวมากเกินไป

๒.๒๔ ผู้ใช้ควรทำตามนโยบายอย่างเคร่งครัด และแจ้งผู้ดูแลระบบเมื่อพบการใช้จดหมายอิเล็กทรอนิกส์ที่ไม่ถูกต้อง

๒.๒๕ ผู้ใช้จะต้องกรอกข้อมูลในช่องข้อมูลส่วนตัว (identity) โดยจะต้องใช้ชื่อผู้ส่ง (Sender) ที่เป็นจริง ตามที่มีบัญชีรายชื่ออยู่จริง เพื่อให้สามารถอ้างอิงในกรณีที่มีปัญหาเกิดขึ้น

๒.๒๖ ผู้ใช้ต้องไม่ตั้งชื่อผู้ส่ง (Sender) หรือข้อมูลอื่น ในลักษณะที่ส่อว่าเป็นผู้ดูแลระบบ (administrator) เช่น webmaster, host master, administrator, postmaster เป็นต้น โดยไม่ได้รับอนุญาต

๒.๒๗ ผู้ใช้ต้องไม่ทำการส่งจดหมายอิเล็กทรอนิกส์ในลักษณะของจดหมายลูกโซ่ จดหมายชี้ชวนหรืออื่น ๆ อันเป็นการกระทำที่เข้าข่าย spam หรือ unsolicited electronic mail อย่างเด็ดขาด

๒.๒๘ ผู้ใช้บริการมีหน้าที่จะต้องรักษาชื่อผู้ใช้ และรหัสผ่านเป็นความลับ ไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๒.๒๙ จดหมายของผู้ใช้บริการ ถือเป็นข้อมูลส่วนบุคคล ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ไม่สามารถจะทำการเก็บ กู้ หรือ ดึงข้อมูลส่วนตัวขึ้นมาได้ ดังนั้นผู้ใช้บริการจะต้องดูแลรักษาข้อมูลดังกล่าวอย่างระมัดระวัง โดยเฉพาะการลบจดหมายที่ไม่ต้องการ รวมทั้งจะต้องดูแลรักษาไม่ให้ขนาดของจดหมายที่จัดเก็บเกินกว่าจำนวนพื้นที่ที่ได้รับอนุญาต

๒.๓๐ ผู้ใช้ต้องมีความรับผิดชอบ และระมัดระวังในการใช้บริการตามสมควร ไม่ให้ล่วงละเมิดบุคคลอื่น รวมถึงศีลธรรม หรือกฎหมายใด ๆ อันเป็นผลให้เกิดความไม่สงบเรียบร้อยในองค์กรและสังคมถูกต้อง

ส่วนที่ ๕

แนวปฏิบัติการใช้งานอินเตอร์เน็ต
(Internet Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูลข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กร ถูกระงับ ชะลอขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

๒.๑ ผู้ใช้งานต้องเป็นบุคลากรสังกัดกรมการแพทย์ สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมาย

๒.๒ ผู้ใช้งานต้องใช้ข้อความที่สุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้เครือข่ายเท่านั้น

๒.๓ ผู้ใช้งานต้องใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิ์ภาพ เช่น ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

๒.๔ ผู้ใช้งานต้องรับผิดชอบต่อข้อมูลของตนเอง ไม่ว่าจะเก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (Server) หรือการส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์

๒.๕ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านรหัสผู้ใช้ (User Account) ของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของรหัสผู้ใช้ (User Account) ต้องเป็นผู้รับผิดชอบ

๒.๖ ผู้ใช้งานต้องไม่ใช้งาน เพื่อการกระทำการดังต่อไปนี้

๒.๖.๑ เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่สถาบันชาติศาสนา พระมหากษัตริย์ กรมการแพทย์ หน่วยงานอื่น และบุคคลอื่น

๒.๖.๒ เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๒.๖.๓ เพื่อการกระทำทางพาณิชย์

๒.๖.๔ เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน

๒.๖.๕ เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญา

๒.๖.๖ เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ หรือผู้ที่มีสิทธิ์ในข้อมูลดังกล่าว

๒.๖.๗ เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่กรมการแพทย์

๒.๖.๘ เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของกรมการแพทย์ หรือของผู้ใช้อื่น หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของกรมฯ ไม่สามารถใช้งานได้ตามปกติ

