ประกาศกรมสนับสนุนบริการสุขภาพ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๘

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ประกอบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้องกับภารกิจของกรมสนับสนุนบริการสุขภาพ ในการเป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure) และการเป็นหน่วยงานหลักในการควบคุม กำกับ มาตรฐานสถานพยาบาล ด้านที่ ๙ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูง เพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ นั้น

เพื่อให้การบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบในการปรับเปลี่ยนหน่วยงานภาครัฐเป็นรัฐบาลดิจิทัลระดับกรม (Department Chief Information Officer) อย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความเชื่อถือได้และให้บริการได้อย่างต่อเนื่อง สามารถป้องกันภัยคุกคามไซเบอร์ ที่อาจก่อให้เกิดความเสียหายแก่กรมสนับสนุนบริการสุขภาพและหน่วยงานในสังกัด จึงประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกาศ ณ วันที่ ๒ สิงหาคม พ.ศ. ๒๕๖๔

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม อธิบดีกรมสนับสนุนบริการสุขภาพ จึงประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๘”

ข้อ ๒ ยกเลิก ประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔ ประกาศ ณ วันที่ ๑๘ มิถุนายน พ.ศ. ๒๕๖๔

ข้อ ๓ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๘ มีวัตถุประสงค์ ดังต่อไปนี้

๑) เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ

๒) เพื่อเผยแพร่ประกาศนโยบายและแนวปฏิบัติให้เจ้าหน้าที่ทุกระดับในสังกัดกรมสนับสนุนบริการสุขภาพ และผู้เกี่ยวข้องทั้งหมดได้รับทราบ เข้าถึง เข้าใจ และถือปฏิบัติตามนโยบายและแนวปฏิบัติอย่างเคร่งครัด

๓) เพื่อกำหนด...

๓) เพื่อกำหนดแนวปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ช่วยปฏิบัติงานให้กรมสนับสนุนบริการสุขภาพ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ โดยจะต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ข้อ ๔ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๘ มีการกำหนดประเด็นสำคัญดังต่อไปนี้

๑) การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

๒) การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล (Database Security and Backup)

๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Management)

๔) การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

๕) การดำเนินการตอบสนองต่อเหตุการณ์ด้านความมั่นคงทางด้านสารสนเทศ

๖) การสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๗) หน้าที่และความรับผิดชอบ

๘) การบริหารจัดการการใช้บริการจากหน่วยงานภายนอกด้านสารสนเทศ

ข้อ ๕ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม ต้องรายงานต่อผู้บริหารเทคโนโลยีสารสนเทศระดับกรม เพื่อสั่งการและตรวจสอบ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของกรมสนับสนุนบริการสุขภาพ เกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติ โดยนโยบายฉบับนี้กำหนดให้ผู้บริหารระดับสูงของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๖ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๘ เป็นไปตามแนบท้ายประกาศ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๕ มกราคม พ.ศ. ๒๕๖๘

(นายภานุวัฒน์ ปานเกตุ)
อธิบดีกรมสนับสนุนบริการสุขภาพ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๘

ตามประกาศกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมสนับสนุนบริการสุขภาพ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะ เกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อกรมสนับสนุนบริการสุขภาพนั้น

กรมสนับสนุนบริการสุขภาพ จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

ข้อ ๑ คำนิยาม

"หน่วยงาน" หมายถึง กรมสนับสนุนบริการสุขภาพ รวมถึงหน่วยงานภายในที่อยู่ภายใต้สังกัดของกรมสนับสนุนบริการสุขภาพ

"ผู้ใช้งาน" หมายถึง ข้าราชการ ลูกจ้าง และพนักงานราชการ ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

"ผู้บริหาร" หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ ผู้อำนวยการสำนัก/กอง/ศูนย์ เป็นต้น

"ผู้บริหารระดับสูงสุด" หมายถึง อธิบดี ของหน่วยงาน

"ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม" (Department Chief Information Officer: DCIO) หมายถึง รองอธิบดี หรือผู้ซึ่งได้รับมอบหมายให้รับผิดชอบงานด้านเทคโนโลยีสารสนเทศของหน่วยงาน

"ผู้ดูแลระบบ" (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

"เจ้าของข้อมูล" หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

"สิทธิของผู้ใช้งาน" หมายถึง สิทธิทั่วไป สิทธิจำเพาะ และสิทธิอื่นใดที่เกี่ยวข้อง กับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์

"สินทรัพย์" หมายถึง ข้อมูล ระบบข้อมูล ระบบเครือข่าย และทรัพย์สินด้านเทคโนโลยี สารสนเทศและการสื่อสาร ของหน่วยงานถือครอง

"ระบบเครือข่าย" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการรับ ส่งข้อมูลและ สารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ ได้แก่ ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN)

