ประกาศศูนย์สนับสนุนบริการสุขภาพที่ ๑
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔

ตามที่ กรมสนับสนุนบริการสุขภาพ มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒ เพื่อให้การบริหารจัดการและการพัฒนาระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความเชื่อถือได้และสามารถให้บริการได้อย่างต่อเนื่องสามารถป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กรมสนับสนุนบริการสุขภาพและหน่วยงานในสังกัด รวมทั้งประชาชนผู้ใช้บริการ ประกอบกับกรมสนับสนุนบริการสุขภาพตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ นั้น

ศูนย์สนับสนุนบริการสุขภาพที่ ๑ จึงออกประกาศนโยบายแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศศูนย์สนับสนุนบริการสุขภาพที่ ๑ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ ในประกาศนี้

(๑) “คณะกรรมการ” หมายความว่า คณะกรรมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑

(๒) “นโยบาย” หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นไปตามพระราชบัญญัติที่เกี่ยวข้อง ดังนี้

(๒.๑) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

(๒.๒) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๒.๓) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๒.๔) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

(๒.๕) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

(๓) “แนวปฏิบัติ” หมายความว่า ขั้นตอน วิธีการหรือข้อกำหนดให้ผู้ใช้งาน (User) และผู้ดูแลระบบ (Administrator) รวมทั้งบุคคลภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑ ได้ถือปฏิบัติตามนโยบาย ข้อ ๓ (๒)

(๔) “ผู้ดูแลระบบ”...

(๔) "ผู้ดูแลระบบ" (Administrator) หมายความว่า บุคลากร ศูนย์สนับสนุนบริการสุขภาพที่ ๑ ผู้ซึ่งได้รับมอบหมายจากเจ้าของระบบ (System Owner) หรือจากผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑ ให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และการบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ ของระบบเทคโนโลยีสารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑

(๕) "เจ้าของระบบ" (System Owner) หมายความว่า สำนัก/กอง/กลุ่ม/ศูนย์ ที่เป็นผู้รับผิดชอบในการพัฒนาระบบคอมพิวเตอร์ หรือ ระบบสารสนเทศ โดยมีวัตถุประสงค์เพื่อสนับสนุนภารกิจการปฏิบัติงานของหน่วยงานให้เกิดประสิทธิภาพต่อกรมสนับสนุนบริการสุขภาพในภาพรวม หรือตามที่อธิบดีให้ดำเนินงาน หรือมีหน้าที่อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน (User)

(๖) "ผู้ใช้งาน" (User) หมายความว่า บุคลากร ศูนย์สนับสนุนบริการสุขภาพที่ ๑ ทุกระดับ ซึ่งเป็นข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานจ้างเหมาและบุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ระบบเครือข่ายและโปรแกรมประยุกต์ของ และ/หรือเกี่ยวข้องกับการใช้ประโยชน์จากระบบเทคโนโลยีสารสนเทศ ศูนย์สนับสนุนบริการสุขภาพที่ ๑

(๗) "สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑

(๘) "สินทรัพย์" (asset) หมายความว่า ฮาร์ดแวร์ ซอฟท์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งอื่นใดก็ตามที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑ ประกอบด้วย

(๘.๑) "ฮาร์ดแวร์" (Hardware) หมายความว่า อุปกรณ์คุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้

- เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบเครื่องแม่ข่ายปกติ (Rack Server)
- เครื่องคอมพิวเตอร์ลูกข่าย (Client) อันได้แก่ เครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Laptop) อุปกรณ์สื่อสารแบบพกพา (Tablet/Smart phone) รวมถึงอุปกรณ์สนับสนุนเครื่องพิมพ์ (printer) และอุปกรณ์สำรองข้อมูลของศูนย์สนับสนุนบริการสุขภาพที่ ๑
- อุปกรณ์โครงข่าย (Network) หรือ อุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) หรืออุปกรณ์สำหรับเชื่อมต่อระบบสื่อสาร (Router, Switch, Access Point) หรืออุปกรณ์จัดเก็บบันทึกการใช้งาน (Log File)

(๘.๒) "โปรแกรมประยุกต์" (Program) หมายความว่าระบบคุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้ ระบบประเภท System Software, Database Software, Software Tool และ Application Software ที่ใช้งานร่วมกับอุปกรณ์ในหัวข้อ Hardware

(๘.๓) "เครือข่าย" (Network and Communication) หมายความว่า ระบบเทคโนโลยีด้านการสื่อสารโทรคมนาคมของ ศูนย์สนับสนุนบริการสุขภาพที่ ๑

(๘.๔) "ระบบสารสนเทศ" หมายความว่า ระบบงานคอมพิวเตอร์ เช่น เว็บไซต์ (Website) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น หรืออุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับการพัฒนา หรือติดตั้ง หรือการนำมาประยุกต์ใช้ เพื่อสนับสนุนการปฏิบัติงานของศูนย์สนับสนุนบริการสุขภาพที่ ๑

(๘.๕) "ข้อมูลสารสนเทศ" หมายความว่า ข้อมูล (Data) หรือ สารสนเทศ (Information) ที่อยู่ในรูปของเอกสารอิเล็กทรอนิกส์ เช่น แฟ้มข้อมูล (Files) ฐานข้อมูล (Database) เป็นต้น ของศูนย์สนับสนุนบริการสุขภาพที่ ๑

(๙) "พื้นที่ปฏิบัติงานทั่วไป"...

(๙) "พื้นที่ปฏิบัติงานทั่วไป" (General Working Area) หมายความว่า พื้นที่สำหรับการปฏิบัติงานภายในศูนย์สนับสนุนบริการสุขภาพที่ ๑ ซึ่งได้มีการติดตั้งเครื่องคอมพิวเตอร์ตั้งโต๊ะ เครื่องคอมพิวเตอร์พกพา อุปกรณ์ต่อพ่วงและเครือข่ายแบบมีสาย (LAN) และไร้สาย (Wireless)

(๑๐) "ห้องเซิร์ฟเวอร์" (Server Room) หมายความว่า ศูนย์ข้อมูลและสารสนเทศของกรมสนับสนุนบริการสุขภาพ ตั้งอยู่ที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑ พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะเพื่อติดตั้งอุปกรณ์ในการประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ระบบจัดเก็บข้อมูล ระบบรักษาความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศและระบบป้องกันอัคคีภัย ซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์ ระบบข้อมูลและระบบสารสนเทศแก่ผู้ใช้งาน

(๑๑) "เครือข่าย" (Network System) หมายถึง ระบบเครือข่ายที่เชื่อมโยงกับอุปกรณ์ในหัวข้อ Hardware, Software และระบบสารสนเทศของ ศูนย์สนับสนุนบริการสุขภาพที่ ๑ ทั้งแบบใช้สายและไร้สาย

(๑๒) "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดแนวปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

ข้อ ๔ ศูนย์สนับสนุนบริการสุขภาพที่ ๑ ได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นลายลักษณ์อักษร ตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

๔.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๕

๔.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๖ ถึง ข้อ ๑๐

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) คณะกรรมการ มีส่วนร่วมในการจัดทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของ ศูนย์สนับสนุนบริการสุขภาพที่ ๑

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติฯ ดังกล่าวให้ชัดเจน

(๔) ต้องทบทวนและปรับปรุงนโยบาย อย่างน้อย ปีละ ๑ ครั้ง

๕.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control) มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง เพื่อให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวก รวดเร็ว และให้ความคุ้มครองข้อมูลที่ไม่เปิดเผย (Business Requirements for Access Control)

(๑.๑) การควบคุม...