๒.๖.๙ เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของกรมการแพทย์ไปยังที่อยู่ของเว็บ (website) ใด ๆ ในลักษณะที่ก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

๒.๖.๑๐ เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายของกรมการแพทย์

๒.๗ ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อประกอบธุรกิจส่วนบุคคล

๒.๘ ผู้ใช้งานต้องปฏิบัติตามนโยบายและแนวทางการใช้ระบบเครือข่ายที่กรมการแพทย์

ส่วนที่ ๖

แนวปฏิบัติการควบคุมการเข้าถึง
(Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์

๒. กระบวนการควบคุมการเข้าออกห้องควบคุมระบบ Network (ห้อง Server)

๒.๑ ผู้ดูแลระบบ และเจ้าหน้าที่องค์กร มีแนวปฏิบัติดังนี้

๒.๑.๑ ผู้ดูแลระบบ ควรจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น

๒.๑.๒ ผู้ดูแลระบบ ต้องทำการกำหนดสิทธิ์บุคคลในการเข้า-ออกห้อง Server โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการติดประกาศ *“ระเบียบการเข้าออกห้อง Server”* พร้อมระบุรายชื่อเจ้าหน้าที่ที่ได้รับการกำหนดสิทธิ์ไว้อย่างชัดเจน

๒.๑.๓ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้อง มีความจำเป็นต้องเข้า-ออกห้อง Server ต้องมีมาตรการการควบคุมอย่างรัดกุม

๓. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๓.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสาร มีระบบรักษาความปลอดภัย (Security) ควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๓.๒ ผู้ดูแลระบบกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูล เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓.๓ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

๓.๔ ผู้ดูแลระบบ จัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมฯ และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ

๓.๕ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๔. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๔.๑ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้

๔.๒ เจ้าของข้อมูล และ เจ้าของระบบ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๔.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๕. การบริหารจัดการการเข้าถึงข้อมูลของผู้ใช้

๕.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อเปลี่ยนตำแหน่งงานภายในองค์กร ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน เป็นต้น

๕.๒ การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

๕.๒.๑ ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ กำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ

๕.๒.๒ มีการกำหนดให้ผู้ใช้ลงนามในเอกสารยอมรับเงื่อนไข ที่จะเก็บรักษารหัสผ่านให้เป็นความลับเฉพาะตนใน *“แบบฟอร์มสมัครเป็นสมาชิกระบบเครือข่าย LDD Network”*

๕.๒.๓ การกำหนดชื่อผู้ใช้ต้องเป็นหนึ่งเดียวคือไม่ซ้ำกัน

๕.๓ กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๕.๔ ผู้ใช้ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๕.๕ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๕.๕.๑ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๕.๕.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๕.๕.๓ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ทีเป็นมาตรฐานสากล

๕.๕.๔ ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๕.๖ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้ ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ เช่น เมื่อเปลี่ยนตำแหน่งงานภายในองค์กร ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน หมดวาระ เกษียณอายุราชการ เป็นต้น

๕.๗ ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรมฯ

๖. การบริหารจัดการการเข้าถึงระบบเครือข่าย

๖.๑ ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของผู้ใช้ เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๖.๒ การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบเทคโนโลยีสารสนเทศและการสื่อสารก่อนที่จะสามารถใช้งานได้ในทุกกรณี

๖.๓ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๖.๔ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๖.๕ ผู้ดูแลระบบ ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้ กำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบ

๖.๖ ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๖.๗ ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กรควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๖.๘ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๖.๙ การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๖.๑๐ IP address ภายในของระบบงานเครือข่ายภายในของกรมฯ จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๖.๑๑ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๖.๑๒ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๖.๑๓ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

๗. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๗.๑ ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๗.๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

๗.๓ ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

๗.๔ ควรดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น web server เป็นต้น

๗.๕ ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๗.๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

๘. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๘.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๘.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๘.๓ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๘.๔ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

๘.๕ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

๙. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Information Access Control)

๙.๑ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของ กรม ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มี สิทธิต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๙.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๙.๓ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากร

๙.๓.๑ กำหนดเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๙.๓.๒ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๙.๓.๓ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีกำหนดระยะเวลาการใช้งานและระงับการใช้งาน ทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๙.๔ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น

๙.๕ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)

๙.๖ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสาร

๙.๗ การควบคุมการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) กำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

๑๐. การควบคุมการเข้าใช้งานระบบจากภายนอก

๑๐.๑ การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กรให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์กร การควบคุมบุคคลที่เข้าสู่ระบบขององค์กรจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๑๐.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสารก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๑๐.๓ ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับกรมฯ อย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๑๐.๔ ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้าองค์กรนั้นต้องมีการดูแลและการจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๑๐.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ไม่ควรเปิดพอร์ตและโมเด็มที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๑๑. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

๑๑.๑ การเข้าสู่ระบบสารสนเทศขององค์กรนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน อย่างน้อย ๑ วิธี

๑๑.๒ การเข้าสู่ระบบสารสนเทศขององค์กรจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย

๑๑.๓ การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการ ตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ส่วนที่ ๗

แนวปฏิบัติการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก
(Intrusion Detection System: IDS and Intrusion Prevention System: IPS)

๑. วัตถุประสงค์

IDS (Intrusion Detection System) หรือระบบตรวจจับการบุกรุก คือ ระบบตรวจจับการบุกรุกของผู้ไม่ประสงค์ดี โดยสามารถวิเคราะห์ข้อมูลที่ผ่านเข้าออกเครือข่ายว่ามีลักษณะการทำงานที่ เป็นความเสี่ยงต่อเครือข่ายหรือไม่ โดย IDS จะทำเพียงแค่แจ้งเตือนให้ผู้ดูแลระบบทราบเท่านั้น ส่วน IPS (Intrusion Prevention System) หรือระบบตรวจสอบและโต้ตอบการบุกรุกนั้น คือ ระบบที่มีลักษณะเช่นเดียวกับระบบ IDS แต่มีความสามารถมากกว่า คือ เมื่อตรวจพบข้อมูลที่มีลักษณะที่เป็นความเสี่ยงต่อเครือข่ายก็จะทำการป้องกันข้อมูลนั้นไม่ให้เข้ามาในเครือข่ายได้

๒. แนวปฏิบัติใช้งานระบบตรวจจับและป้องกันผู้บุกรุก

ผู้ใช้งานระบบตรวจจับและป้องกันผู้บุกรุก (Intrusion Detection System : IDS and Intrusion Prevention System : IPS) ขององค์กร มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๒.๑ ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ (IDS/IPS) เหตุการณ์ผิดปกติและการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบจะถูกทำการวิเคราะห์และหาสาเหตุของการบุกรุกในระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อเป็นเครื่องมือสำหรับการสืบสวนหาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด ป้องกันก่อนที่จะเกิดการโจมตี

๒.๒ ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามที่บุกรุกหรือโจมตีองค์กรเป็นเครื่องมือในการวัดประสิทธิ์ภาพในการป้องกันภัยของระบบรักษาความปลอดภัยอื่น เช่น ไฟร์วอลล์ เป็นต้น และเพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตรายที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือ Hacker รวมทั้งไวรัสประเภทต่าง ๆ

๒.๓ ผู้ดูแลระบบต้องมีการบริหารจัดการเหตุการณ์บุกรุกระบบ (Incident Management) เป็นการตอบสนองต่อเหตุการณ์บุกรุกทางเครือข่าย สามารถช่วยวิเคราะห์ลักษณะการบุกรุกทางเครือข่าย และทำให้สามารถแก้ไขสถานการณ์ได้อย่างถูกต้อง ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการบุกรุก โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับองค์กรและจัดทำวิธีปฏิบัติที่ถูกต้องให้กับองค์กรเพื่อป้องกันเหตุการณ์เกิดซ้ำ การตอบสนองต่อเหตุการณ์การบุกรุกแบ่งเป็น ๔ ขั้นตอน คือ

๒.๕.๑ จำกัดขอบเขต (Containment) จำกัดพื้นที่ที่เสี่ยงต่อการบุกรุกและจำกัดความ รุนแรงของการบุกรุก

๒.๕.๒ กำจัดต้นเหตุ (Eradication) กำจัดต้นเหตุของการบุกรุก รวมถึงปิดกั้นช่องทางของการบุกรุก

๒.๕.๓ กู้คืนระบบ (Recovery) แก้ไขระบบที่ถูกบุกรุกให้สามารถกลับมาทำงานได้ตามปกติ

๒.๕.๔ ติดตามผล (Follow-Up) บันทึกผลกระทบของเหตุการณ์และแนะนำวิธีปฏิบัติเพื่อป้องกันเหตุการณ์เกิดซ้ำ

๒.๔ ผู้ดูแลระบบต้องกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่าย และอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและมีการทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละครั้ง

๒.๕ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๒.๖ การใช้เครื่องมือต่าง ๆ (tools) เพื่อตรวจเช็คระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๗ ผู้ดูแลระบบต้องทำการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอต้องประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (operation) ระบบรักษาความปลอดภัย (security) และการทำงาน (functionality) ของระบบงานที่เกี่ยวข้อง

ส่วนที่ ๘

การกำหนดผู้รับผิดชอบ

กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อังเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. ระดับนโยบาย

ให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงาน ที่ทำหน้าที่ CIO และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมการแพทย์

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ติดตามและกำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

๒. ระดับปฏิบัติ ได้แก่

๒.๑ นายรังสรรค์ จันทนสมิต หัวหน้ากลุ่มงานพัฒนาเครือข่ายและบำรุงรักษา รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

๒.๑.๑ ควบคุมการเข้า-ออกห้อง Server ตามการกำหนดสิทธิการเข้าถึง Server

๒.๑.๒ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในกรมการแพทย์ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.

๒.๑.๓ กำกับดูแล การติดตั้ง รื้อถอน ดูแล ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN , Internet , Intranet ที่ให้บริการในกรมการแพทย์

๒.๑.๔ กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของเครื่อง Server ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้

๒.๑.๕ แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

๒.๑.๖ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาทราบทุกเดือน

๒.๑.๗ กับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

๒.๑.๘ กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๑.๙ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ใน Server ของระบบฐานข้อมูลทั้งหมดที่ให้บริการในเว็บไซต์กรมการแพทย์ ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.

๒.๑.๑๐ กำกับดูแล ตรวจสอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบ

๒.๑.๑๑ อื่น ๆ ตามที่ได้รับมอบหมาย

๒.๒ นายคมสันต์ สดชื่น นักวิชาการคอมพิวเตอร์ รับผิดชอบ ดังนี้

๒.๒.๑ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Back up and Recovery) ตามรอบระยะเวลาที่กำหนด

๒.๒.๒ บริหารจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๒.๒.๓ อื่น ๆ ตามที่ได้รับมอบหมาย

๒.๓ นายอานนท์ พัฒน์ชนะ นักวิชาการคอมพิวเตอร์ รับผิดชอบ ดังนี้

๒.๓.๑ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๓.๒ รายงานผลการปฏิบัติงานตามแผนการบริหารความเสี่ยงฯ ให้ผู้บังคับบัญชาทราบ

๒.๓.๓ อื่น ๆ ตามที่ได้รับมอบหมาย

๒.๔ ผู้ดูแลระบบ จากบริษัทที่จัดจ้างให้ดูแลระบบเครือข่ายและคอมพิวเตอร์ รับผิดชอบดังนี้

๒.๔.๑ แก้ไขปัญหา อุปสรรค จากสถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศที่เกิดจากการถูกเจาะระบบจากบุคคลภายนอก (Hack) และการถูกทำลายจากโปรแกรมไวรัส

๒.๔.๒ กำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่าย

๒.๔.๓ รายงานสภาพปัญหา และสถานการณ์ความเสียหายของระบบฐานข้อมูลและสารสนเทศที่ถูกทำลายจากบุคคลภายนอก (Hacker) และจากไวรัส (Virus)

๒.๔.๔ บำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในกรมการแพทย์ ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม. แก้ไขปัญหาขัดข้องของการเชื่อมโยงเครือข่ายในองค์กร

๒.๔.๕ อื่น ๆ ตามที่ได้รับมอบหมาย

ภาคผนวก

กฎหมาย / ระเบียบ / ประกาศ
ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ

๑. พระราชบัญญัติเผยแพร่ข้อมูลข่าวสาร พ.ศ. ๒๕๔๐
๒. พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ แก้ไขเพิ่มเติม
๓. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔
๔. พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑
๕. พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙
๖. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
๗. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐
๘. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
๙. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
๑๐. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
๑๑. คู่มือ หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปข้อมูลอิเล็กทรอนิกส์

สามารถดูเนื้อหาของกฎหมายข้างต้นได้จาก
http://intranet.ldd.go.th/Information_Law/index.html