แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมวิทยาศาสตร์การแพทย์

ศูนย์เทคโนโลยีสารสนเทศ กรมวิทยาศาสตร์การแพทย์

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมวิทยาศาสตร์การแพทย์

ศูนย์เทคโนโลยีสารสนเทศ กรมวิทยาศาสตร์การแพทย์

คำนำ

ปัจจุบันระบบเครือข่ายคอมพิวเตอร์ (Computer Network) ถูกนำมาใช้เป็นเครื่องมือในการช่วยอำนวยความสะดวกต่อการดำเนินงานเพื่อให้สามารถเข้าถึงข้อมูลได้อย่างรวดเร็ว มีประสิทธิภาพโดยเหตุดังกล่าวจึงทำให้ความไม่มั่นคงของระบบเครือข่ายคอมพิวเตอร์มีอิทธิพลต่อการปฏิบัติราชการได้เช่นกัน ทั้งนี้เกิดจากการใช้งานระบบเครือข่ายคอมพิวเตอร์เพื่อติดต่อกับโลกภายนอกเปรียบเสมือนการเปิดช่องทางการบุกรุกให้กับผู้ไม่ประสงค์ดีต่อหน่วยงานในการที่จะทำให้เกิดความเสียหายต่อทางราชการในรูปแบบต่าง ๆ เช่น การขโมยข้อมูลหรือความลับทางราชการ การนำข้อมูลไปใช้ในการทำลายชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนดลยีสารสนเทศและการสื่อสาร จึงต้องตระหนักถึงการดูแลรักษาในเรื่องความมั่นคงปลอดภัยและความพร้อมใช้งานด้านสารสนเทศเป็นอย่างยิ่ง

เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง กรมวิทยาศาสตร์การแพทย์จึงให้มีการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์การแพทย์

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติจากทุกหน่วยที่เกี่ยวข้องและต้องทำอย่างต่อเนื่องรวมถึงมีการตรวจสอบ และปรับปรุงเพื่อให้สอดคล้อง กับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็วอย่างสม่ำเสมอ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของกรมวิทยาศาสตร์การแพทย์ทุกคน ในการปฏิบัติเพื่อให้เกิดความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์การแพทย์

ศูนย์เทคโนโลยีสารสนเทศ

สารบัญ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมวิทยาศาสตร์การแพทย์

๑. หลักการและเหตุผล

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ จึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมวิทยาศาสตร์การแพทย์เพื่อใช้เป็นเครื่องมือที่สำคัญในการปฏิบัติงานและการบริหารราชการต่อไป

๒. วัตถุประสงค์

๑. เพื่อให้มีแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์การแพทย์ซึ่งเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒. เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้บุคคลากรและบุคคลที่ปฏิบัติงานให้กับหน่วยงานรวมทั้งการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

๓. เพื่อรักษาความถูกต้องสมบูรณ์ ความพร้อมใช้อยู่เสมอของระบบเทคโนโลยีสารสนเทศและให้มีการเตรียมความพร้อมในกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๔. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๕. เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจและการให้การอบรมทางด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่บุคลากรและบุคคลที่เกี่ยวข้อง

๓. แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมวิทยาศาสตร์การแพทย์

๑. ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของหน่วยงาน

๒. มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือ ฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓. เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๔. เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

๕. ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

๔. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมวิทยาศาสตร์การแพทย์

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมวิทยาศาสตร์การแพทย์จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งแนวปฏิบัติออกเป็นส่วนๆ ดังต่อไปนี้

ส่วนที่ ๑. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๒ แนวปฏิบัติการประเมินความเสี่ยง