(๑.๑) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๑.๒) การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Program and Information Access Control)

(๑.๓) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๒) การบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยแยกประเภทและจัดเก็บเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์และสภาพพร้อมใช้งาน และมีแผนฉุกเฉินเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องดำเนินการอย่างสม่ำเสมอ โดยกำหนดให้ต้องตรวจสอบ ควบคุมคุณภาพและดำเนินการตรวจประเมินระบบรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๔) การกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการรายงานเหตุการณ์ที่เสี่ยงต่อความมั่นคงปลอดภัยที่เกิดขึ้น

(๕) การสร้างความรู้ ความเข้าใจการใช้งานระบบสารสนเทศหรือระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ ความเข้าใจ โดยการจัดทำคู่มือ การฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ผู้ใช้งาน

ข้อ ๖ ศูนย์สนับสนุนบริการสุขภาพที่ ๑ ได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พร้อมทั้งได้กำหนดให้ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑ เป็นผู้กำกับ ดูแล และติดตามผู้ใช้งาน (User) ปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าวไว้อย่างชัดเจน ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้ระบบสารสนเทศและการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

(๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน

(๓) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๔) การควบคุมการเข้าถึงเครือข่าย

(๕) การควบคุมการเข้าถึงระบบปฏิบัติการ

(๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

(๗) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ

(๘) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ ๗ ศูนย์สนับสนุนบริการสุขภาพที่ ๑ ได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติด้วยวิธีการใดวิธีการหนึ่ง ให้ผู้ใช้งาน (User) และบุคคลภายนอกทราบ เพื่อให้สามารถเข้าใจ เข้าถึงและปฏิบัติตามด้วยหนังสือเวียนภายในองค์กร หรือเว็บไซต์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑

ข้อ ๘ หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ ของศูนย์สนับสนุนบริการสุขภาพที่ ๑ เกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืน

การปฏิบัติตามนโยบาย...

ที่ก่อให้เกิดความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑ เพื่อรายงานต่อผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑

ข้อ ๙ ศูนย์สนับสนุนบริการสุขภาพที่ ๑ กำหนดให้ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์ ระบบสารสนเทศและข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่ศูนย์สนับสนุนบริการสุขภาพที่ ๑ หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับนี้

ประกาศ ณ วันที่ ๓๐ ตุลาคม พ.ศ. ๒๕๖๓

(ลงชื่อ)

(นายกำพล ใหลมา)

ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔
ศูนย์สนับสนุนบริการสุขภาพที่ ๑

กฎหมายและกฎระเบียบที่เกี่ยวข้อง

๑. ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม
๒. ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒
๓. ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๔. ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม
๕. ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

แนวปฏิบัติประกอบด้วย ดังนี้

หมวด ๑
การเข้าถึงและควบคุมการใช้งานสารสนเทศ
และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

วัตถุประสงค์

เพื่อให้บุคลากรศูนย์สนับสนุนบริการสุขภาพที่ ๑ และบุคลากรภายนอก ให้มีความรู้ ความเข้าใจและสามารถปฏิบัติตามแนวทางการปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศและการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ พร้อมทั้งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ

นโยบาย

บุคลากรศูนย์สนับสนุนบริการสุขภาพที่ ๑ และบุคลากรภายนอกต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศและการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูลให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้

๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศและการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ต้องสอดคล้อง และเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ

๑.๒ งานเทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มบริหารงานทั่วไปและแผนงาน มีหน้าที่หน้าในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน (User) สำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๓ เจ้าของระบบ (system Owner) มีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน

๑.๓ ผู้ดูแลระบบ (Administrator) มีหน้าที่กำหนดสิทธิให้แก่ผู้ใช้งาน

๑.๔ ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

๑.๕ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ และอุปกรณ์ในการประมวลผลข้อมูล ทั้งทางกายภาพ และจากระยะไกล บุคคลภายนอกดังกล่าว ต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจ จากคณะกรรมการและต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

๑.๖ การเข้าถึงห้องเซิร์ฟเวอร์ (Server Room) เพื่อปฏิบัติงานที่เกี่ยวข้องกับอุปกรณ์ในการประมวลผลข้อมูล ให้ดำเนินการ ดังนี้

๑.๖.๑ งานเทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มบริหารงานทั่วไปและแผนงาน ต้องกำหนดหลักเกณฑ์การปฏิบัติงานควบคุมระบบห้องเซิร์ฟเวอร์ (Server Room) และการเข้าใช้งานห้องเซิร์ฟเวอร์ (Server Room)

๑.๖.๒ การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องเซิร์ฟเวอร์ (Server Room) ต้องได้รับอนุมัติจากผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑ ก่อนเริ่มดำเนินการทุกครั้ง

๒. การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนดดังนี้

๒.๑ สิทธิของผู้ใช้งาน (User) ประกอบด้วย

๒.๑.๑ อ่านอย่างเดียว

๒.๒.๒ สร้างข้อมูล

๒.๒.๓ แก้ไขข้อมูล

๒.๒.๔ ลบข้อมูล

๒.๒ สิทธิผู้ดูแลระบบ (Administrator) กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การกำหนดประเภทของข้อมูล ลำดับความสำคัญ ลำดับชั้นความลับ รวมถึงระดับชั้น การเข้าถึง เวลาที่เข้าถึง และช่องทางการเข้าถึง ดังนี้

๓.๑ ประเภทของข้อมูล แบ่งเป็น ๓ ประเภท ดังนี้

๓.๑.๑ ข้อมูลสารสนเทศสำหรับการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร และข้อมูลงบประมาณรายจ่าย (SMART)

๓.๑.๒ ข้อมูลสารสนเทศสำหรับการสนับสนุนการปฏิบัติงาน ได้แก่ ข้อมูลระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ (GFMIS)