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิ หรือ การมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ ทางดิจิทัลและทางกายภาพตามหน้าที่ที่ได้รับมอบหมาย

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือของสารสนเทศ ของหน่วยงาน

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด”หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

หมวดที่ ๑
การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อให้บุคลากรกรมสนับสนุนบริการสุขภาพ และบุคคลภายนอก ให้มีความรู้ ความเข้าใจและสามารถปฏิบัติตามแนวทางปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control) พร้อมทั้งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ

นโยบาย

บุคลากรกรมสนับสนุนบริการสุขภาพ และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุน การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสินทรัพย์ทางสารสนเทศ (Asset Access Control) ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ให้เป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ และต้องสอดคล้องกับการกำหนดสิทธิ์ การเข้าถึงตามบทบาทหน้าที่ของบุคลากร (Role-Based Access Control - RBAC) ดังนี้

(๑) ผู้ใช้ทั่วไป (General User)

(๒) ผู้ดูแลระบบ (System Administrator)

(๓) ผู้ดูแลความปลอดภัยสารสนเทศ (Information Security Officer)

๑.๒ ผู้ดูแลระบบมีหน้าที่ในการอนุมัติสิทธิ ในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน

๑.๓ ผู้ดูแลระบบมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งานสำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๔ ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

๑.๕ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ ต้องแจ้งเหตุผลความจำเป็น ขอบเขตการเข้าถึง และระยะเวลาที่ชัดเจน เพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจ จากผู้ดูแลระบบ และต้องรักษาความลับทางราชการ หากในกรณีที่เกิดความเสียหายต่อระบบบุคคลภายนอกต้องรับผิดชอบทุกกรณี

๑.๖ ใช้ระบบยืนยันตัวตนที่ปลอดภัย (ถ้ามี) เช่น การยืนยันตัวตนสองขั้นตอน (Two-Factor Authentication - ๒FA) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๗ กำหนดรหัสผ่านที่มีความซับซ้อน เช่น มีความยาวขั้นต่ำ ๘ ตัวอักษร และประกอบด้วยตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และสัญลักษณ์พิเศษ ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๘ การควบคุมการเข้าถึงจากภายนอก (Remote Access) ให้ใช้การเชื่อมต่อผ่าน VPN หรือระบบที่มีการเข้ารหัสข้อมูลเพื่อความปลอดภัย เท่านั้น

๑.๙ กำหนดเงื่อนไขในการเข้าถึง โดย จัดอุปกรณ์ที่สามารถเข้าถึงและเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศ

๒. การบริหารจัดการเข้าถึงของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งานที่ได้รับอนุญาตแล้วและสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการควบคุม จำกัด และเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้

๑.๑ ผู้ดูแลระบบสารสนเทศของหน่วยงานต้องกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สามารถนำข้อมูลไปตรวจสอบได้ ประกอบด้วย ชื่อ นามสกุล ตำแหน่ง สังกัด และหมายเลขโทรศัพท์ เป็นต้น

๑.๒ การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

๑.๒.๑ กรณีบุคลากรภายใน

(๑) ให้บุคลากรกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศและส่งแบบฟอร์มให้กับผู้ดูแลระบบ

(๒) ผู้ดูแลระบบนำส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับเจ้าของระบบ

(๓) ให้เจ้าของระบบพิจารณาและอนุมัติสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๒.๒ กรณีบุคคลภายนอก

(๑) ให้บุคคลภายนอกกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมระบุเหตุผลในการเข้าใช้งาน หรือหนังสือขอเข้าใช้งานจากบริษัทหรือหน่วยงานต้นสังกัด

(๒) ให้หน่วยงานพิจารณาเหตุผล และดำเนินการส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้เจ้าของระบบที่ขอใช้งาน

(๓) ให้เจ้าของระบบพิจารณาและอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่าน (Password) ให้ดำเนินการ ตามหลักเกณฑ์ดังนี้

๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้เจ้าของระบบ กำหนด เช่น ชื่อภาษาอังกฤษ หรือบัตรประจำตัวประชาชน ตามด้วยอักษรนามสกุลตัวแรก หรือลักษณะอื่นใดตามที่เจ้าของระบบ ที่มีการตกลงร่วมกัน

๑.๓.๒ การกำหนดรหัสผ่าน (Password) ประกอบไปด้วย ชุดของตัวอักษรภาษาอังกฤษ ตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และอักขระพิเศษ รวมอย่างน้อย ๘ ตัวขึ้นไป และยากต่อการคาดเดา

๑.๓.๓ การกำหนดบัญชีผู้ใช้งานครั้งแรกให้ผู้ดูแลระบบ แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ผู้ใช้งาน ทราบโดยตรง

