บันทึกข้อความ

ส่วนราชการ งานนโยบาย กิจกรรมพิเศษและเทคโนโลยีสารสนเทศ กองแบบแผน โทร ๑๘๓๐๘

ที่ สธ ๐๗๐๓.๐๑๘/๒๕ **วันที่** ๑๒ มีนาคม ๒๕๖๙

เรื่อง แนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

เรียน ผู้อำนวยการกองแบบแผน

ตามที่กรมสนับสนุนบริการสุขภาพ ได้ประกาศนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ พ.ศ. ๒๕๖๙ เพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้องกับภารกิจของกรมสนับสนุนบริการสุขภาพ นั้น

ในการนี้ เพื่อให้การบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศสอดคล้องกับบทบาทหน้าที่ความรับผิดชอบในการปรับเปลี่ยนหน่วยงานภาครัฐเป็นรัฐบาลดิจิทัล ที่สอดคล้องกับกรมสนับสนุนบริการสุขภาพ อย่างมีประสิทธิภาพมีความมั่นคงปลอดภัย มีความเชื่อถือได้ และให้บริการได้อย่างต่อเนื่องสามารถป้องกันภัยคุกคามไซเบอร์ กองแบบแผนจึงขอประกาศแนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ดังรายละเอียดเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ หากเห็นชอบ โปรดลงนามประกาศแนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ต่อไปด้วยจะเป็นพระคุณ

(นายอนิวัฒน์ อารีย์กิจ)
นักวิเคราะห์นโยบายและแผนชำนาญการ
หัวหน้างานนโยบาย กิจกรรมพิเศษและเทคโนโลยีสารสนเทศ

(นายอับดุลกอเดส อมรึก)
ผู้อำนวยการกองแบบแผน

ประกาศ กองแบบแผน กรมสนับสนุนบริการสุขภาพ
เรื่อง แนวปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ตามประกาศนโยบายกรมสนับสนุนบริการสุขภาพ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ เพื่อให้ระบบเทคโนโลยีสารสนเทศของกองแบบแผน เป็นไปอย่างเหมาะสม มีประสิทธิ์ภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นในการใช้เทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจัดการภัยคุกคามต่างๆ ซึ่งอาจเกิดความเสียหายต่อกองแบบแผน นั้น

กองแบบแผน จึงกำหนดแนวปฏิบัติในการใช้งานระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

ข้อ ๑ คำนิยาม

"หน่วยงาน" หมายถึง กองแบบแผน กรมสนับสนุนบริการสุขภาพ

"ผู้ใช้งาน" หมายถึง ข้าราชการ ลูกจ้าง และพนักงานราชการ และพนักงานจ้างเหมาบริการ รวมถึงหน่วยงานที่ใช้งานระบบสารสนเทศของกองแบบแผน

"ผู้บริหาร" หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน

"ผู้บริหารสูงสุด" หมายถึง ผู้อำนวยการกองแบบแผน

"ผู้ดูแลระบบ" (System Administrator) หมายถึง ผู้ได้รับมอบหมายจากหัวหน้าหน่วยงานให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

"เจ้าของข้อมูล" หมายถึง บุคลากรกองแบบแผน

"สิทธิ์ผู้ใช้งาน" หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ และสิทธิ์อื่นใดที่เกี่ยวข้อง กับระบบสารสนเทศของกองแบบแผน โดยกองแบบแผนจะเป็นผู้พิจารณาสิทธิ์ในการใช้งาน

"สินทรัพย์" หมายถึง ข้อมูล ระบบข้อมูล ระบบเครือข่าย และทรัพย์สินด้านเทคโนโลยีสารสนเทศ ของกองแบบแผน

"ระบบเครือข่าย" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการรับ ส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของกองแบบแผน ได้แก่ระบบเครือข่ายมีสาย (LAN) และระบบเครือข่ายไร้สาย (Wireless LAN)

"การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือ การมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ ทางดิจิทัลและทางกายภาพตามที่ได้รับมอบหมาย