๓.๑.๓ ข้อมูลสารสนเทศสำหรับการเผยแพร่แก่ประชาชนทั่วไปและผู้ที่สนใจ ได้แก่ ข้อมูลในเว็บไซต์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑

๓.๒ ลำดับความสำคัญของข้อมูล แบ่งเป็น ๓ ระดับ ดังนี้

๓.๒.๑ สำคัญมากที่สุด

๓.๒.๒ สำคัญมาก

๓.๒.๓ ปกติ

๓.๓ ลำดับชั้นความลับของข้อมูล แบ่งเป็น ๔ ระดับ ดังนี้

๓.๓.๑ ลับที่สุด หมายความว่า ความลับที่มีความสำคัญที่สุดเกี่ยวกับข่าวสาร วัตถุ หรือบุคคล ซึ่งถ้าหากความลับดังกล่าวทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือเป็นภัยอันตรายต่อความมั่นคงปลอดภัย หรือความสงบเรียบร้อยของประเทศชาติ หรือพันธมิตร หรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้องอย่างร้ายแรงที่สุด

๓.๓.๒ ลับมาก หมายความว่า ความลับที่มีความสำคัญมากเกี่ยวกับข่าวสาร วัตถุ หรือบุคคล ซึ่งถ้าหากความลับดังกล่าวทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือเป็นภัยอันตรายต่อความมั่นคงปลอดภัย หรือความสงบเรียบร้อยของประเทศชาติ หรือพันธมิตร หรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้องอย่างร้ายแรง

๓.๓.๓ ลับ หมายความว่า ความลับที่มีความสำคัญเกี่ยวกับข่าวสาร วัตถุ หรือบุคคล ซึ่งถ้าหากความลับดังกล่าวทั้งหมด หรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายต่อราชการ หรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้องได้

๓.๓.๔ ปกปิด หมายความว่า ความลับซึ่งไม่พึงเปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบ โดยสงวนไว้ให้ทราบเฉพาะบุคคลที่มีหน้าที่ต้องทราบเพื่อประโยชน์ในการปฏิบัติภารกิจองค์กรเท่านั้น

๓.๔ ระดับชั้นการเข้าถึง แบ่งเป็น ๓ ระดับ ดังนี้

๓.๔.๑ กลุ่มผู้บริหาร

๓.๔.๒ กลุ่มผู้ปฏิบัติงาน

๓.๔.๓ กลุ่มประชาชนทั่วไปและผู้ที่สนใจ

๓.๕ เวลาที่เข้าถึง

ระบบคอมพิวเตอร์และระบบสารสนเทศสามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง ๗ วัน

๓.๖ ช่องทางการเข้าถึง

ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศได้ ๒ ช่องทาง ดังนี้

๓.๖.๑ ระบบเครือข่ายภายใน (Intranet)

๓.๖.๒ ระบบเครือข่ายภายนอก (Internet)

๔. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ แบ่งเป็น ๒ ส่วน ดังนี้

๔.๑ การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้สอดคล้องตามภารกิจ

๔.๑.๑ เจ้าของระบบ (System Owner) อนุมัติสิทธิให้ผู้ใช้งาน (User) ตามภารกิจ เพื่อให้สามารถเข้าถึงข้อมูลในระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะในส่วนที่ได้รับมอบหมาย ตามความจำเป็นในการใช้งาน

๔.๑.๒ ผู้ดูแลระบบ (Administrator) กำหนดสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน (User) ตามที่เจ้าของระบบ (system Owner) อนุมัติ

๔.๒ การปรับปรุงการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศให้สอดคล้อง ตามภารกิจและการรักษาความมั่นคงปลอดภัย ผู้ดูแลระบบ (Administrator) ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย โอน ลาออก หรือสิ้นสุดการจ้างเพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัยตามที่กำหนด

หมวด ๒
การบริหารจัดการการเข้าถึงของผู้ใช้งาน

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งาน (User) ที่ได้รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดสารสนเทศ และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนบุคลากรใหม่ เพื่อรับสิทธิ การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

๒. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อบุคลากรไม่ได้ปฏิบัติงานที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑ แล้ว

๓. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน อย่างรัดกุมโดยให้มีการ ควบคุม จำกัด และเปลี่ยนสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ ที่ได้รับมอบหมาย ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๔. กำหนดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจาง

๕. กำหนดให้มีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักและความเข้าใจเรื่องภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

แนวปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้

๑.๑ ให้งานเทคโนโลยีสารสนเทศและการสื่อสารกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศสำหรับบุคลากร ศูนย์สนับสนุนบริการสุขภาพ และบุคคลภายนอกอย่างน้อย ประกอบด้วยชื่อ นามสกุล ตำแหน่ง กลุ่มงาน หมายเลขโทรศัพท์ และจดหมายอิเล็กทรอนิกส์ (E - Mail) ที่ใช้งานในปัจจุบันเพื่อเป็นการยืนยันตัวตน

๑.๒ การขออนุญาตเขาถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

๑.๒.๑ กรณีบุคลากรศูนย์สนับสนุนบริการสุขภาพที่ ๑

(๑) ให้บุคลากรใหม่กรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคลากรของศูนย์สนับสนุนบริการสุขภาพที่ ๑ ในวันรายงานตัว

(๒) ให้งานเทคโนโลยีสารสนเทศและการสื่อสาร ทำหนังสือแจ้งขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคลากร ให้กลุ่มเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ เพื่อสร้างบัญชีผู้ใช้งานและกำหนดรหัสผ่าน

(๓) ให้เจ้าของระบบ (System Owner) อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคลากรใหม่

(๔) ให้ผู้ดูแลระบบ (Administrator) กำหนดสิทธิให้บุคลากรใหม่ หรือแจ้งเรื่องไปยังเจ้าของระบบ (System Owner) เพื่อกำหนดสิทธิให้บุคลากรใหม่ ตามที่ เจ้าของระบบ (System Owner) อนุมัติ พร้อมทั้งแจ้งให้บุคลากรใหม่ได้รับทราบ

๑.๒.๒ กรณีบุคคลภายนอก

(๑) ให้บุคลคลภายนอกกรอกข้อมูลลงในแบบฟอร์มการขออนุญาต แจ้งความประสงค์พร้อมเหตุผลในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ สำหรับบุคคลภายนอก

(๒) ให้ผู้ดูแลระบบ (Administrator) พิจารณาเหตุผลดังกล่าวก่อนดำเนินการสร้างบัญชีผู้ใช้งานและกำหนดรหัสผ่าน หรือแจ้งเรื่อง

(๓) ให้เจ้าของระบบ (System Owner) อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคคลภายนอก

(๔) ให้ผู้ดูแลระบบ (Administrator) กำหนดสิทธิให้ผู้ใช้งาน (User) หรือแจ้งเรื่องไปยังเจ้าของระบบ (System Owner) เพื่อกำหนดสิทธิให้ผู้ใช้งาน (User) ตามที่เจ้าของระบบ (System Owner) อนุมัติ พร้อมทั้งแจ้งให้บุคคลภายนอกได้รับทราบ

๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และการกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้ใช้ชื่อภาษาอังกฤษตามบัตรประจำตัวประชาชนตามด้วยเครื่องหมาย “.”ตามด้วยอักษรนามสกุลตัวแรกเป็นภาษาอังกฤษ

๑.๓.๒ การกำหนดรหัสผ่าน (Password) ชุดของตัวอักษร ตัวเลข และอักขระพิเศษ อย่างน้อย ๘ ตัวขึ้นไป และยากต่อการคาดเดา โดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือ ในการตรวจสอบยืนยันตัวตน (Authentication) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๓.๓ ให้ผู้ดูแลระบบ (Administrator) แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้อยู่ใช้งาน (User) ทราบโดยตรง

๑.๓.๔ เมื่อบุคลากรศูนย์สนับสนุนบริการสุขภาพที่ ๑ มีการเปลี่ยนชื่อหรือนามสกุล งานเทคโนโลยีสารสนเทศและการสื่อสาร ต้องทำการเปลี่ยนบัญชีผู้ใช้งาน (Username)

๑.๔ บัญชีผู้ใช้งาน (Username) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ได้จนกว่าบุคลากรหรือบุคคลภายนอกสิ้นสุดการปฏิบัติหน้าที่ในศูนย์สนับสนุนบริการสุขภาพที่ ๑ และงานเทคโนโลยีสารสนเทศและการสื่อสารดำเนินการยกเลิกสิทธิการใช้งาน

๒. การยกเลิกสิทธิการใช้งานของบุคลากรหรือบุคคลภายนอกให้ดำเนินการ ดังนี้

๒.๑ กรณีบุคลากรศูนย์สนับสนุนบริการสุขภาพที่ ๑

๒.๑.๑ ให้งานบุคลากร แจ้งงานเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก ให้โอน หรือสิ้นสุดการจ้าง

๒.๑.๒ งานเทคโนโลยีสารสนเทศและการสื่อสารจะปิดบัญชีผู้ใช้งาน (Username) เมื่อครบกำหนด ๑ วันหลังมีคำสั่งเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑

๒.๒ กรณีบุคคลภายนอก

งานเทคโนโลยีสารสนเทศและการสื่อสาร ยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศได้ทันทีที่หมดความจำเป็น

๓. การบริหารจัดการสิทธิของผู้ใช้งาน ในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศของผู้ใช้งาน (User) ให้ดำเนินการ ดังนี้

๓.๑ ผู้ดูแลระบบ (Administrator) ตรวจสอบสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศตามแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ สำหรับบุคลากร ศูนย์สนับสนุนบริการสุขภาพที่ ๑ หรือบุคคลภายนอกให้สอดคล้องกับคำสั่งมอบหมายให้ปฏิบัติราชการ และคำสั่งมอบอำนาจ หรือเหตุผลความจำเป็นของหน่วยงาน ที่มีความประสงค์ให้บุคคลภายนอก เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ แล้วแต่กรณี

๓.๒ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้งานบุคลากรแจ้งงานเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเปลี่ยนสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว

๓.๓ ในกรณีที่ผู้ใช้งาน (User) ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สูงกว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่องานเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งนี้ ต้องมีการกำหนดระยะเวลาการใช้งาน และยกเลิกสิทธิการใช้งานทันทีที่หมดความจำเป็น

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๔.๑ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๑ ปี และรหัสผ่าน (Password) ใหม่ ต้องไม่ซ้ำกับรหัสผ่านเดิมหรือตามความต้องการของผู้ใช้งานเอง โดยแจ้งความประสงค์มายังงานเทคโนโลยีสารสนเทศและการสื่อสาร

๔.๒ ในกรณีที่ผู้ใช้งาน (User) ลืมรหัสผ่าน (Password) ให้แจ้งงานเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อกำหนดรหัสผ่านชุดใหม่ โดยเลือกรับรหัสผ่านทาง Email ส่วนตัวเท่านั้น

๔.๓ ผู้ดูแลระบบ (Administrator) ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง

๔.๔ งานเทคโนโลยีสารสนเทศและการสื่อสารจัดอบรม หรือถ่ายทอดสื่อสารให้ความรู้แก้ผู้ใช้งาน (User) เพื่อให้มีความรู้ ความเข้าใจ และเกิดความตระหนักถึงและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ อย่างน้อยปีละ ๑ ครั้ง หรือจัดให้ผู้ใช้งาน (User) เข้าร่วมการฝึกอบรมที่หน่วยงานอื่นจัดขึ้น

๔.๕ งานเทคโนโลยีสารสนเทศและการสื่อสารกำหนดมาตรการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศ ตามความเหมาะสม ได้แก่ การไม่เปิดจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่ระบุที่มาหรือชื่อผู้ส่งที่น่าสงสัย โดยให้ลบจดหมายอิเล็กทรอนิกส์ทันที หรือแจ้งเตือนผู้ใช้งาน (User) เมื่อมีไวรัสแพร่ระบาด

หมวด ๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนา ข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

๑. กำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)

๒. กำหนดแนวปฏิบัติในการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งานดูแล เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศได้

๓. กำหนดแนวปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศ เพื่อไม่ให้สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งาน ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔. กำหนดให้ผู้ใช้งาน อาจนำการเข้ารหัสข้อมูล (Encryption) มาใช้กับการรับส่งข้อมูลที่สำคัญ หรือข้อมูลที่เป็นความลับของศูนย์สนับสนุนบริการสุขภาพที่ ๑ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

แนวปฏิบัติ

๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการดังนี้

๑.๑ ผู้ใช้งาน (User) ต้องกำหนดรหัสผ่าน ตามหมวด ๒ ข้อ ๑.๓.๒

๑.๒ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่าน ใหม่ทุก ๖ เดือน

๑.๓ ผู้ใช้งาน (User) ต้องไม่ใช้รหัสผ่าน (Password) ร่วมกับบุคคลอื่น และไม่ควรให้ระบบคอมพิวเตอร์หรือระบบสารสนเทศจำรหัสผ่าน (Password) ในการเข้าใช้งานโดยอัตโนมัติ

๑.๔ ผู้ใช้งาน (User) ต้องไม่เปิดเผยรหัสผ่าน (Password) สำหรับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเก็บเป็นความลับเสมือนเป็นสมบัติส่วนตัว ห้ามจดหรือเขียน รหัสผ่าน(Password) ที่ใช้งานไว้ในที่เปิดเผย