๑.๓.๔ เมื่อผู้ใช้งานมีการเปลี่ยนแปลงข้อมูลให้หน่วยงานทำการแจ้งเจ้าของระบบ เพื่อปรับปรุงข้อมูลให้เป็นปัจจุบัน

๒. การยกเลิกสิทธิการใช้งานของบุคลากรหรือบุคคลภายนอกและผู้ดูแลระบบให้ดำเนินการ ดังนี้

๒.๑ ให้หน่วยงานแจ้งเจ้าของระบบ เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก โอนย้าย หรือสิ้นสุดการจ้าง

๒.๑.๑ กรณีบุคลากรหรือบุคคลภายนอก ให้ผู้ดูแลระบบดำเนินการปิดบัญชีผู้ใช้งาน (Account) และแจ้งกลับไปยังหน่วยงานรับทราบ ภายใน ๑๕ วัน

๒.๑.๒ กรณีผู้ดูแลระบบหน่วยงานภายใน ให้ผู้ดูแลระบบระดับกรม ดำเนินการยกเลิกสิทธิการใช้งานของทุกระบบงาน ทั้งนี้ให้ดำเนินการแจ้งหน่วยงานต้นสังกัดหรือเจ้าของระบบรับทราบการยกเลิกสิทธิการใช้งาน ภายใน ๗ วัน

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้ใช้งาน ให้ดำเนินการ ดังนี้

๓.๑ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้หน่วยงานแจ้ง เจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๓.๒ ในกรณีที่ผู้ใช้งาน ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สูงกว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อเจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการตามหลักเกณฑ์ดังนี้

๔.๑ ในกรณีผู้ใช้งานลืมรหัสผ่าน (Password) ให้แจ้งหน่วยงานที่รับผิดชอบ โดยใช้วิธีการของระบบตามที่เจ้าของระบบได้กำหนดไว้

๔.๒ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๓ - ๖ เดือน หรือตามความเสี่ยงของระบบโปรแกรม และรหัสผ่าน (Password) ใหม่ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม และมีความสอดคล้องตามข้อ ๑.๓.๒

๕. ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสุดสิ้นการจ้าง เพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัย ตามที่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้

๓. การควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ (Computer Network Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึง

๒. กำหนดแนวปฏิบัติในการยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาต ให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถใช้งานเครือข่าย ระบบคอมพิวเตอร์และระบบสารสนเทศของหน่วยงานได้

๓. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดยต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๔. กำหนดแนวปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) โดยต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕. กำหนดแนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

๖. กำหนดแนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศและการส่งข้อมูลสารสนเทศสอดคล้องกับแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

๑. การเข้าถึงเครือข่ายของผู้ใช้งาน

๑.๑ การใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet) ให้ดำเนินการ ดังนี้

๑.๑.๑ ผู้ใช้งานสามารถเข้าบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองที่ได้รับอนุญาตจากหน่วยงาน เพื่อเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet)

๑.๑.๒ ควรควบคุมการใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) สูง และที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ เช่น รายการบันเทิงต่าง ๆ ในเวลาราชการ เป็นต้น

๑.๑.๓ ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดศีลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์เสื่อมเสีย เป็นต้น

๑.๑.๔ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของหน่วยงาน เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๕ ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเคร่งครัด

๑.๑.๖ ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่าง ๆ เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ โดยแจ้งให้ผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัดทราบก่อนติดตั้งใช้งาน

๑.๒ การใช้งานโดเมนเนม (Domain Name) ของหน่วยงานให้ดำเนินการ ดังนี้

๑.๒.๑ หน่วยงานภายในกรมสนับสนุนบริการสุขภาพ ต้องจดทะเบียนโดเมนเนม (Domain Name) เว็บไซต์หรือระบบ ที่อยู่ภายใต้ hss.moph.go.th เท่านั้น เพื่อความมั่นคงปลอดภัยด้านสารสนเทศ และความน่าเชื่อถือในการเข้าถึงของผู้รับบริการ

๑.๒.๒ ห้ามนำโดเมนเนม (Domain Name) ในทางที่ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศีลธรรม

๑.๒.๓ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจด้วยการใช้โดเมนเนม (Domain Name) ของหน่วยงาน

๑.๓ การใช้งานเครือข่าย Local Area Network (LAN) ให้ดำเนินการ ดังนี้

๑.๓.๑ ผู้ดูแลระบบต้องทำการตั้งค่า (Configuration) เลขที่อยู่ไอพี (IP Address) เมื่อมีการนำอุปกรณ์มาใช้ภายในหน่วยงาน

๑.๓.๒ ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายภายในกรมสนับสนุนบริการสุขภาพ