"ความมั่นคงปลอดภัยด้านสารสนเทศ" การธำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติ อื่นๆ ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือของสารสนเทศ กองแบบแผน

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายถึง กรณีที่ระบุเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์ที่ไม่อาจรู้ได้ว่าเกี่ยวกับความมั่นคงปลอดภัย

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

หมวดที่ ๑
การเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อให้บุคลากรกองแบบแผน และบุคคลภายนอก ให้มีความรู้ ความเข้าใจและสามารถปฏิบัติตามแนวปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control) พร้อมทั้งตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ

นโยบาย

บุคลากรกองแบบแผน กรมสนับสนุนบริการสุขภาพ และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและการควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

แนวปฏิบัติ

๑.การควบคุมสินทรัพย์ทางสารสนเทศ (Asset Access Control) ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๑.๑ การเข้าถึงและการควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ให้เป็นไปตามคำสั่งที่มอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ และต้องสอดคล้องกับการกำหนดสิทธิ์ การเข้าถึงตามบทบาทหน้าที่ของบุคลากร (Role-Base Access Control-RBAC) ดังนี้

(๑) ผู้ใช้งานทั่วไป (General User)

(๒) ผู้ดูและระบบ (System Administrator)

(๓) ผู้ดูแลความปลอดภัยสาสนเทศ (Information Security Officer)

๑.๒ ผู้ดูและระบบมีหน้าที่ในการอนุมัติสิทธิ์ ในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน

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

๑.๔ ผู้ใช้งานคอมพิวเตอร์สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิ์ที่ได้รับเท่านั้น

๑.๕ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ ต้องแจ้งเหตุผลความจำเป็น ขอบเขตการเข้าถึง และระยะเวลาที่ชัดเจน เพื่อขออนุมัติสำหรับการปฏิบัติตามภารกิจจากผู้ดูแลระบบ และต้องรักษาความลับทางราชการ หากมีความเสียหายต่อระบบบุคคลภายนอกต้องรับผิดชอบทุกกรณี

๑.๖ กำหนดรหัสผ่านที่มีความซับซ้อน เช่น มีความยาวขั้นต่ำ ๘ ตัวอักษร และประกอบด้วยตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และสัญลักษณ์พิเศษ ในการเข้าถึงระบบสารสนเทศ

๑.๗ การควบคุมการเข้าถึงจากภายนอก (Remote Access) การเข้าถึงต้องได้รับอนุญาตจาก ผู้บริหารหน่วยงาน หรือ ผู้บริหารสุงสุดของหน่วยงาน

๒. การบริหาจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งานที่ได้รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

กำหนดให้มีการบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการ ควบคุม จำกัด และเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้

๑.๑ ผู้ดูแลระบบสารสนเทศกองแบบแผน ต้องกำหนดแบบฟอร์มการขอเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สามารถนำไปตรวจสอบได้ ประกอบด้วย ชื่อ นามสกุล ตำแหน่ง กลุ่ม เป็นต้น

๒. การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการดังนี้

๒.๑ ให้บุคคลากรกรอกข้อมูลลงแบบฟอร์มขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศกับเจ้าของระบบ

๒.๒ ผู้ดูแลระบบนำส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศต่อเจ้าของระบบ

๒.๓ เจ้าของระบบพิจารณาและอนุมัติสิทธิ์การเข้าถึงระบบสารสนเทศ

๒.๔ ผู้ดูแลระบบกำหนดสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมทั้งแจ้งให้บุคลากรรับทราบ

๒.๕ กรณีบุคคลภายนอก

(๑) ให้บุคคลภายนอก กรอกข้อมูลลงในแบบฟอร์การขอเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมระบุเหตุผลการเข้าใช้งาน หรือหนังสือขอเข้าใช้งานจากบริษัทหรือหน่วยงานต้นสังกัด

(๒) ให้หน่วยงานพิจารณาเหตุผล และดำเนินการส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้เจ้าของระบบ

(๓) ให้เจ้าของระบบพิจารณาอนุมัติสิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมทั้งแจ้งข้อมูลให้รับทราบ