๑.๕ หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็น ในการเข้าถึง หลังจากดำเนินการเสร็จแล้วให้แจ้งเปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

๑.๖ หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของบัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดในเอกสารฉบับนี้แล้ว

๑.๗ ผู้ดูแลระบบ (Administrator) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๓ เดือน

๒. การป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน ผู้ใช้งานต้องออกจากระบบ (log Out) ทันทีเมื่อเลิกใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการตามหลักเกณฑ์ดังนี้

๓.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ในการประมวลผลข้อมูล มีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานของศูนย์สนับสนุนบริการสุขภาพที่ ๑ เท่านั้น

๓.๒ ระบบคอมพิวเตอร์และระบบสารสนเทศ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ตั้งโต๊ะ เครื่องคอมพิวเตอร์พกพา ควรติดตั้งด้วยซอฟต์แวร์ที่มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมาย หรือได้รับอนุญาตจากผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑

๓.๓ ระบบคอมพิวเตอร์และระบบสารสนเทศ ต้องได้รับการป้องกันด้วยรหัสผ่าน ของระบบพิสูจน์ตัวตนทุกครั้ง เมื่อเข้าใช้งานและออกจากระบบทันที ทุกครั้งเมื่อเลิกใช้งาน

๓.๔ ผู้ใช้งาน (User) ต้องรับผิดชอบต่อสินทรัพย์ (Asset) ของศูนย์สนับสนุนบริการสุขภาพที่ ๑ และให้ใช้งานด้วยความระมัดระวังเสมือนเป็นทรัพย์ของตน

๓.๕ ผู้ใช้งาน (User) ต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใด ๆ ที่เครื่องคอมพิวเตอร์ตั้งโต๊ะ หรือเครื่องคอมพิวเตอร์พกพา หรือระบบคอมพิวเตอร์และระบบสารสนเทศ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลต่องานเทคโนโลยีสารสนเทศและการสื่อสาร

๓.๖ ผู้ใช้งาน (User) ต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา หรืออุปกรณ์บันทึกข้อมูลอื่น ๆ เพื่อป้องกันการรั่วไหลของข้อมูล

๓.๗ บุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานระบบคอมพิวเตอร์และระบบสารสนเทศ ต้องขออนุมัติผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑ เป็นลายลักษณ์อักษร ก่อนเข้าปฏิบัติงาน

๓.๘ การทำลายอุปกรณ์บันทึกข้อมูลหรือการนำอุปกรณ์บันทึกข้อมูลกลับมาใช้งานใหม่ ให้ดำเนินการดังนี้

๓.๘.๑ การทำลายอุปกรณ์บันทึกข้อมูล เช่น Flash Drive CD/DVD Hard disk เป็นต้น ให้ใช้วิธีการทุบ หรือบดให้เสียหาย หรือเผาทำลายด้วยวิธีการทำลายตามมาตรฐานสากล

๓.๘.๒ การนำอุปกรณ์บันทึกข้อมูลไปใช้งานใหม่ ให้ฟอร์แมต (Format) อุปกรณ์บันทึกข้อมูลนั้นโดยใช้วิธีการตามมาตรฐานสากล

หมวด ๔
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึง

๒. กำหนดแนวปฏิบัติในการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาต ให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่าย ระบบคอมพิวเตอร์และระบบสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑ ได้

๓. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย โดยต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่าย เป็นการยืนยัน

๔. กำหนดให้บริหารจัดการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) โดยต้องปฏิบัติตามแนวปฏิบัติของกรมสนับสนุนบริการสุขภาพ

๕. กำหนดแนวปฏิบัติในการแบ่งแยกเครือข่าย โดยต้องแบ่งแยกเครือข่ายสำหรับผู้ใช้งาน (User) และสำหรับผู้ดูแลระบบ (Administrator)

๖. กำหนดแนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกันระหว่างหน่วยงาน

๗. กำหนดแนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลสารสนเทศ สอดคล้องกับแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

แนวปฏิบัติ

๑. การเข้าถึงเครือข่ายของผู้ใช้งาน (User)

๑.๑ การใช้งานระบบเครือข่ายภายนอก (Internet) ให้ดำเนินการดังนี้

๑.๑.๑ กำหนดให้ใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าใช้งานระบบเครือข่ายภายนอก (Internet)

๑.๑.๒ ห้ามใช้งานระบบเครือข่ายภายนอก (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) สูงที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ ได้แก่ สื่อบันเทิงต่าง ๆ ในเวลาราชการ

๑.๑.๓ ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม ลามก อนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์ เสื่อมเสีย

๑.๑.๔ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของศูนย์สนับสนุนบริการสุขภาพที่ ๑ ผ่านระบบเครือข่าย ภายนอก (Internet) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๕ ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๔ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเคร่งครัด ได้แก่ ห้ามเปิดเผยข้อมูลของทางราชการโดยไม่ได้รับอนุญาต ห้ามแพร่ภาพหรือข้อมูลใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือที่มีลักษณะลามก อนาจาร และไม่ทำการเผยแพร่หรือ

ส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าว ผ่านระบบเครือข่ายภายนอก (Internet) ห้ามเผยแพร่ภาพขอผู้อื่นที่เกิดจากการสร้างขึ้น ตัดต่อ ต่อเติม หรือดัดแปลงด้วยวิธีการ ทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่จะทำให้ผู้นั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑.๑.๖ ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่าง ๆ จากระบบเครือข่าย ภายนอก (Internet) เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๑.๗ หลักจากใช้งานระบบเครือข่ายภายนอก (Internet) แล้วให้ปิดเว็บบราวเซอร์ เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

๑.๒ การใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ให้ดำเนินการดังนี้

๑.๒.๑ ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม โดยเคร่งครัด และห้ามใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ในทางที่ ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศีลธรรม

๑.๒.๒ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ ด้วยการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ส่งโดยโดเมนเนม (Domain Name) ของกรมสนับสนุนบริการสุขภาพ (@hss.mail.go.th)

๑.๒.๓ ต้องตรวจสอบชื่อผู้ส่งจดหมายอิเล็กทรอนิกส์ ก่อนเปิดจดหมายอิเล็กทรอนิกส์ (E-Mail) เพื่อป้องกันการเปิดไฟล์อันตรายที่อาจมีไวรัสคอมพิวเตอร์ โดยเพราะไฟล์ปฏิบัติการ (Executable file) ได้แก่ ไฟล์ที่มีนามสกุล .exe, .com, .bat และ .inf ที่อาจนำเข้าสู่ระบบเครือข่ายศูนย์สนับสนุนบริการสุขภาพที่ ๑