๑.๔ การใช้งานเครือข่ายไร้สาย (WiFi) ให้ดำเนินการ ดังนี้

๑.๔.๑ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดจากผู้ผลิตทันทีเมื่อนำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้งเพื่อใช้งาน

๑.๔.๒ ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (WiFi) ภายในกรมสนับสนุนบริการสุขภาพ

๑.๔.๓ ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็นทรัพย์สินของหน่วยงานไปใช้งานเครือข่ายไร้สาย (WiFi) ที่ไม่น่าเชื่อถือ

๑.๔.๔ ผู้ใช้งานควรระมัดระวังในการทำธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ระหว่างการใช้งานเครือข่ายไร้สาย (WiFi) เนื่องจากอาจเกิดความไม่ปลอดภัยและอาจขาดการเชื่อมต่อของสัญญาณ

๑.๔.๕ ห้ามผู้ใช้งานติดตั้งและเปิดการทำงานโปรแกรมดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สาย (WiFi) ของหน่วยงานและมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๕ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

๑.๕.๑ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ภายใต้หน่วยงาน ควรนำเสนอเกี่ยวกับภารกิจงานของหน่วยงาน เช่น ผลการดำเนินงาน และข่าวสาร โดยการนำเข้าข้อมูลต้องเป็นผู้ที่ได้รับมอบหมายจากหน่วยงาน และต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๕.๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของหน่วยงานผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๕.๓ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงต่อไป

๑.๕.๔ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากหน่วยงาน และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑.๕.๕ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งานต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที ทั้งนี้ให้แจ้งผู้บังคับบัญชารับทราบ

๒. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ให้ดำเนินการ ดังนี้

๒.๑ ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องจัดทำผังระบบเครือข่าย (Network Diagram) พร้อมรายละเอียดอุปกรณ์บนเครือข่ายที่เห็นว่าจำเป็นต่อการใช้งาน ได้แก่ กลุ่มอุปกรณ์ เลขที่อยู่ไอพี (IP Address) และหมายเลขเฉพาะอุปกรณ์ (MAC Address) โดยให้ปรับปรุงทุก ๑ ปี หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อระบบสารสนเทศ

๒.๒ การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ มาใช้งานบนเครือข่ายต้องได้รับอนุญาตจากผู้รับผิดชอบด้านสารสนเทศของหน่วยงาน เช่น แท็ปเลต โทรศัพท์มือถือ เป็นต้น

๓. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) ให้ดำเนินการ ดังนี้

๓.๑ หน่วยงานที่ดูแลด้านสารสนเทศต้องดูแลตรวจสอบพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) รวมทั้งการควบคุมการเข้าถึงพอร์ตทางกายภาพและเครือข่าย

๓.๒ หน่วยงานที่ดูแลด้านสารสนเทศต้องเปิดใช้งานเฉพาะพอร์ตที่จำเป็นสำหรับการใช้งานเท่านั้น และต้องตรวจสอบพอร์ตที่เปิดให้บริการ อย่างน้อยทุก ๆ ๓ - ๖ เดือน หรือตามความเหมาะสม

๔. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้ดำเนินการ ดังนี้

๔.๑ หน่วยงานที่ดูแลด้านสารสนเทศควรมีระบบป้องกันการบุกรุกโจมตีทางเครือข่าย Firewall เพื่อใช้เป็นจุดควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๔.๒ ผู้ดูแลระบบต้องไม่เปิดเผยข้อมูลการเชื่อมต่อทางเครือข่าย ก่อนได้รับอนุญาตจากหน่วยงานที่ดูแลด้านสารสนเทศ

๔.๓ ผู้ดูแลระบบมีหน้าที่ในการควบคุมการเชื่อมต่อสัญญาณหรือยกเลิก การเชื่อมต่อสัญญาณตามที่ได้รับอนุญาตจากหน่วยงานที่ดูแลด้านสารสนเทศ ทั้งนี้หากพบข้อผิดพลาดหรือเห็นว่า หมดความจำเป็นในการเชื่อมต่อสัญญาณให้รายงานหน่วยงานที่ดูแลด้านสารสนเทศทันที

๔.๔ การเชื่อมต่อเครือข่ายสารสนเทศกับหน่วยงานภายนอกหรือเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ของผู้ให้บริการที่มีความน่าเชื่อถือ ต้องได้รับอนุญาตจากผู้บังคับบัญชาของหน่วยงาน

๕. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ให้ดำเนินการ ดังนี้

๕.๑ ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ และการรับ – ส่งหรือการไหลเวียนของข้อมูลหรือสารสนเทศเป็นไปอย่างรวดเร็ว

๕.๒ ผู้ดูแลระบบต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ใช้งานเป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกัน การเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการโดยต้องมีการควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวตนที่ปลอดภัย

๒. กำหนดแนวปฏิบัติใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการ ความมั่นคงปลอดภัยที่ได้กำหนดไว้

แนวปฏิบัติ

๑. การกำหนดขั้นตอนการปฏิบัติงาน ดังนี้

๑.๑ ผู้ใช้งานไม่มีสิทธิ์เปลี่ยนแปลงแก้ไขค่าต่าง ๆ ของระบบปฏิบัติการ เช่น Product Key หรือ License ของระบบปฏิบัติการ และค่าคอนฟิกกูเรชั่น (Configuration) ต่าง ๆ เช่น Computer Name, IP Address เป็นต้น

๑.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๑.๓ หลังจากผู้ดูแลระบบติดตั้งระบบปฏิบัติการเสร็จ ผู้ใช้งานต้องบริหารจัดการรหัสผ่านหรือเปลี่ยนรหัสผ่านที่กำหนดไว้ตั้งแต่ต้นโดยทันที

๑.๔ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งานเป็นเวลา ๑๕ นาที หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๑.๕ ก่อนการเข้าใช้ระบบปฏิบัติการผู้ใช้งานจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

๑.๖ ห้ามให้ผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม บนระบบปฏิบัติและเว็บไซต์แสดงข้อมูลของหน่วยงาน

๑.๗ ห้ามผู้ใช้งานของหน่วยงานเข้าควบคุมระบบปฏิบัติการคอมพิวเตอร์หรือระบบสารสนเทศจากภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๑.๘ ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer โปรแกรมประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรมประเภท Formatter หรือโปรแกรมที่มีความเสี่ยง เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

๑.๙ ซอฟต์แวร์ที่หน่วยงาน ใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

๑.๑๐ ซอฟต์แวร์ที่หน่วยงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๑.๑๑ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข เพื่อประโยชน์ทางการค้า

๒.การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมสำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญให้ดำเนินการ ดังนี้

๒.๑ การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับการอนุมัติจากผู้ดูแลระบบ เพื่อจำกัดและควบคุมการใช้งาน

๒.๒ โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

๒.๓ ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

๕. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control) โดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศของผู้ใช้งาน

๒. กำหนดแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน โดยต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่ปฏิบัติงานจากภายนอกหน่วยงาน

๓. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสม เพื่อปกป้องระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศจากความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๔. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกหน่วยงาน โดยต้องกำหนดข้อปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกหน่วยงาน

๕. กำหนดแนวปฏิบัติการประชุมออนไลน์ผ่านแพลตฟอร์มต่าง ๆ

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งานที่เข้าถึงระบบคอมพิวเตอร์ และ ระบบสารสนเทศผ่านเครือข่ายภายนอก ให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN)

๑.๒ การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) รายละเอียดปรากฏตามภาคผนวก

๒. ระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพให้ดำเนินการ ดังนี้

๒.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ดังนี้

๒.๑.๑ ระบบการบริหารจัดการความมั่นคงปลอดภัยและเครือข่าย ได้แก่ ระบบ Antivirus, ระบบ Backup System, 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 และมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพ ต้องได้รับการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกออกจากระบบอื่น ๆ

๒.๓ ผู้ดูแลระบบต้องแบ่งพื้นที่สำหรับการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายตามระดับความสำคัญและความปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพ เพื่อควบคุมสภาพแวดล้อมโดยเฉพาะ

๒.๔ การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking) เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องเข้าถึงในสถานที่ที่มีความปลอดภัยและต้องได้รับอนุญาตจากกลุ่มเทคโนโลยีสารสนเทศ

๓. การควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ให้ดำเนินการ ดังนี้

๓.๑ อุปกรณ์สื่อสารเคลื่อนที่ ได้แก่ Smart Phone และ Tablet ต้องได้รับการยืนยันตัวตัน โดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของผู้ใช้งานสำหรับการเข้าใช้งาน

๔. การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) กำหนด ดังนี้

๔.๑ ผู้ใช้งานต้องปฏิบัติตามหมวด ๑ แนวปฏิบัติ ข้อ ๑ การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

๔.๒ เมื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศแล้ว ผู้ใช้งานต้องระมัดระวังไม่ให้ผู้ไม่มีส่วนเกี่ยวข้องเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ สื่อสารเคลื่อนที่ได้

หมวดที่ ๒
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล (Database Security and Backup)

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศและการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมฉุกเฉิน และการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่องแม่ในสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่าง ๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสมและสามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง

นโยบาย

๑. พิจารณาคัดเลือกระบบสารสนเทศที่เหมาะสมในการจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน

๒. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ เพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