๓. การสร้างบัญชีผู้ใช้งาน (Username) และการกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้เจ้าของระบบ กำหนด เช่น ชื่อภาษาอังกฤษตามด้วยนามสกุลตัวแรก หรือลักษณะอื่นใดตามที่เจ้าของระบบ ที่มีการตกลงร่วมกัน

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

๓.๓ เมื่อมีการเปลี่ยนแปลงข้อมูลให้แอดมินแจ้งเจ้าของระบบทราบ เพื่อปรับปรุงข้อมูลให้เป็นปัจจุบัน

๔. การยกเลิกสิทธิ์การใช้งานของบุคลากรหรือบุคคลภายนอกผู้ดูแลระบบให้ดำเนินการ ดังนี้

๔.๑ ให้บุคลากรหรือบุคคลภายนอกแจ้งเจ้าของระบบเพื่อขอยกเลิกการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ของบุคลกร เมื่อมีการลาออก โอนย้าย หรือสิ้นสุดการจ้าง

๔.๑.๑ กรณีบุคลากร หรือ บุคคลภายนอก ให้ผู้ดูแลระบบดำเนินการปิดบัญชีผู้ใช้งาน (Account) แจ้งกลับไปยังหน่วยงานรับทราบ ภายใน ๑๕ วัน

๔.๑.๒ กรณีผู้ดูแลระบบหน่วยงานภายใน ให้ผู้ดูแลระบบระดับกรม ดำเนินการยกเลิกสิทธิ์การใช้งานของทุกระบบงาน และแจ้งให้ทราบการยกเลิกสิทธิ์ภายใน ๗ วัน

๕. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และสารสนเทศของผู้ใช้งาน ให้ดำเนินการ ดังนี้

๕.๑ กรณีที่มีการเปลี่ยนตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้แจ้งเจ้าของระบบสารสนเทศ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๕.๒ ในกรณีที่ผู้ใช้งาน ต้องการเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศที่สูงกว่าสิทธิ์ที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อเจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๖. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๖.๑ กรณีผู้ใช้งานลืมรหัสผ่าน (Password) ให้แจ้งแอดมินและให้ดำเนินการตามที่เจ้าของระบบกำหนดไว้

๖.๒ ผู้ใช้งานต้องเปลี่ยน (Password) ใหม่ ทุก ๓ - ๖ เดือน หรือตามความเสี่ยงของระบบ และรหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสเดิม

๗. ผู้ดูแลระบบ ต้องทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง เพื่อกำหนดสิทธิ์ให้สอดคล้องกับภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัย ตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์กำหนดไว้

๓. การควบคุมการเข้าถึงเครือข่าย (Computer Network Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายคอมพิวเตอร์ที่มีความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงเรือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึง

๒. กำหนดแนวปฏิบัติในการยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายในองค์กร (User Authentication for External Connections) โดยต้องยืนยันตัวตนบุคคลก่อนที่จะอนุญาต ให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่าย ระบบคอมพิวเตอร์และรบบสารสนเทศของหน่วยงานได้

แนวปฏิบัติ

๑. การเข้าถึงเครือข่ายของผู้ใช้งาน

๑.๑ การใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet) ให้ดำเนินการดังนี้

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

๑.๑.๒ ควบคุมการเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) สูงและไม่เกี่ยวข้องกับการปฏิบัติราชการ เช่น รายการบันเทิงต่างๆ ในเวลาราชการ เป็นต้น

๑.๑.๓ ห้าเข้าชมเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ผิดศีลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์เสื่อมเสีย เป็นต้น

๑.๑.๔ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลความลับของหน่วยงาน เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๕ ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุมครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเคร่งครัด

๑.๑.๖ ต้องระมัดระวังการดาวน์โหลดข้อมูลหรือโปรแกรมต่างๆ เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ โดยแจ้งให้ผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัดทราบก่อนติดตั้งใช้งาน