๑.๒.๔ หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องออกจากระบบ (Log Out) ทันทีเพื่อป้องกันบุคคลอื่นเข้าใช้งาน

๑.๓ การใช้งานเครือข่ายไร้สาย (WiFi) ให้ดำเนินการดังนี้

๑.๓.๑ ผู้ดูแลระบบ (Administrator) ต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดเป็นค่ามาตรฐานมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้งเพื่อใช้งาน

๑.๓.๒ ผู้ใช้งาน (User) ต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (WiFi)

๑.๓.๓ ในการเข้าถึงเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายไร้สาย (WiFi) ผู้ใช้งาน (User) จะสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะที่ได้รับอนุญาตตามสิทธิ ของเครือข่ายไร้สาย (WiFi) เท่านั้น

๑.๓.๔ ผู้ใช้งาน (User) ต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็นทรัพย์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑ ไปใช้งานเครือข่ายไร้สาย (WiFi) ที่ไม่น่าเชื่อถือ

๑.๓.๕ ผู้ใช้งาน (User) ไม่ควรทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ระหว่างการใช้งาน เครือข่ายไร้สาย (WiFi) เนื่องจากอาจเกิดความไม่ปลอดภัยและอาจขาดการเสื่อมต่อของสัญญาณ

๑.๓.๖ ห้ามผู้ใช้งาน (User) ติดตั้งและเปิดการทำงานโปรแกรมประเภทดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายของศูนย์สนับสนุนบริการสุขภาพที่ ๑ และมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๔ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการดังนี้

๑.๔.๑ การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ ในนามของศูนย์สนับสนุนบริการสุขภาพที่ ๑ ผู้รับผิดชอบต้องแสดงตำแหน่ง หน้าที่ สังกัด ให้ชัดเจน เพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์ หรือเครื่องหมายแสดงสังกัดได้

๑.๔.๒ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ ควรนำเสนอเกี่ยวกับภารกิจของศูนย์สนับสนุนบริการสุขภาพที่ ๑ ได้แก่ วิสัยทัศน์ พันธกิจ ผลการดำเนินงาน และข่าวสาร ที่เป็นประโยชน์ มีความถูกต้อง ใช้

ภาษาที่สุภาพ และมีรูปแบบที่น่าสนใจ โดยเนื้อหาต้องผ่านความเห็นชอบจากผู้ได้รับมอบหมายหรือผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑ ก่อนทุกครั้ง

๑.๔.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของศูนย์สนับสนุนบริการสุขภาพที่ ๑ ผ่านเครือข่ายสังคมออนไลน์ เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๔.๔ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงในเรื่องที่เกี่ยวข้องต่อไป

๑.๔.๕ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากศูนย์สนับสนุนบริการสุขภาพที่ ๑ และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑.๔.๖ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที

๒. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร

การระบุและยืนยันตัวตนของผู้ใช้งานอยู่ภายนอกองค์กรต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง เพื่อตรวจสอบความถูกต้องในการพิสูจน์ยืนยันตัวตน (Authentication) ก่อนเข้าถึงเครือข่าย ระบบคอมพิวเตอร์ และระบบสารสนเทศ

๓. การระบุอุปกรณ์บนเครือข่าย ให้ดำเนินการดังนี้

๓.๑ งานเทคโนโลยีสารสนเทศและการสื่อสารต้องจัดทำผังระบบเครือข่าย (Network Diagram) พร้อมรายละเอียดอุปกรณ์บนเครือข่ายที่เห็นว่าจำเป็นต่อการใช้งาน ได้แก่ กลุ่มอุปกรณ์ เลขที่อยู่ไอพี (IP Address) และหมายเลขเฉพาะอุปกรณ์ (MAC Address) โดยให้ปรับปรุงทุก ๒ ปี หรือตามความเหมาะสม

๓.๒ การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ มาใช้งานบนเครือข่ายต้องได้รับอนุญาตจากงานเทคโนโลยีสารสนเทศและการสื่อสาร และผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑

๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ดำเนินการตามแนวปฏิบัติของกรมสนับสนุนบริการสุขภาพ

๕. การแบ่งแยกเครือข่าย แบ่งเป็น ๒ กลุ่ม ดังนี้

๕.๑ กลุ่มผู้ใช้งาน (User) ได้แก่ ระบบคอมพิวเตอร์และระบบสารสนเทศเพื่อสนับสนุนภารกิจหลักและระบบสารสนเทศเพื่อการสนับสนุนการปฏิบัติงาน

๕.๒ กลุ่มผู้ดูแลระบบ (Administrator) ได้แก่ อุปกรณ์รักษาความมั่นคงปลอดภัยสารสนเทศ อุปกรณ์บริหารจัดการเครือข่าย และระบบเครือข่ายโซนพิเศษ (Demilitarized Zone : DMZ)

๖. การควบคุมการเชื่อมต่อทางเครือข่าย ให้ดำเนินการดังนี้

๖.๑ ศูนย์สนับสนุนบริการสุขภาพที่ ๑ ต้องติดตั้งระบบป้องกันการบุกรุกโจมตีทางเครือข่าย (Firewall) เพื่อใช้เป็นจุดควบคุมการเชื่อมต่อทางเครือข่าย

๖.๒ ผู้ดูแลระบบ (Administrator) ต้องไม่เปิดเผยข้อมูลการเชื่อมต่อทางเครือข่าย ก่อนได้รับอนุญาตจากผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑

๖.๓ ผู้ดูแลระบบ (Administrator) มีหน้าที่ในการควบคุมการเชื่อมต่อสัญญาณหรือยกเลิก การเชื่อมต่อสัญญาณตามที่ได้รับอนุญาตจากผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑ ทั้งนี้ หากพบข้อผิดพลาดหรือเห็นว่าหมดความจำเป็นในการเชื่อมต่อสัญญาณให้รายงานผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑ ทันที

๖.๔ การเชื่อมต่อเครือข่ายสารสนเทศระหว่างหน่วยงานภายนอก ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑ และกลุ่มเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ พร้อมทั้งเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ของผู้ให้บริการที่มีความน่าเชื่อถือ

๗. การควบคุมการจัดเส้นทางบนเครือข่าย ให้ดำเนินการดังนี้

๗.๑ ผู้ดูแลระบบ (Administrator) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ และการรับ – ส่งหรือการไหลเวียนของข้อมูลหรือสารสนเทศเป็นไปอย่างรวดเร็ว

๗.๒ ผู้ดูแลระบบ (Administrator) ต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ใช้งาน (User) เป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

หมวด ๕
การควบคุมการเข้าถึงระบบปฏิบัติการ

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกัน การเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการ โดยต้องมีการควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวตนที่ปลอดภัย