๑. ผู้ดูแลระบบจะต้องจัดทำการสำรองของระบบสารสนเทศโดยมีขั้นตอน ดังนี้

๑.๑ ผู้ดูแลระบบจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูล และการกู้คืนข้อมูลสารสนเทศ

๑.๒ กำหนดรูปการสำรองข้อมูลระบบสารสนเทศ ดังนี้

๑.๒.๑ คัดเลือกระบบสารสนเทศในการสำรองข้อมูล

๑.๒.๒ กำหนดรูปแบบการสำรองข้อมูล เช่น เฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) แบบสมบูรณ์ (Full Backup)

๑.๒.๓ กำหนดความถี่ในการสำรองข้อมูลตามความเหมาะสมของระบบสารสนเทศ

๑.๓ ผู้ดูแลระบบดำเนินการสำรองของระบบสารสนเทศ ตามข้อที่ ๑.๒

๒. ผู้ดูแลระบบต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศที่สำรองไว้ อย่างน้อยร้อยละ ๕๐ ของระบบที่มีอยู่ โดยอย่างน้อย ๖ เดือน/ครั้ง

๓. กลุ่มเทคโนโลยีสารสนเทศดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่องโดยกำหนดให้ปรับปรุงแผนดังกล่าวทุก ๑ ปี

๔. มีการทบทวนระบบสารสนเทศในการระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๕. เจ้าของระบบต้องดำเนินการกำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูลที่ได้รับมอบหมายให้ดูแล

๕.๑ จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๕.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

๕.๒.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

๕.๒.๒ กำหนดเกณฑ์การระงับสิทธิ การมอบอานาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๕.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๕.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

๕.๓.๑ จัดแบ่งประเภทของข้อมูล โดยแบ่งออกเป็น

(๑) ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

(๒) ข้อมูลสารสนเทศด้านที่ให้บริการตามภารกิจ เช่น ข้อมูลผู้รับบริการ ข้อมูลสถานพยาบาล ข้อมูลอาสาสมัครสาธารณสุขประจำหมู่บ้าน (อสม.) เป็นต้น

๕.๓.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

(๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(๒) ข้อมูลที่มีระดับความสำคัญปานกลาง

(๓) ข้อมูลที่มีระดับความสำคัญน้อย

๕.๓.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

(๑) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

(๒) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

(๓) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

(๔) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๕.๓.๔ จัดแบ่งระดับชั้นการเข้าถึง

(๑) ระดับชั้นสำหรับผู้บริหาร

(๒) ระดับชั้นสำหรับผู้ใช้งานทั่วไป

(๓) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๕.๓.๕ การกำหนดระยะเวลาในการเข้าถึงและกำหนดจำนวนช่องทางที่สามารถเข้าถึง

๖. ข้อมูล ข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิเข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

๗. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวดที่ ๑

๘. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิและอานาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีระบบแฟ้มลงบันทึกเข้าออกระบบฐานข้อมูล (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

๙. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงานภายนอก ดังต่อไปนี้

๙.๑ กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

๙.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกัน หรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

๙.๓ กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

๙.๔ กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธความรับผิดชอบ

๙.๕ กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

๙.๖ กำหนดสิทธิ์การเข้าถึงข้อมูลตามความจำเป็น (Least Privilege)

๙.๗ กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๙.๘ กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส (Encryption key) เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล

๑. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

๒. ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

๓. ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๔. ต้องกำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

๔.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๔.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

๔.๓ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรองสำเร็จ/ไม่สำเร็จ เป็นต้น

๔.๔ ตรวจสอบการตั้งค่าต่าง ๆ (Configuration) ของระบบการสำรองข้อมูล

๔.๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๔.๖ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

๔.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๔.๘ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๔.๙ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๔.๑๐ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

๔.๑๑ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๕. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

๕.๑ มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๕.๒ มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๕.๓ มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๕.๔ มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๕.๕ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๕.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๖. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้งรวมถึงต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๗. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้นเพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

๘. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Management)

วัตถุประสงค์

เพื่อให้มีการประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ และเพื่อตรวจสอบแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ทำให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนด มีความมั่นคงปลอดภัยและหน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

นโยบาย

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

แนวปฏิบัติ

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒. กำหนดให้มีผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๒.๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศประจำปีงบประมาณ ให้ดำเนินการโดยกลุ่มตรวจสอบภายใน (Internal Auditor)

๒.๒ หากมีความประสงค์ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศเชิงเทคนิค ให้ดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๓. กำหนดแนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๓.๑ ผู้ตรวจสอบต้องจัดการทำรายงานพร้อมข้อเสนอแนะในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๒ กลุ่มเทคโนโลยีสารสนเทศต้องอำนวยความสะดวกแก่ผู้ตรวจสอบในการตรวจสอบข้อมูลที่สำคัญ

๓.๓ ในกรณีที่ผู้ตรวจสอบจำเป็นต้องเข้าถึงข้อมูลสำคัญให้กลุ่มเทคโนโลยีสารสนเทศ สร้างสำเนาสำหรับข้อมูลนั้น โดยให้ผู้ตรวจสอบใช้งานและทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือหากประสงค์จัดเก็บข้อมูลนั้นเป็นหลักฐานให้แจ้งกลุ่มเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๓.๔ ในกรณีการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบประเมินความเสี่ยงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้แยกการติดตั้งเครื่องมือออกจากระบบที่ให้บริการจริง หรือระบบที่ใช้ในการพัฒนาและกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว (Read Only)

๓.๕ ผู้ตรวจสอบต้องแจ้งความเสี่ยงและระบุความรุนแรงของเครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยง

หมวดที่ ๔
การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศข้อมูลซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

นโยบาย

กำหนดขอบเขตการเข้าถึงห้องปฏิบัติการคอมพิวเตอร์ รวมถึงพื้นที่ในการบริหารจัดการระบบเครือข่ายทางด้านกายภาพ สถานที่และสภาพแวดล้อม ของกรมสนับสนุนบริการสุขภาพ

แนวปฏิบัติ

๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง สถานที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

๒. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

๒.๑ กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

๒.๒ ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก

๒.๓ จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

๒.๔ จะต้องปิดล็อกห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่หรือเมื่อไม่ได้ใช้งานแล้ว

๒.๕ ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

๒.๖ จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๓.๑ มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยสารสนเทศ จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๔. การควบคุมการเข้าออก อาคารสถานที่

๔.๑ กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๔.๒ การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor) โดยผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๔.๓ ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

๔.๔ บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรพนักงานให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๔.๕ จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center)เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๔.๖ ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๔.๗ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๔.๘ สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๔.๙ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๔.๑๐ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาตจากผู้ที่มีส่วนเกี่ยวข้อง

๔.๑๑ มีการพิสูจน์ตัวตน เช่น การใช้บัตรแตะ การใช้รหัสผ่าน การสแกนนิ้ว เป็นต้น เพื่อควบคุมการเข้า-ออก ในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

๔.๑๒ จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๔.๑๓ จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๕.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และระบบควบคุมความชื้น

๕.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๕.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้อง Data Center ทำงานผิดปกติหรือหยุดการทำงาน

๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ (Cabling Security)

๖.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๖.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๖.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซง รบกวนของสัญญาณซึ่งกันและกัน

๖.๔ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๖.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๖.๖ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๗.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิตหรือผู้จัดจำหน่าย

๗.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๗.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๗.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๗.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๗.๖ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่เป็นผู้ให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๘.๑ ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๘.๒ กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๘.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๘.๔ เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๘.๕ บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises)

๙.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การเกิดอุบัติเหตุกับอุปกรณ์ เป็นต้น

๙.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้ในที่สาธารณะ

๙.๓ เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment)

๑๐.๑ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๑๐.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่ ๕
การดำเนินการตอบสนองต่อเหตุการณ์ด้านความมั่นคงทางด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการตอบสนองและรับมือต่อเหตุการณ์ด้านความมั่นคงทางด้านสารสนเทศ เพื่อให้ระบบที่ให้บริการตามภารกิจของกรมสนับสนุนบริการสุขภาพ มีความมั่นคงปลอดภัยทางด้านสารสนเทศ

นโยบาย

กำหนดแนวทางในการรับมือ และตอบสนองต่อเหตุการณ์ด้านความมั่นคงทางด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ และแนวทางการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศต่อผู้หน่วยงานที่มีส่วนเกี่ยวข้อง ให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

แนวปฏิบัติ

๑. ระบบป้องกันผู้บุกรุก

๑.๑ ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลข IP Address ของเครือข่ายที่เป็นผู้โจมตี

๑.๒ ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๔ ครั้งหรือต่อเมื่อมีเหตุการณ์ที่เกี่ยวข้องทางด้านความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน

๑.๓ ดำเนินการตรวจสอบบันทึกของ Log File จากรายงานจากระบบ SIEM ของกรมสนับสนุนบริการสุขภาพและรายงานจาก Firewall สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Dashboard แสดงข้อมูล Incident report และ การรวบรวม Log แบบศูนย์กลาง
- Packet ที่ Firewall ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลข IP Address ของเครือข่ายใดถูก Block เป็นจำนวนมาก

๒. ระบบป้องกันภัยคุกคามในการใช้งานอินเทอร์เน็ต

๒.๑ ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในกรมสนับสนุนบริการสุขภาพไปยังหน่วยงานภายนอกหรือไม่

๒.๒ ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของกรมสนับสนุนบริการสุขภาพ

๒.๓ ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไป ภายนอกต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

หมวดที่ ๖
การสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. เพื่อเสริมสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของ กรมสนับสนุนบริการสุขภาพ
๒. เพื่อให้การใช้งานระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ เป็นไปอย่างมีความมั่นคงปลอดภัย
๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

นโยบาย

กำหนดแนวทางปฏิบัติ เนื้อหา หลักสูตร ในการส่งเสริมความตระหนักด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้แก่เจ้าหน้าที่ กรมสนับสนุนบริการสุขภาพ

แนวปฏิบัติ

๑. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง
๒. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรม โดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน
๓. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้
๔. ประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ
๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน
๖. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร
๗. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

๘. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของกระทรวงสาธารณสุข และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ ๗
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

๑. เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ

๒. เพื่อสนับสนุนให้การดำเนินงานด้านสารสนเทศขององค์กรเป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับพันธกิจและเป้าหมายของกรมสนับสนุนบริการสุขภาพ

๓. เพื่อให้บุคลากรทุกระดับมีความตระหนักถึงบทบาทของตนเองและปฏิบัติงานตามมาตรฐานที่กำหนด

แนวปฏิบัติ

๑. ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้บริหารระดับสูงสุด (Chief Executive Office : CEO) ของหน่วยงาน
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Department Chief Information Officer: DCIO)

(๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ระดับบริหาร ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการกอง กลุ่ม ศูนย์ หัวหน้ากลุ่ม หรือเทียบเท่าหัวหน้ากลุ่ม

(๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผนติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

๓. ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการ กรมสนับสนุนบริการสุขภาพ เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่ที่ปฏิบัติหน้าที่ด้านเทคโนโลยีสารสนเทศ เป็นต้น

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(๓) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(๔) ดำเนินการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่หน่วยงานกำหนด

(๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๖) รับผิดชอบในการรักษาความปลอดภัย ระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ

(๗) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ

หมวดที่ ๘
การบริหารจัดการการใช้บริการจากหน่วยงานภายนอกด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อกำหนดแนวทางที่ชัดเจนในการบริหารจัดการการใช้บริการด้านสารสนเทศจากหน่วยงานภายนอก

๒. เพื่อสนับสนุนให้การใช้บริการจากหน่วยงานภายนอกเกิดประสิทธิภาพสูงสุด สอดคล้องกับเป้าหมายและนโยบายของกรมสนับสนุนบริการสุขภาพ

๓. เพื่อให้มั่นใจว่าการใช้บริการจากหน่วยงานภายนอกปฏิบัติตามข้อกำหนดทางกฎหมายและมาตรฐานที่เกี่ยวข้อง

แนวปฏิบัติ

๑. ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูลและระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

๒. การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของหน่วยงานจากหน่วยงานภายนอกต้องมีการขออนุญาตอย่างเป็นทางการ และได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

๓. การบริการ และการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตาม นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่าง ๆ ของกรมสนับสนุนบริการสุขภาพ

๔. ผู้ดูแลระบบต้องให้สิทธิ์การเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น และกำหนดระยะเวลาการเข้าถึงและการยกเลิกสิทธิ์อย่างชัดเจน

๕. ต้องมีการทำสัญญาการรักษาความลับขององค์กร ระหว่างกรมสนับสนุนบริการสุขภาพและหน่วยงานภายนอกที่เข้ามาปฏิบัติงานก่อนเปิดให้ใช้บริการระบบเสมอ

๖. ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน และวิธีการดำเนินงาน เป็นอย่างน้อยเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการให้เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และเป็นไปตามขอบเขตที่ได้กำหนดไว้

๗. สัญญาระหว่างหน่วยงาน และ หน่วยงานภายนอก ในการให้บริการต้องระบุถึงหัวข้อต่าง ๆ ดังต่อไปนี้ เป็นอย่างน้อย

๗.๑ รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ

๗.๒ ระดับการให้บริการ (Service Level)

๗.๓ หน้าที่และความรับผิดชอบของกรมสนับสนุนบริการสุขภาพและหน่วยงานภายนอก ในการให้บริการในครั้งนี้

๗.๔ ระยะเวลาในการให้บริการ และการตรวจรับงานบริการในครั้งนี้

๗.๕ ราคา และเงื่อนไขการชำระเงิน

๗.๖ ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อหรือพัฒนาขึ้น (ถ้ามี)

๗.๗ การรักษาความลับของข้อมูลที่ได้รับจากการให้บริการแก่กรมสนับสนุนบริการสุขภาพ