ส่วนที่ ๓. แนวปฏิบัติของผู้ดูแลระบบ

ส่วนที่ ๔. แนวปฏิบัติการควบคุมการเข้าถึงพัฒนาระบบสารสนเทศและระบบเครือข่าย

ส่วนที่ ๕. แนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

ส่วนที่ ๖. แนวปฏิบัติการสำรองข้อมูล

ส่วนที่ ๗. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

"หน่วยงาน" หมายความว่า กรมวิทยาศาสตร์การแพทย์ และศูนย์วิทยาศาสตร์การแพทย์รวมถึงกอง สำนัก สถาบัน ศูนย์ หน่วยงานที่มีฐานะเทียบเท่ากองที่อธิบดีกรมวิทยาศาสตร์การแพทย์ตั้งขึ้นเป็นการภายใน

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย" หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

"ความมั่นคงปลอดภัย" หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

"ระบบแลน (Local Area Network)"และ **"ระบบอินทราเน็ต (Intranet)"** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

"ระบบอินเทอร์เน็ต (Internet)" หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

"ระบบเทคโนโลยีสารสนเทศ (Information Technology System)" หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

"เครื่องคอมพิวเตอร์" หมายความว่า เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

"สารสนเทศ (Information)" หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมวิทยาศาสตร์การแพทย์

"ผู้ใช้บริการ" หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างในสงกัดหน่วยงาน และให้หมายความรวมถึงบุคคลในวงงานของกรมวิทยาศาสตร์การแพทย์ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

"ผู้ดูแลระบบ (System Administrator)" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

"หน่วยงานภายนอก" หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

"พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร" หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

(๑) พื้นที่ทำงาน หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)

(๒) พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

(๓) พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายความว่า พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

"ทรัพย์สิน" หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

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

"รหัสผ่าน (Password)" หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"บัญชีผู้ใช้บริการ (Account)" หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

"โปรแกรมประสงค์ร้าย (Malware)" หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

"ชื่อเครื่องคอมพิวเตอร์ (Computer Name)" หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

"สื่อบันทึกพกพา" หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

"ปุ่มกดง่าย (Shortcut)" หมายความว่า เครื่องมือที่ช่วยในการเรียกใช้โปรแกรมได้อย่างรวดเร็วและสามารถเข้าถึงโปรแกรมหรือแฟ้มข้อมูลที่ต้องการได้ทันที ซึ่งผู้ใช้สามารถลบหรือสร้างใหม่ได้

"ไบออส (BIOS)" หมายความว่า ซอฟต์แวร์ขนาดเล็กซึ่งเก็บอยู่ในหน่วยความจำบนเมนบอร์ดของเครื่องคอมพิวเตอร์ ทำหน้าที่ควบคุมขั้นตอนการบู๊ตและการทำงานของอุปกรณ์พื้นฐานต่างๆ ที่ติดตั้งอยู่บนเมนบอร์ด

"การตั้งค่าระบบ (Configuration)" หมายความว่า ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

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

"เลขที่อยู่ไอพีสาธารณะ (Public IP Address)" หมายความว่า เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

"แบนด์วิดท์ (Bandwidth)" หมายความว่า ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

"ชื่อผู้ใช้ (Username)" หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

"ลงบันทึกเข้า (Login)" หมายความว่า กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

"ลงบันทึกออก (Logout)" หมายความว่า กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

"อัพเดท (Update)" หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

"ช่องโหว่ (Vulnerability)" หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยขอบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

"ไฟล์ที่สามารถประมวลผลได้ (Executable file)" หมายความว่า ไฟล์โปรแกรมที่สามารถเรียกใช้งานได้ทันที เช่น .exe, .com, .bat, .vbs, .scr, .pif, .hta, .txt.exe, .doc.exe, .xls.exe ในขณะที่ไฟล์ข้อมูลอื่นๆ จะเป็นไฟล์ข้อมูลประกอบ

"การเข้ารหัส (Encryption)" หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

"อุปกรณ์กระจายสัญญาณ (Access Point)" หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

"SSID (Service Set Identifier)" หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

"โดยปริยาย (Default)" หมายความว่า ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้า และนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้บริการ

"WEP (Wired Equivalent Privacy)" หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

"WPA (Wi-Fi Protected Access)" หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

"Wireless LAN Client" หมายความว่า เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลน โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE ๘๐๒.๑๑

"MAC Address (Media Access Control Address)" หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

"ไฟร์วอลล์ (Firewall)" หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

"VPN (Virtual Private Network)" หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

"Web Server" หมายความว่า เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่างๆ

"ชื่อโดเมนย่อย (Sub Domain Name)" หมายความว่า ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่มต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ "ที่อยู่เว็บไซต์" แทนก็ได้

"อุปกรณ์จัดเส้นทาง (Router)" หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

"อุปกรณ์กระจายสัญญาณข้อมูล (Switch)" หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

"การพิสูจน์ยืนยันตัวตน (Authentication)" หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

"แผนผังระบบเครือข่าย (Network Diagram)" หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

"Command Line" หมายความว่า บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความ เพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

"Firewall Log" หมายความว่า การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบประเภทของการ

สื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

"เวลาอ้างอิงสากล (Stratum o)" หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่าย ที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ) เพื่อให้สอดคล้องกับพระราชบัญญัติว่าการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ข้อมูลจราจรทางคอมพิวเตอร์ (Log)" หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่นๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

ส่วนที่ ๑
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สนที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๒. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑ ให้ศูนย์เทคโนโลยีสารสนเทศและศูนย์วิทยาศาสตร์การแพทย์ เป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน เช่นการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย พื้นที่เฉพาะผู้เกี่ยวข้อง เป็นต้น

๒.๒ กรณีส่วนกลางให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่าย

กรณีส่วนภูมิภาคให้หน่วยงานที่มีหน้าที่รับผิดชอบดูแลเทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่าย

๒.๓ กรณีส่วนกาลงให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

กรณีส่วนภูมิภาคให้หน่วยงานที่มีหน้าที่รับผิดชอบดูแลเทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานรับทราบ

ส่วนที่ ๒
แนวปฏิบัติการประเมินความเสี่ยง

๑. วัตถุประสงค์

เพื่อให้มีแนวปฏิบัติในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยต่อระบบสารสนเทศรวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง และระบุความเสี่ยงได้อย่างชัดเจน สามารถควบคุมความเสี่ยงได้อย่างมีประสิทธภาพ

๒. แนวปฏิบัติการประเมินความเสี่ยง

๒.๑ ระบุประเด็นความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงาน เพื่อนำไปใช้การประเมินความเสี่ยงนั้น ดังต่อไปนี้

๑. ความเสี่ยงเชิงยุทธศาสตร์ คือ ความเสี่ยงที่เกิดจากการกำหนดกลยุทธ์ และนโยบายในการบริหารงานที่ทำให้ไม่บรรลุผลตามเป้าหมายในแต่ละประเด็นยุทธศาสตร์ของหน่วยราชการ

๒. ความเสี่ยงด้านธรรมาภิบาล คือ ความเสี่ยงด้านธรรมาภิบาลที่เกิดขึ้นในกระบวนงานหลักขององค์กร เช่นความมีประสิทธิภาพ ความคุ้มค่า ความโปร่งใสตรวจสอบได้ เป็นต้น

๓. ความเสี่ยงด้านกระบวนการ คือความเสี่ยงที่เกิดขึ้นในกระบวนงานต่าง ๆ ที่ทำให้เกิดความผิดพลาดในการปฏิบัติงาน จึงต้องมีการกำหนดมาตรฐานในการปฏิบัติงาน

๔. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ ความเสี่ยงที่ก่อให้เกิดความเสียหายแก่ระบบสารสนเทศของหน่วยราชการ เช่น ความเสี่ยงจากการไม่ทำการสำรองข้อมูล ความเสี่ยงจากการติดไวรัส ความเสี่ยงจากระบบไฟฟ้าสำรองไม่ทำงาน เป็นต้น

๒.๒ กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๒.๓ ประเมินความเสี่ยงโดยคำนึงถึงองค์ประกอบดังต่อไปนี้

๒.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๒.๓.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๒.๓.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๒.๔ เลือกประเด็นความเสี่ยงมาควบคุมตามความเหมาะสมและทรัพยากร

๒.๕ มีการทบทวนประเมินความเสี่ยงเป็นระยะเวลาสม่ำเสมอหรือตามที่กำหนด

ส่วนที่ ๓
แนวปฏิบัติของผู้ดูแลระบบ

๑. วัตถุประสงค์

เพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ดูแลระบบ ในการบริหารจัดการ กำกับ ดูแลเครื่องคอมพิวเตอร์และระบบเครือข่ายให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งการสอดส่องดูแลการใช้งานของผู้ใช้บริการให้เป็นไปตามแนวนโยบาย

๒. แนวปฏิบัติของผู้ดูแลระบบ

๒.๑ ผู้ดูแลระบบ มีหน้าที่ ดังต่อไปนี้

๒.๑.๑ กำกับให้มีการตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ กำหนดวิธีการแก้ไขเมื่อเกิดข้อบกพร่อง หากเกิดจากการใช้งานของผู้ใช้บริการ ให้รีบแจ้งผู้ใช้บริการผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบ (System Administrator) พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

๒.๑.๒ เฝ้าระวังกำกับการติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๒.๑.๓ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย

๒.๑.๔ ตรวจสอบการลบข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์แม่ขาย (Server) อย่างถาวร หรือทำลายข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของหน่วยงานบนเครื่องคอมพิวเตอร์และระบบเครือข่าย เมื่อหมดความจำเป็นในการใช้งาน ด้วยวิธีการตามมาตรฐาน DOD ๕๒๒๐.๒๒-M

๒.๑.๕ กำกับและตรวจสอบรวมถึงดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๒.๑.๖ ดูแลรักษาและปรับปรุงบัญชีจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์การใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

๒.๑.๗ ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้บริการให้มีการกำหนดรหัสผ่าน(Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password)

๒.๑.๘ ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๒.๑.๙ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

๒.๑.๑๐ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๒.๑.๑๑ เมื่อผู้ดูแลระบบ (System Administrator) พ้นจากหน้าที่จะต้องคืนทรัพย์สินของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้หัวหน้าหน่วยงาน หรือผู้ที่ได้รับมอบหมาย ตรวจสอบการคืนทรัพย์สิน

๒.๒ ผู้ดูแลระบบ (System Administrator) จะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

๒.๒.๑ เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคล ที่เข้าถึงสื่อดังกล่าวได้

๒.๒.๒ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ (System Administrator) สามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบพัฒนาระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

๒.๒.๓ ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้

๒.๒.๔ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum ๐) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ส่วนที่ ๔
แนวปฏิบัติการควบคุมการเข้าถึงพัฒนาระบบสารสนเทศและระบบเครือข่าย

๑. วัตถุประสงค์

มาตรการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน จัดทำเพื่อป้องกันการบุกรุกผ่านระบบเครือข่ายจนสามารถสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายได้ รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

๒. แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย

๒.๑ หน่วยงานในสังกัดกรมวิทยาศาสตร์การแพทย์ กำหนดมาตรหรือวิธีการเข้าใช้งานระบบสารสนเทศของหน่วยงาน โดยบุคคลจากหน่วยงานภายนอกที่ต้องการเข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือหัวหน้าหน่วยงานในกรณีที่เป็นศูนย์วิทยาศาสตร์การแพทย์

๒.๒ ผู้ดูแลระบบ กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศและเครือข่ายให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศและเครือข่าย โดยมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๒.๓ ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามสถานะการเข้าใช้งานระบบสารสนเทศของหน่วยงาน และเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลเป็นระยะ

๒.๔ ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ เพื่อเป็นหลักฐานในการตรวจสอบ

๒.๕ ผู้ดูแลระบบ แจ้งสิทธิ์ในการเข้าใช้ให้ผู้ใช้บริการรับทราบสิทธิ์ที่มีในการเข้าใช้ระบบสารสนเทศ

๓. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบสารสนเทศและเครือข่าย

๓.๑ ผู้ดูแลระบบ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการในการขอใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๓.๒ ผู้ดูแลระบบ กำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๓ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๓.๓.๑ ทบทวนการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๓.๓.๒ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password) และกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

๓.๓.๓ ควรให้ผู้ใช้งานเก็บรหัสผ่านที่ได้รับไว้เป็นความลับส่วนบุคคลและไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓.๓.๔ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๓.๓.๕ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานด้วยสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบหรืออนุมัติจากผู้บังคับบัญชาและเจ้าของข้อมูล โดยมีการกำหนดระยะเวลาใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๔ ผู้ดูแลระบบ ต้องบริหารจัดการควบคุมการเข้าถึงข้อมูลตามประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลตามประเภทชั้นความลับ ดังต่อไปนี้

๓.๔.๑ กำหนดรายชื่อผู้ใช้ และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓.๔.๒ ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓.๔.๓ ควรใช้การเข้ารหัสที่เป็นมาตรฐานสากลเมื่อมีการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ เช่น SSL VPN หรือ XML Encryption เป็นต้น

๓.๔.๔ ควรกำหนดให้มีอายุของหัสผ่าน (Password) ตามระดับความสำคัญของข้อมูล

๓.๔.๕ กำหนดให้มีมาตรการหรือวิธีการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ก่อนการส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๔.๑ ผู้ดูแลระบบ ควรมีข้อมูลขอบเขตของสัญญาณเครือข่ายจากอุปกรณ์กระจายสัญญาณ (Access Point) ควบคุมให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด โดยการสร้างและประเมินขอบเขตพื้นที่สัญญาณเป็นระยะ

๔.๒ ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำ อุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

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

๔.๔ ผู้ดูแลระบบ ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ รหัสผ่านของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address ชื่อผู้ใช้ และรหัสผ่าน ตามที่กำหนดให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๔.๕ ผู้ดูแลระบบ ควรมีกำหนดสิทธิการเข้าถึงและการใช้งานหรือทำการการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๔.๖ ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๔.๗ ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย ในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติอันเป็นปัญหาต่อระบบ ให้ผู้ดูแลระบบ รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบหรือหัวหน้าหน่วยงานทันที

๔.๘ ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือ

ข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๕. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๕.๑ ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๕.๒ ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๕.๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

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

๕.๕ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๕.๕.๑ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๕.๒ ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๕.๕.๓ ต้องกำหนดให้มีวิธีจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย ให้เป็นไปตามที่กำหนด

๕.๕.๔ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก ที่มีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๕.๕.๕ ระบบเครือข่ายควรติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๕.๕.๖ การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน ผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

๕.๕.๗ ควรมีการจัดการให้เลขที่อยู่ไอพีที่ใช้ภายในหน่วยงานไม่สามารถมองเห็นได้จากเครือข่ายภายนอก

๕.๕.๘ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๕.๙ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๖ ผู้ดูแลระบบ (System Administrator) ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในเรื่องการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

๕.๗ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๕.๗.๑ ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้

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

๕.๗.๓ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๕.๗.๔ ควรตรวจสอบการทำงานของบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๕.๘ ให้ศูนย์เทคโนโลยีสารสนเทศ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

๕.๘.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องดำเนินการขออนุญาตเข้าใช้งานเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้มีหน้าที่รับผิดชอบหรือหัวหน้าหน่วยงาน

๕.๘.๒ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๕.๘.๓ วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย หรือหัวหน้าหน่วยงาน

๕.๘.๔ การขอเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๕.๘.๕ การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

ส่วนที่ ๕
แนวปฏิบัติของผู้ใช้บริการในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

๑. วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้บริการ ได้รับทราบหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งสามารถปฏิบัติได้อย่างสอดคล้องกับระเบียบกรมวิทยาศาสตร์การแพทย์ว่าด้วย การใช้งานระบบเครือข่ายคอมพิวเตอร์อย่างปลอดภัย พ.ศ. ๒๕๕๔ อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความถูกต้องและพร้อมใช้งานอยู่เสมอ

๒. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๑ ผู้ใช้บริการจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑.๑ ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๒.๑.๒ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๒.๑.๓ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

๒.๑.๔ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

๒.๑.๕ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

๒.๑.๖ นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๒.๑.๗ เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม ๒.๑.๑ ๒.๑.๒ ๒.๑.๓ ๒.๑.๔ ๒.๑.๕ หรือ ๒.๑.๖

๒.๒ ผู้ใช้บริการจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตาม ๒.๑ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๒.๓ ผู้ใช้บริการจะต้องไม่กระทำการดังต่อไปนี้

๒.๓.๑ เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

๒.๓.๒ นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๒.๓.๓ เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

๒.๓.๔ กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูล

คอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

๒.๓.๕ ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

๒.๓.๖ กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

๒.๓.๗ ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-mail) แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

๒.๓.๘ กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๒.๓.๙ จำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม ๒.๓.๑ ๒.๓.๒ ๒.๓.๓ ๒.๓.๔ ๒.๓.๕ ๒.๓.๖ ๒.๓.๗ หรือ ๒.๓.๘

๒.๔ การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

๒.๔.๑ ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่ทางราชการ

๒.๔.๒ ไม่คัดลอกโปรแกรมต่างๆ ที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๔.๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ของหน่วยงานจะต้องกำหนดโดยเจ้าหน้าที่ที่รับผิดชอบของหน่วยงานเท่านั้น

๒.๔.๔ ไม่ทำการปรับแต่งไบออส (BIOS) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

๒.๔.๕ ไม่ทำการเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์ของหน่วยงานที่กำหนดไว้แล้ว

๒.๔.๖ หากผู้ใช้บริการที่มีความประสงค์จะขอใช้เลขที่อยู่ไอพีสาธารณะ (Public IP Address) จะต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๒.๔.๗ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๒.๔.๘ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานได้ เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๒.๔.๙ ไม่ใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

๓. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑ ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

๓.๒ ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓.๓ ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๓.๔ ผู้ใช้บริการควรทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ประจำที่หน้าจอเป็นเวลานาน

๔. แนวปฏิบัติการใช้งานบัญชีผู้ใช้บริการ (Account)

๔.๑ ผู้ใช้บริการที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๔.๒ ผู้ใช้บริการจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา เพื่อการรับผิดชอบตามข้อ ๔.๑

๔.๓ ผู้ใช้บริการจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๕. แนวปฏิบัติการกำหนดรหัสผ่าน (Password) สำหรับเครื่องคอมพิวเตอร์

๕.๑ รหัสผ่าน ควรมีความยาวไม่น้อยกว่า ๖ ตัวอักษร โดยรหัสผ่านที่ดีควรมีการผสมกันระหว่างตัวเลข ตัวอักษรตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆ ด้วย

๕.๒ ไม่ควรกำหนดรหัสผ่าน จากชื่อ หรือชื่อสกุลของผู้ใช้บริการ ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์

๕.๓ ควรทำการเปลี่ยนรหัสผ่าน เพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานทุก ๓-๖ เดือน หรือเปลี่ยนรหัสผ่าน ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๕.๔ ผู้ใช้บริการจะต้องเก็บรักษารหัสผ่าน สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มาโดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๖. แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

๖.๑ เครื่องคอมพิวเตอร์ที่ใช้งานภายในหน่วยงานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๖.๒ ผู้ใช้บริการควรทำการอัพเดท (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๖.๓ ห้ามมิให้ผู้ใช้บริการทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้าย (Malware) ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๖.๔ หากผู้ใช้บริการพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย (Malware) ห้ามมิให้ผู้ใช้บริการเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้าย (Malware) ไปยังเครื่องคอมพิวเตอร์อื่นๆ

๖.๕ ก่อนการใช้งานสื่อบันทึกพกพาเชื่อมต่อเข้าระบบ ควรมีการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware)

๖.๖ ในการรับส่งข้อมูลคอมพิวเตอร์ หรือสารสนเทศ (Information) ผ่านทางระบบเครือข่าย ผู้ใช้บริการต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) ก่อนการรับส่งทุกครั้ง

๖.๗ ผู้ใช้บริการควรทำการตรวจสอบไฟล์ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันโปรแกรมประสงค์ร้าย (Malware) เป็นการป้องกันในการเปิดไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น

๗. แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet)

๗.๑ ผู้ใช้บริการต้องเชื่อมต่อระบบคอมพิวเตอร์ของหน่วยงานเพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามผู้ใช้บริการทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรแล้ว

๗.๒ ผู้ใช้บริการต้องเข้าถึงแหล่งข้อมูลที่มั่นใจว่าไม่เป็นอันตรายต่อระบบสารสนเทศและเครือข่ายของหน่วยงาน และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน เป็นต้น

๗.๓ ห้ามผู้ใช้บริการเปิดเผยข้อมูลที่เป็นความลับของหน่วยงานผ่านระบบอินเทอร์เน็ต (Internet)

๗.๔ ผู้ใช้บริการต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๗.๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้บริการต้องคำนึงถึงความรับผิดชอบในการเสนอความคิดเห็นและการเปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน และต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคคลากรของหน่วยงานอื่นๆ

๗.๖ ผู้ใช้งานควรตั้งค่าในเว็บบราวน์เซอร์ให้ทำการลบค่าการใช้งาน เช่น คุ๊กกี้ รหัสผ่าน และข้อมูลสำรองระหว่างใช้งานของโปรแกรมเว็บบราวน์เซอร์เมื่อปิดการทำงานโปรแกรม

๗.๗ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้บริการทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๘. แนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑ แนวปฏิบัติการใช้งานสำหรับผู้ใช้บริการ

๘.๑.๑ ผู้ใช้บริการที่ต้องการขอลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงาน ยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์บัญชีผู้ใช้บริการรายใหม่และรหัสผ่าน (Password)

๘.๑.๒ ผู้ใช้บริการที่ได้รับรหัสผ่าน (Password) ครั้งแรกในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นจะต้องเปลี่ยนรหัสผ่าน (Password) โดยทันที

๘.๑.๓ ผู้ใช้บริการไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๘.๑.๔ ผู้ใช้บริการควรมีการเปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือน

๘.๑.๕ ผู้ใช้บริการไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

๘.๑.๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นผู้ใช้บริการควรทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑.๗ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้บริการไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑.๘ ผู้ใช้บริการมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๘.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ

๘.๒.๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้บริการ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การโอนย้าย เป็นต้น

๘.๒.๒ ผู้ดูแลระบบ (System Administrator) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้บริการใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

ส่วนที่ ๖
แนวปฏิบัติการสำรองข้อมูล

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๒. แนวปฏิบัติการสำรองข้อมูล

๒.๑ จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลพัฒนาระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

๒.๒ มีขั้นตอนการปฏิบัติการสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในพัฒนาระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

๒.๓ จัดเก็บข้อมูลที่สำรองในสื่อเก็บข้อมูล โดยมีข้อมูลของสิ่งที่เก็บบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน คงทนถาวร ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๒.๔ ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

ส่วนที่ ๗

แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒.๒ จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

๒.๓ ประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

ผู้เสนอ

ลงชื่อ.....

(นายปนิสภ์ วณิชชานนท์)

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

ผู้อนุมัติ

ลงชื่อ.....

(นายปฐม สวรรค์ปัญญาเลิศ)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

กรมวิทยาศาสตร์การแพทย์