๒. กำหนดแนวปฏิบัติในการระบุและยืนยันตัวตนของผู้ใช้งาน โดยต้องกำหนดให้ผู้ใช้งาน (User) มีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบบตัวตนของผู้ใช้งาน (User) ได้ เพื่อรองรับการยืนยันว่าเป็นผู้ใช้งานที่ได้รับอนุญาต

๓. กำหนดแนวปฏิบัติในการบริหารจัดการรหัสผ่าน โดยต้องจัดทำทะเบียนคุมจัดการรหัสผ่าน (Password) ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๔. กำหนดแนวปฏิบัติในการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการ ความมั่นคงปลอดภัยที่ได้กำหนดไว้

๕. กำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน (Session Time - Out)

๖. กำหนดระยะเวลาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time)

แนวปฏิบัติ

๑. ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าถึงระบบปฏิบัติการ

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน กำหนดให้ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง เพื่อตรวจสอบ ความถูกต้องในการพิสูจน์ยืนยันตัวตน (Authentication) ก่อนเข้าถึงระบบปฏิบัติการ (Operating System)

๓. งานเทคโนโลยีสารสนเทศและการสื่อสารต้องจัดทำทะเบียนคุมจัดการรหัสผ่าน (Password) ที่มีคุณภาพ กำหนดดังนี้

๓.๑ กรณีปกติ

การใช้รหัสผ่าน (Password) เดิม เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตน (Authentication) และตั้งรหัสผ่าน (Password) ใหม่ ไปในคราวเดียวกัน

๓.๒ กรณีลืมรหัสผ่าน

การเลือกใช้วิธีการตอบคำถามจากระบบ หรือแจ้งผู้ดูแลระบบ (Administrator) ดำเนินการตั้งค่ารหัสผ่านใหม่สำหรับผู้ใช้งาน (User)

๔. การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) กำหนดดังนี้

๔.๑ ผู้ใช้งาน (User) ต้องไม่ดัดแปลงหรือติดตั้งโปรแกรมอรรถประโยชน์ใด ๆ บนระบบปฏิบัติการ ทั้งนี้ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์ต่องานเทคโนโลยีสารสนเทศ

๔.๒ การใช้งานโปรแกรมอรรถประโยชน์อื่น ๆ นอกจากที่ติดตั้งมากับระบบปฏิบัติการ ได้แก่ โปรแกรมประประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรมแปลงไฟล์ข้อมูล (Formatter) กำหนดให้ผู้ดูแลระบบ (Administrator) เท่านั้นที่มีสิทธิใช้งาน

๕. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อเว้นว่างจากการใช้งาน (Session Time - Out) เมื่อครบ ๑๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง โดยให้ใช้งานได้ เป็นเวลา ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง และในกรณีที่เชื่อมต่อจากภายนอกกำหนดให้ใช้งานได้ภายใน วันเวลาราชการ เว้นแต่กรณีที่มีเหตุผลความจำเป็นให้ขออนุญาตผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑ และกลุ่มเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ

หมวด ๖
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยไม่ได้นับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศของผู้ใช้งาน (User) และฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่นตามสิทธิที่กำหนดไว้

๒. กำหนดแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อศูนย์สนับสนุนบริการสุขภาพที่ ๑ โดยต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ ที่ปฏิบัติงานจากภายนอกองค์กร

๓. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศจากความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๔. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) โดยต้องกำหนด ข้อปฏิบัติ แผนงาน และขั้นตอนการปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกหน่วยงาน

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ ให้ดำเนินการดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User) การกำหนดสิทธิตามตำแหน่งและหน้าที่ที่ได้รับมอบหมาย และการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้ แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง ซึ่งรวมถึงบุคลากรภายนอกหรือผู้รับจ้าง (Outsource) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศด้วย

๑.๒ ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งาน (User) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายภานอก ให้รับส่งข้อมูลข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) โยมรการเข้ารหัสรักษาความปลอดภัย Secure Sockets Layer (SSL)

๑.๓ การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) ให้ยึดแนวปฏิบัติกรมสนับสนุนบริการสุขภาพ

๒. ระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อศูนย์สนับสนุนบริการสุขภาพที่ ๑ ให้ดำเนินการดังนี้

๒.๑. ระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญต่อหน่วยงาน ดังนี้

๒.๑.๑ ระบบการบริหารจัดการความมั่นคงปลอดภัยและเครือข่าย ได้แก่ ระบบ Antivirus , ระบบ Active Directory , ระบบ Backup Systems , ระบบ Domain Name Server , ระบบ Dynamic Host Configuration Protocol , ระบบ Network Management , ระบบ Network Monitoring และระบบจัดเก็บข้อมูลกลาง

๒.๑.๒ ระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ (GFMIS)

๒.๒ ระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อศูนย์สนับสนุนบริการสุขภาพที่ ๑ ต้องได้รับการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกออกจากระบบอื่นๆ

๒.๓ ผู้ดูและระบบ (Administrator) ต้องแบ่งพื้นที่สำหรับการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายตามระดับความสำคัญและความปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อศูนย์สนับสนุนบริการสุขภาพที่ ๑ เพื่อควบคุมสภาพแวดล้อมโดยเฉพาะ

๒.๔ การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่ปฏิบัติงานจากภายนอกหน่วยงานเพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการ รบกวนมีผลกระทบและมีความสำคัญต่อหน่วยงานต้องเข้าถึงในสถานที่ที่มีความปลอดภัยและต้องได้รับอนุญาตจากงานเทคโนโลยีสารสนเทศและการสื่อสาร

๓. การควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ให้ดำเนินการดังนี้

๓.๑ ผู้ดูแลระบบ (Administrator) ต้องตรวจสอบเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ของผู้ใช้งาน (User) หรือบุคลากรภายนอก ก่อนนำมาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศ

๓.๑.๑ เครื่องคอมพิวเตอร์ต้องตรวจสอบ ดังนี้

๑. ระบบปฏิบัติการต้องได้รับการติดตั้งเวอร์ชั่นล่าสุด

๒. โปรแกรมตรวจสอบและป้องกันไวรัสคอมพิวเตอร์ต้องได้รับการอัพเดทฐานข้อมูลไวรัสคอมพิวเตอร์ที่เป็นปัจจุบัน

๓. ไม่ติดตั้งโปรแกรมประเภทดักจับข้อมูล (Network Sniffer) และโปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer)

๓.๑.๒ อุปกรณ์สื่อสารเคลื่อนที่ ได้แก่ Smart Phone และ tablet ต้องได้รับการยืนยันตัวตนโดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของผู้ใช้งาน (User) สำหรับเข้าใช้งาน