๑.๒ การใช้งานเครือข่าย Local Area Network (Lan) ให้ดำเนินการ ดังนี้

๑.๒.๑ ผู้ดูแลระบบต้องทำการตั้งค่า (Configuration) เลขที่อยู่ไอพี (IP Address) เมื่อมีการนำอุปกรณ์มาใช้ในหน่วยงาน

๑.๒.๒ ผู้ใช้งานต้องใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตัวเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายกรมสนับสนุนบริการสุขภาพ

๑.๓ การใช้งานเครือข่ายไร้สาย (WI-FI) ให้ดำเนินการ ดังนี้

๑.๓.๑ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า Services Set Identifier (SSID) ที่ถูกกำหนดจากผู้ผลิตทันทีเมื่อนำอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) มาติดตั้งใช้งาน

๑.๓.๒ ผู้ใช้งานต้องใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตัวเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (WI-FI) ภายในเครือข่ายกรมสนับสนุนบริการสุขภาพ

๑.๓.๓ ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่ ที่เป็นทรัพย์สินของหน่วยงานไปใช้งานเครือข่ายไร้สาย (WI-FI) ที่ไม่น่าเชื่อถือ

๑.๓.๔ ผู้ใช้งานต้องระวังในการทำธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ระหว่างใช้งานเครือข่ายไร้สาย (W-IFI) เนื่องจากอาจเกิดความไม่ปลอดภัยและอาจขาดการเชื่อมต่อของสัญญาณ

๑.๓.๕ ห้ามผู้ใช้งานติดตั้งและเปิดใช้งานโปรแกรมดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สาย (WI-FI) ของหน่วยงานและมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๔๐ และที่แก้ไขเพิ่มเติม

๑.๔ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการดังนี้

๑.๔.๑ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ภายใต้หน่วยงานควรนำเสนอเกี่ยวกับภารกิจของหน่วยงาน เช่น ผลการดำเนินงาน และข่าวสาร โดยการนำเข้าข้อมูลต้องเป็นผู้ที่ได้รับมอบหมายจากหน่วยงาน และต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๔๐ และที่แก้ไขเพิ่มเติม

๑.๔.๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของหน่วยงานผ่านสื่อสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๔.๓ กรณีหน่วยงานอื่นมีความคิดเห็นที่แตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงต่อไป

๑.๔.๔ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากหน่วยงาน และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑.๔.๕ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งานต้องรับผิดชอบความเสียหายและดำเนินการแก้ไขทันที ทั้งนี้ให้แจ้งผู้บังคับบัญชารับทราบ

๒. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Network) ให้ดำเนินการ ดังนี้

๒.๑ ผู้รับผิดชอบด้านสารสนเทศต้องจัดทำผังระบบเครือข่าย (Network Diagram) พร้อมรายละเอียดบนเครือข่ายที่เห็นว่ามีความจำเป็นต่อการใช้งาน เช่น กลุ่มอุปกรณ์ เลขไอพี (IP Address) และให้มีการปรับปรุงทุก ๑ ปี หรือมีนัยสำคัญ

๒.๒ การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ มาใช้เชื่อมต่อเครือข่ายต้องได้รับอนุญาตจากผู้รับผิดชอบด้านสารสนเทศหน่วยงาน เช่น แทปเลต โทรศัพท์มือถือ เป็นต้น

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

นโยบาย

๔.๑ กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการโดยต้องมีการควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวตนที่ปลอดภัย

๔.๒ กำหนดแนวปฏิบัติใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและควบคุมการใช้โปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการ ความมั่นคงปลอดภัยที่กำหนดไว้

แนวปฏิบัติ

๑. การกำหนดขั้นตอนการปฏิบัติงาน ดังนี้

๑.๑ ผู้ใช้งานไม่มีสิทธิ์เปลี่ยนแปลงแก้ไขค่าต่างๆ ของระบบปฏิบัติการ เช่น (Product Key) หรือ License ของระบบปฏิบัติการ และคอนฟิกกูเรชั่น (Configuration) ต่างๆ เช่น Computer Name , IP Address เป็นต้น

๑.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านในการเข้าใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๑.๓ หลังจากผู้ดูแลระบบติดตั้งระบบปฏิบัติการเสร็จ ผู้ใช้งานต้องบริหารจัดการรหัสผ่านหรือเปลี่ยนรหัสผ่านที่กำหนดไว้แต่ต้นทันที

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

๑.๕ ก่อนการเข้าใช้งานระบบปฏิบัติการผู้ใช้งานจะต้องลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

๑.๖ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม บนระบบปฏิบัติการและเว็บไซต์ของหน่วยงาน

๑.๗ ห้ามผู้ใช้งานเข้าควบคุมระบบปฏิบัติการคอมพิวเตอร์หรือระบบสารสนเทศจากภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๑.๘ ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรม peer-to-peer โปรแกรมประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมดักจับรหัสผ่าน (Network Sniffer) และโปรแกรมประเภท Formatter หรือโปรแกรมที่มีความเสี่ยง เว้นแต่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๑.๙ ซอฟต์แวร์ที่หน่วยงานใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

๑.๑๐ ซอฟต์แวร์ที่หน่วยงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้งถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๑.๑๑ ห้ามใช้ทรัพยากรทุกประเภทของกองแบบแผน เพื่อประโยชน์ทางการค้า

๒. การใช้งานโปรแกรมยูทิลิตี้(Use system utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมสำหรับคอมพิวเตอร์ที่สำคัญให้ดำเนินการ ดังนี้

๒.๑ การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับอนุมัติจากผู้ดูแลระบบ เพื่อจำกัดและควบคุมการใช้งาน

๒.๒ โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

๒.๓ ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

หมวดที่ ๒

การรักษาความปลอดภัยฐานข้อมูลและการสำรองข้อมูล (Database Security and Backup)

วัตถุประสงค์

เพื่อจัดทำระบบสำรองข้อมูลระบบสารสนเทศกองแบบแผนให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศและการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศกองแบบแผน ซึ่งได้รวบรวมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ การเตรียมความพร้อมฉุกเฉิน และการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและการกู้คืนข้อมูลสารสนเทศไว้แล้วด้วย เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่องแม้ในสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่างๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม

การรักษาความปลอดภัยข้อมูล

๒.๑ การทดสอบและปรับปรุงแผนเตรียมความพร้อมให้ผู้ที่ได้รับมอบหมายปฏิบัติดังต่อไปนี้

๒.๑.๑ กำหนดให้มีการจัดทำแผนการทดสอบการกู้คืนระบบงานที่สำคัญและการทดสอบแผนอย่างน้อยปีละ ๑ ครั้ง

๒.๑.๒ ปรับปรุงแผนกู้คืนระบบงานที่สำคัญให้ทันสมัยอยู่เสมอ

๒.๒ การสำรองและทดสอบข้อมูลระบบฐานข้อมูลที่สำคัญตามระยะเวลาที่เหมาะสมสำหรับผู้ดูแลระบบ ให้ปฏิบัติดังต่อไปนี้

๒.๒.๑ ให้เจ้าหน้าที่งานเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย ดำเนินการสำรองข้อมูลระบบฐานข้อมูลกองแบบแผน ให้อยู่ในสภาพพร้อมใช้งานอย่างสม่ำเสมอ โดยจะต้อง Backup Database ของกองแบบแผนทุกวันศุกร์ทุกสัปดาห์ หากไม่สามารถดำเนินการได้ในวันดังกล่าวให้ดำเนินการในวันก่อนหน้า และจะต้องเก็บไฟล์ Backup ไว้ย้อนหลังอย่างน้อย ๓ เดือน

๒.๒.๒ สำรองข้อมูล Database กองแบบแผน ไว้อย่างน้อย ๒ แห่ง ได้แก่ external Hard Disk และ คอมพิวเตอร์ผู้รับผิดชอบ

๒.๒.๓ ดำเนินการตรวจสอบการสำรองข้อมูลว่าสำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จให้หาสาเหตุเพื่อแก้ไขและดำเนินการตรวจสอบใหม่ จนกว่าการสำรองข้อมูลจะครบถ้วน

๒.๒.๔ ดำเนินการทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง และตรวจสอบว่าข้อมูลยังคงสามารถใช้งานได้เป็นปกติ

๒.๓ การสำรองข้อมูลสำหรับเจ้าหน้าที่กองแบบแผน ให้ปฏิบัติดังต่อไปนี้

๒.๓.๑ เจ้าหน้าที่กองแบบแผนทุกคนจะต้องมีการสำรองงานที่ตนรับผิดชอบไว้อย่างน้อย ๑ แห่ง โดยแนะนำให้เก็บ External Hard Disk และระบบ Cloud เช่น Google Drive OneDrive เป็นต้น

หมวดที่ ๓
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Management)

๓.๑ ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกองแบบแผน กรมสนับสนุนบริการสุขภาพ อย่างน้อยปีละ ๑ ครั้ง

๓.๒ ระบุความเสี่ยง

- ความเสี่ยงที่อาจเกิดขึ้นในระบบเทคโนโลยีสารสนเทศ เช่น ความเสี่ยงจากการถูกโจมตีทางไซเบอร์ หรือความเสี่ยงจากความผิดพลาดของมนุษย์

๓.๓ ประเมินความเสี่ยง

- วิเคราะห์ความเสี่ยงที่ระบุโดยพิจารณาจากความเป็นไปได้ของการเกิดเหตุการณ์และผลกระทบที่อาจจะเกิดขึ้น ซึ่งสามารถใช้เกณฑ์คะแนนในการประเมินได้

๓.๔ จัดเรียงลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและนำความเสี่ยงที่อยู่ในระดับสูงถึงระดับสูงมากมาจัดทำแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ

- ทำการจัดเรียงความเสี่ยงตามลำดับความสำคัญโดยพิจารณาจากคะแนนการประเมิน ซึ่งความเสี่ยงที่มีคะแนนสูงจะได้รับการจัดลำดับเป็นความเสี่ยงสำคัญที่สุดทำการจัดเรียงความเสี่ยงตามลำดับความสำคัญโดยพิจารณาจากคะแนนการประเมิน ซึ่งความเสี่ยงที่มีคะแนนสูงจะได้รับการจัดลำดับเป็นความเสี่ยงสำคัญที่สุด

๓.๓ จัดทำแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศไปสู่การปฏิบัติ

- ความเสี่ยงที่จัดลำดับความสำคัญสูงถึงสูงมาก ควรทำการจัดทำแผนควบคุมเพื่อรับมือกับความเสี่ยงเหล่านี้ เช่น การเพิ่มระบบรักษาความปลอดภัยที่มีประสิทธิภาพ หรือการอบรมบุคลากรให้มีความรู้เกี่ยวกับการป้องกันภัยทางไซเบอร์

๓.๔ ติดตามประเมินผลแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓.๕ จัดทำแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ

หมวดที่ ๔
การดำเนินการต่อเหตุการณ์ด้านความมั่นคงทางด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าพื้นที่ใช้งานระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศซึ่งมีผลบังคับใช้กับผู้ใช้งาน และผู้เกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศกองแบบแผน ให้ดำเนินการ ดังนี้

๔.๑ การเตรียมตัว (Preparation):

- จัดทำแผนการรับมือกับเหตุการณ์และกระบวนการทำงานที่ชัดเจน
- ฝึกอบรมบุคลากรให้มีความรู้และทักษะในการจัดการเหตุการณ์

๔.๒ การตรวจจับ (Detection and Analysis)

- รวบรวมข้อมูลที่เกี่ยวข้องกับเหตุการณ์และทำการวิเคราะห์เพื่อประเมินความรุนแรงและผลกระทบ

๔.๓ การควบคุมเหตุการณ์ (Containment, Eradication, and Recovery)

- ทำการควบคุมเหตุการณ์เพื่อป้องกันการแพร่กระจายของภัยคุกคาม
- กำจัดภัยคุกคามออกจากระบบและทำการกู้คืนระบบให้กลับสู่สภาพปกติ
- ตรวจสอบและฟื้นฟูข้อมูลที่อาจได้รับความเสียหาย

๔.๔ การป้องกันและปรับปรุง (Post-Incident Activity)

- ทำการวิเคราะห์เหตุการณ์เพื่อหาสาเหตุและช่องโหว่ที่ทำให้เกิดเหตุการณ์
- ปรับปรุงแผนการรับมือและระบบรักษาความปลอดภัยให้มีประสิทธิภาพมากยิ่งขึ้น
- จัดทำรายงานเหตุการณ์และสื่อสารผลการวิเคราะห์กับผู้ที่เกี่ยวข้อง

หมวดที่ ๕
การสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

วัตถประสงค์

๑. เพื่อเสริมสร้างความรู้ความเข้าใจในการใช้ระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งาน กองแบบแผน

๒. เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศ กองแบบแผน เป็นไปอย่างมีความมั่นคงปลอดภัย

๓. เพื่อป้องกันการกระทำความผิดที่เกิดจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

นโยบาย

กำหนดแนวทางปฏิบัติ เนื้อหา หลักสูตร ในการส่งเสริมความตระหนักด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้กับเจ้าหน้าที่กองแบบแผน

แนวปฏิบัติ

๑. จัดให้มีการทบทวน ปรับปรุง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กองแบบแผน อย่างน้อยปีละ ๑ ครั้ง

๒. ฝึกอบรมแนวปฏิบัติตามนโยบาย โดยใช้วิธีเสริมเนื้อหาแนวปฏิบัติตามนโยบายกับหลักสูตรต่างๆ

๓. ประกาศประชาสัมพันธ์นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ หรือข้อระวัง ในรูปแบบที่สามารถเข้าใจง่าย โดยปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๔. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๕. ผู้ใช้งานจะต้องปฏิบัติตามกฎหมายใด ๆ ที่ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบของกรมสนับสนุนบริการสุขภาพ ทั้งนี้หากไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๖. จัดทำทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยอย่างน้อยควรมีรายละเอียดเกี่ยวกับชื่ออุปกรณ์ หมายเลขครุภัณฑ์ ชื่อผู้ใช้งาน IP สถานที่ใช้งาน รายละเอียดเกี่ยวกับคุณลักษณะของทรัพย์สิน เช่น CPU RAM Hard Disk เป็นต้น

- ขึ้นทะเบียนทรัพย์สินที่ได้รับการจัดสรรทุกครั้ง
- ตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง
- หน่วยงานต้องระบุรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงเครือข่ายและ Software

หมวดที่ ๖
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

๑. เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศของกองแบบแผน กรมสนับสนุนบริการสุขภาพ

๒. เพื่อสนับสนุนให้การดำเนินงานด้านเทคโนโลยีสารสนเทศขององค์กรเป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับพันธกิจและเป้าหมายของกองแบบแผน กรมสนับสนุนบริการสุขภาพ

๓. เพื่อให้บุคลากรทุกระดับมความตระหนักถึงบทบาทของตนเองและปฏิบัติงานตามมาตรฐานที่กำหนด

แนวปฏิบัติ

๑. ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

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

(๑) รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติการ

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ระดับบริหาร ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการกองแบบแผน

(๑) รับผิดชอบ กับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษาทบทวน วางแผนติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

๓. ระดับปฏิบัติการ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนราชการ กองแบบแผน เช่น เจ้าหน้าที่ที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) ปฏิบัติตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการความไม่แน่นอนและภัยพิบัติ

(๓) ดำเนินการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่หน่วยงานกำหนด

(๔) รายงานกลุ่มเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ กรณีตรวจเจอการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker)

(๕) รับผิดชอบในการรักษาความปลอดภัยระบบสารสนเทศ กองแบบแผน กรมสนับสนุนบริการสุขภาพ

(๖) ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองแบบแผน

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๒ มีนาคม พ.ศ. ๒๕๖๙

(นายอับดุลกอเดส อมรีก)
ผู้อำนวยการกองแบบแผน