๔. การปฏิบัติงานจากภายนอกศูนย์สนับสนุนบริการสุขภาพที่ ๑ (Teleworking) กำหนด ดังนี้

๔.๑ ผู้ใช้งาน (User) ต้องปฏิบัติตามหมวด ๔ แนวปฏิบัติ ข้อ ๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร

๔.๒ บุคคลภายนอกต้องปฏิบัติตามหมวด ๒ แนวปฏิบัติ ข้อ ๑.๒ การขออนุญาตเขาถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (๑.๒.๒) กรณีบุคคลภายนอก และหากต้องปฏิบัติงานด้านเทคนิค จากภายนอกศูนย์สนับสนุนบริการสุขภาพที่ ๑ (Teleworking) ให้ดำเนินการตามที่งานเทคโนโลยีสารสนเทศและการสื่อสารกำหนดเป็นการเฉพาะคราว

๔.๓ เมื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศแล้ว ผู้ใช้งาน (User) ต้องระมัดระวัง ไม่ให้ผู้ไม่มีส่วนเกี่ยวข้องเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ สื่อสารเคลื่อนที่ได้และต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งาน

หมวด ๗
การจัดทำระบบสำรองของระบบสารสนเทศ

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูล สารสนเทศ และการกู้คืนข้อมูลสารสนเทศ และการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของศูนย์สนับสนุนบริการสุขภาพที่ ๑ ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉิน และการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและการกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่องแม้ในสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่างๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม และสามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง

นโยบาย

๑. พิจารณาคัดเลือกระบบสารสนเทศที่เหมาะสมในการจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้

๒. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑ เพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ

๓. กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบตามแผนบริหารความต่อเนื่อง ของศูนย์สนับสนุนบริการสุขภาพที่ ๑ ด้านสารสนเทศ

๔. ทดสอบสภาพพร้อมใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ และระบบสำรองตามแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑ อย่างน้อยปีละ ๑ ครั้ง

๕. กำหนดความถี่ของการปฏิบัติในแต่ละข้อ โดยต้องมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของหน่วยงาน

แนวปฏิบัติ

๑. งานเทคโนโลยีสารสนเทศและการสื่อสารต้องจัดทำระบบสำรองสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยมีขั้นตอน ดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) จัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูล และการกู้คืนข้อมูลสารสนเทศ

๑.๒ ผู้ดูแลระบบ (Administrator) กำหนดรูปแบบการสำรองข้อมูลของระบบการสำรองข้อมูล (Backup System) ดังนี้

๑.๒.๑ รายชื่อระบบคอมพิวเตอร์และระบบสารสนเทศที่ได้รับการพิจารณาคัดเลือก ดังนี้

๑. ระบบเว็บไซต์ศูนย์สนับสนุนบริการสุขภาพที่ ๑

๑.๒.๒ กำหนดรูปแบบการสำรองข้อมูลแบบสมบูรณ์ (Full Backup) ทุกเดือน

๑.๓ ผู้ดูระบบ (Administrator) ต้องพิมพ์รายละเอียดติดบนอุปกรณ์สื่อบันทึกข้อมูล ได้แก่ วัน เวลา ผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล

๑.๓.๑ การกู้คืนข้อมูลรายเดือนจากอุปกรณ์สื่อบันทึกข้อมูลข้อมูลใดๆ ที่ใช้สำหรับสำรองแบบสมบูรณ์

๒. งานเทคโนโลยีสารสนเทศดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑ เพื่อให้สมารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ดังนี้

๒.๑ กำหนดผู้มีหน้าที่รับผิดชอบระบบสารสนเทศ

๒.๒ กำหนดผู้มีหน้าที่รับผิดชอบสำรองข้อมูลสารสนเทศ

๒.๓ กำหนดผู้มีหน้าที่รับผิดชอบการจัดทำแผนดังกล่าว

๒.๔ กำหนดให้ปรับปรุงแผนดังกล่าวทุก ๑ ปี

๓. งานเทคโนโลยีสารสนเทศและการสื่อสารต้องดำเนินการทดสอบสภาพความพร้อมใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศ และระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้อย่างน้อย ปีละ ๑ ครั้ง

ทั้งนี้ แผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และแผนการสำรองข้อมูล ศูนย์สนับสนุนบริการสุขภาพที่ ๑ รวมถึงการทดสอบสภาพความพร้อมใช้งานได้นำข้อมูลไปรวมไว้ในแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑

หมวด ๘
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ทำให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนด มีความมั่นคงปลอดภัยและหน่วยงานสามารถปฏิบัติตามได้อย่างประสิทธิภาพ

นโยบาย

๑. กำหนดให้มรการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๒. การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานภาครัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระบบความเสี่ยงและระบบความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

แนวปฏิบัติ

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๒. กำหนดให้มีผู้ตรวจสอบและเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๒.๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศประจำปีงบประมาณ ให้กำเนินการโดยกลุ่มตรวจสอบภายใน (Internal Auditor)

๒.๒ หากมีความประสงค์ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศเชิงเทคนิค ให้ดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๓. กำหนดแนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๓.๑ ผู้ตรวจสอบต้องจัดทำรายงานพร้อมข้อเสนอแนะในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๒ งานเทคโนโลยีสารสนเทศและการสื่อสารต้องอำนวยความสะดวกแก่ผู้ตรวจสอบในการตรวจสอบข้อมูลที่สำคัญ

๓.๓ ในกรณีที่ผู้ตรวจสอบจำเป็นต้องเข้าถึงข้อมูลสำคัญให้งานเทคโนโลยีสารสนเทศและการสื่อสาร สร้างสำเนาสำหรับข้อมูลนั้น โดยให้ผู้ตรวจสอบใช้งานและทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือหากประสงค์จัดเก็บข้อมูลนั้นเป็นหลักฐานให้แจ้งงานเทคโนโลยีสารสนเทศและการสื่อสารทราบ

๓.๔ งานเทคโนโลยีสารสนเทศต้องจัดสรรอุปกรณ์ที่จำเป็นต้องใช้ในการตรวจสอบเชิงเทคนิค หรือดำเนินการประสานงานเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม

๓.๕ ในกรณีมีการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบประเมินความเสี่ยงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้แยกการติดตั้งเครื่องมือออกจากระบบที่ให้บริการจริง หรือระบบที่ใช้ในการพัฒนาและกำหนดให้ผู้ตรวจสอบเข้าถึงข้อมูลที่เป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว (Read Only)

๓.๖ ผู้ตรวจสอบต้องแจ้งความเสี่ยงและระบุความรุนแรงของเครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยง

๓.๗ ผู้ดูแลระบบ (Administrator) ต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ตรวจสอบเป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม