การติดตามผลการประกาศใช้ข้อปฏิบัติด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
กลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ ครั้งที่ ๑/๒๕๖๔
วันที่ ๒๐ มกราคม ๒๕๖๔

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
หมวดที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)			
๑.การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูลให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้			
๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศและการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ต้องสอดคล้องและเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการ	✓		
๑.๒ งานเทคโนโลยีสารสนเทศ โดยผู้ดูแลระบบ มีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) รวมทั้งกำหนดสิทธิ ให้กับผู้ใช้งาน (User) สำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุมการใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศของกลุ่มตรวจสอบภายใน	✓		
๑.๓ ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น	✓		
๑.๔ เมื่อมีความจำเป็นให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ และอุปกรณ์การประมวลผลข้อมูล ทั้งทางกายภาพและจากระยะไกล (Remote Access) บุคคลภายนอกดังกล่าว ต้องแจ้งเหตุผลความจำเป็นเพื่อรายงานเป็นลายลักษณ์อักษรแก่ผู้อำนวยการกลุ่มตรวจสอบภายใน และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหายบุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน	-	-	ยังไม่เคยเกิดขึ้น
๑.๕ การติดตั้ง ซ่อมแซมและนำอุปกรณ์ใดที่เป็นระบบคอมพิวเตอร์ออกจากห้องกลุ่มตรวจสอบภายใน ต้องได้รับการอนุมัติจากผู้อำนวยการกลุ่มตรวจสอบภายในก่อนเริ่มดำเนินการทุกครั้ง	-	-	ยังไม่เคยเกิดขึ้น
๑.๖ ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในเครื่องควบคุมและศูนย์ปฏิบัติคอมพิวเตอร์(เครื่องData Center) ของกลุ่มตรวจสอบภายใน เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบที่รับผิดชอบในการควบคุมและปฏิบัติที่เครื่อง Data Center	✓		

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
๑.๗ เจ้าหน้าที่ผู้ปฏิบัติงาน หรือบุคคลภายนอก ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน		✓	ยังมีบุคลากรบางท่านไม่ปฏิบัติ จึงขอความร่วมมือ
๒.การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนดดังนี้			
๒.๑ สิทธิของผู้ใช้งาน (user) ประกอบด้วย ๒.๑.๑ อ่านอย่างเดียว ๒.๑.๒ สร้างข้อมูล ๒.๑.๓ แก้ไขข้อมูล ๒.๑.๔ ลบข้อมูล	✓		
๒.๒ สิทธิผู้ดูแลระบบ (Administrator) กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ	✓		
๓.การปรับปรุงการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศให้สอดคล้อง ตามภารกิจและการรักษาความมั่นคงปลอดภัย			
๓.๑ ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง เพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัย ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด	✓		
หมวดที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (Use Access Management)			
๑.การลงทะเบียนผู้ใช้งาน (User Registration) ให้ดำเนินการ ดังนี้			
๑.๑ ให้งานเทคโนโลยีสารสนเทศ กำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศสำหรับบุคลากร กลุ่มตรวจสอบภายในและบุคคลภายนอกอย่างน้อยประกอบด้วย ชื่อ นามสกุล ตำแหน่ง สังกัด หมายเลขโทรศัพท์ และจดหมายอิเล็กทรอนิกส์ ที่ใช้งานในปัจจุบัน รวมทั้งจดหมายอิเล็กทรอนิกส์สำรองของผู้ขอใช้งาน		✓	ยังไม่ได้กำหนดแบบฟอร์มงานเทคโนโลยีสารสนเทศรับดำเนินการต่อไป
๑.๒ การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้			
๑.๒.๑ กรณีบุคลากรกลุ่มตรวจสอบภายใน			
(๑) ให้บุคลากรใหม่กรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศ ในวันรายงานตัว	-	-	ยังไม่เคยเกิดขึ้น
(๒) ให้กลุ่มตรวจสอบภายในส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคลากรของ	-	-	ยังไม่เคยเกิดขึ้น

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
กลุ่มตรวจสอบภายใน ให้กลุ่มเทคโนโลยีสารสนเทศ เพื่อสร้างบัญชี ผู้ใช้งาน และกำหนดรหัสผ่านชั่วคราว			
(๓) ให้ผู้ดูแลระบบ กำหนดสิทธิให้บุคลากรใหม่ พร้อมทั้งแจ้งให้บุคลากรใหม่รับทราบ			
๑.๒.๒ กรณีบุคลากรภายนอกกลุ่มฯ			
(๑) ให้สำนัก/กอง/ศูนย์/กลุ่ม แจ้งความประสงค์พร้อมเหตุผลในการให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคคลภายนอก	-	-	ยังไม่เคยเกิดขึ้น
(๒) ให้งานเทคโนโลยีสารสนเทศ พิจารณาเหตุผลดังกล่าวและอนุมัติการเข้าใช้งานระบบ ก่อนดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านชั่วคราว	✓		
(๓) ให้ผู้ดูแลระบบ กำหนดสิทธิให้ผู้ใช้งานตามที่ได้รับอนุมัติ พร้อมทั้งแจ้งให้บุคลากรภายนอกได้รับทราบ	✓		
๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และการกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้			
๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้ใช้ชื่อภาษาอังกฤษตามบัตรประจำตัวประชาชนตามด้วยเครื่องหมาย “_” หรือ “.” ตามด้วยอักษรนามสกุลตัวแรก หรืออักษรอื่นใดที่มีการตกลงร่วมกัน	✓		
๑.๓.๒ การกำหนดรหัสผ่าน (Password) ชุดของตัวอักษร ตัวเลข และอักขระพิเศษ อย่างน้อย ๘ ตัวอักษรขึ้นไปและยากต่อการคาดเดา โดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตน (Authentication) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ		✓	ยังกำหนดเป็น ๖ ตัวอักษรอยู่
๑.๓.๓ ให้ผู้ดูแลระบบ แจ้งบัญชีผู้ใช้งานและรหัสผ่านชั่วคราวให้ผู้ใช้งานทราบโดยตรง	✓		
๑.๓.๔ เมื่อบุคลากร กลุ่มตรวจสอบภายในและบุคลากรภายนอกมีการเปลี่ยนชื่อหรือนามสกุลให้แจ้งมายังงานเทคโนโลยีสารสนเทศ เพื่อเปลี่ยนบัญชีผู้ใช้งาน (Username)	-	-	ยังไม่เคยเกิดขึ้น
๑.๔ บัญชีผู้ใช้งาน สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ได้จนกว่าบุคลากรหรือบุคคลภายนอกสิ้นสุดการ	-	-	ยังไม่เคยเกิดขึ้น

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
ปฏิบัติหน้าที่ในหน่วยงานของตนเอง และงานเทคโนโลยีสารสนเทศต้องดำเนินการยกเลิกสิทธิการใช้งาน			
๒. การยกเลิกสิทธิการใช้งานของบุคลากรหรือบุคคลภายนอกให้ดำเนินการ ดังนี้			
๒.๑ กรณีบุคลากรของกลุ่มตรวจสอบภายใน			
๒.๑.๑ ให้แจ้งงานเทคโนโลยีสารสนเทศ เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก ให้โอน หรือสิ้นสุดการจ้าง	-	-	ยังไม่เคยเกิดขึ้น
๒.๑.๒ งานเทคโนโลยีสารสนเทศจะปิดบัญชีผู้ใช้งานชั่วคราวเป็นเวลา ๙๐ วัน หากบุคลากรที่มีความประสงค์จะใช้ข้อมูลในบัญชีผู้ใช้งานดังกล่าว ให้แจ้งความประสงค์พร้อมเหตุผลต่องานเทคโนโลยีสารสนเทศ เพื่อขอเปิดใช้งานบัญชีผู้ใช้งานดังกล่าวชั่วคราว พร้อมทั้งกำหนดรหัสผ่านชั่วคราว ทั้งนี้ เมื่อครบกำหนด ๙๐ วัน นับจากมีคำสั่งเป็นลายลักษณ์อักษร งานเทคโนโลยีสารสนเทศจะยกเลิกการเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศและลบข้อมูลสารสนเทศของบัญชีผู้ใช้งานดังกล่าวเป็นการถาวร	-	-	ยังไม่เคยเกิดขึ้น กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม เป็นผู้ปฏิบัติ แต่ไม่ได้ปฏิบัติตามขั้นตอนที่ประกาศไว้
๒.๒ กรณีบุคคลภายนอก			
๒.๒.๑ ให้หน่วยงาน แจ้งความประสงค์ยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศต่องานเทคโนโลยีสารสนเทศทันทีที่หมดความจำเป็น อย่างถาวร	-	-	ยังไม่เคยเกิดขึ้น
๓.การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้ใช้งานให้ดำเนินการ ดังนี้			
๓.๑ ผู้ดูแลระบบ ทำหน้าที่ตรวจสอบสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ตามแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ สำหรับบุคลากร กลุ่มตรวจสอบภายในหรือบุคคลภายนอกให้สอดคล้องกับคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ หรือเหตุผลความจำเป็นของหน่วยงาน ที่ได้แจ้งความประสงค์ในการให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศแล้วแต่กรณี	✓		
๓.๒ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้หน่วยงานแจ้งงานเทคโนโลยีสารสนเทศ เพื่อเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบ	-	-	ยังไม่เคยเกิดขึ้น

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
สารสนเทศ ให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว			
๓.๓ ในกรณีที่ผู้ใช้งาน (User) ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศที่สูงกว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่องานเทคโนโลยีสารสนเทศ ทั้งนี้ ต้องมีการกำหนดระยะเวลาการใช้งานและยกเลิกสิทธิการใช้งานทันที่ที่หมดความจำเป็น	-	-	ยังไม่เคยเกิดขึ้น
๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการตามหลักเกณฑ์ดังนี้			
๔.๑ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านชั่วคราว ทันทีที่เข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศในครั้งแรก		✓	ผู้ดูแลระบบเป็นคนแจ้งเวียนให้เปลี่ยนรหัสผ่าน จริงเลยไม่มีการเปลี่ยนรหัสอีก
๔.๒ การเปลี่ยนรหัสผ่านใหม่ (Password) ให้ดำเนินการผ่านระบบบริหารจัดการรหัสผ่าน โดยใช้บัญชีผู้ใช้งานและรหัสผ่านเดิม	✓		
๔.๓ กรณีผู้ใช้งานไม่สามารถเปลี่ยนรหัสผ่านใหม่ได้ ให้แจ้งงานเทคโนโลยีสารสนเทศ เพื่อขอรับรหัสผ่านชั่วคราว ยกเว้นเป็นระบบยืนยันตัวตนของการเข้าใช้งานเครือข่ายให้แจ้งกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม		✓	ผู้ดูแลระบบแจ้งรหัสจริง ถึงแม้เปลี่ยนรหัสแล้ว ผู้ดูแลระบบก็สามารถทราบได้อยู่ดีเพราะไม่ได้เข้ารหัสไว้ที่ฐานข้อมูล
๔.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านใหม่ ทุก ๖ เดือน และรหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม		✓	จากการสอบถามผู้ใช้งาน สามารถเปลี่ยนได้ปีละ๑ ครั้ง
๕. ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง	✓		
๖. ให้งานเทคโนโลยีสารสนเทศ กลุ่มตรวจสอบภายใน จัดฝึกอบรมให้แก่ผู้ใช้งาน เพื่อให้มีความรู้ ความเข้าใจและเกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ อย่างน้อยปีละ ๑ ครั้ง หรือจัดให้ผู้ใช้งาน เข้าร่วมการฝึกอบรมที่หน่วยงานอื่นจัดขึ้น	-	-	เข้าวาระการประชุมกลุ่ม **ยังไม่ได้ดำเนินการ

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
๗. ให้งานเทคโนโลยีสารสนเทศ กลุ่มตรวจสอบภายใน กำหนดมาตรการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศ ตามความเหมาะสม ได้แก่ การไม่เปิดจดหมายอิเล็กทรอนิกส์ที่ไม่ระบุที่มาหรือชื่อผู้ส่งที่น่าสงสัย โดยให้ลบจดหมายอิเล็กทรอนิกส์ทันที หรือการแจ้งเตือนผู้ใช้งาน เมื่อมีไวรัสแพร่ระบาด	✓		เป็นกำหนดมาตรการการแสดงทรัมไดร์ก่อนนำมาใช้
หมวด ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)			
๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้			
๑.๑ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านชั่วคราวทันทีที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในครั้งแรก		✓	ขอความร่วมมือ
๑.๒ ผู้ใช้งาน ต้องกำหนดรหัสผ่านตามหมวดที่ ๒ ข้อที่ ๑.๓	✓		
๑.๓ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่านใหม่ทุก ๖ เดือน และรหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม		✓	จากการสอบถามผู้ใช้งานสามารถเปลี่ยนได้ปีละ๑ ครั้ง
๑.๔ ผู้ใช้งาน ต้องไม่ใช้รหัสผ่านร่วมกับบุคคลอื่น และไม่ควรให้ระบบคอมพิวเตอร์หรือระบบสารสนเทศจำรหัสผ่านในการเข้าใช้งานโดยอัตโนมัติ		✓	เพราะง่ายต่อการจำ จึงขอความร่วมมือ
๑.๕ ผู้ใช้งาน ต้องไม่เปิดเผยรหัสผ่านสำหรับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเป็นความลับเสมือนเป็นสมบัติส่วนตัว ห้ามจดหรือเขียน รหัสผ่านที่ใช้งานไว้ในที่เปิดเผย		✓	ยังมีบุคลากรบางคนจดรหัสผ่านไว้หน้าคอมพิวเตอร์ จึงขอความร่วมมือ
๑.๖ หากมีความจำเป็นต้องบอกรหัสผ่านแก่บุคคลอื่นเนื่องจากความจำเป็นในการเข้าถึงหลังจากดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่านใหม่ทันที		✓	ยังมีบุคลากรบางคนไม่เปลี่ยนรหัส
๑.๗ หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งานและรหัสผ่านของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของบัญชีผู้ใช้งาน ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดในเอกสารฉบับนี้แล้ว	-	-	ยังไม่เคยเกิดขึ้น
๑.๘ ผู้ดูแลระบบ ต้องเปลี่ยนรหัสผ่านใหม่ทุก ๓ เดือน และรหัสผ่านใหม่ ต้องไม่ซ้ำกับรหัสผ่านเดิม		✓	ยังไม่ได้ดำเนินการ
๒.การป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งานต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ	✓		

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
๓. การควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้ดำเนินการตามหลักเกณฑ์ ดังนี้			
๓.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ในการประมวลผลข้อมูลมีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานของกรมสนับสนุนบริการสุขภาพเท่านั้น	✓		
๓.๒ ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ของกลุ่มตรวจสอบภายในและให้ใช้งานด้วยความระมัดระวังเสมือนเป็นทรัพย์สินของตน	✓		
๓.๓ ผู้ใช้งานต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใดๆ ที่เครื่องคอมพิวเตอร์ลูกข่ายหรือเครื่องคอมพิวเตอร์พกพาหรือระบบคอมพิวเตอร์หรือระบบสารสนเทศ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลต่องานเทคโนโลยีสารสนเทศ เพื่อประสานไปยังกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรมต่อไป	✓		
๓.๔ ผู้ใช้งาน ต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา หรือการ์ดจำในโทรศัพท์มือถือ เพื่อป้องกันการรั่วไหลของข้อมูล	✓		สำหรับมือถือให้ระมัดระวังในการบันทึกเก็บข้อมูลอันเป็นความลับ
๓.๕ การทำลายอุปกรณ์บันทึกข้อมูลหรือการนำอุปกรณ์บันทึกข้อมูลกลับมาใช้งานใหม่ให้ดำเนินการ ดังนี้			
๓.๕.๑ การทำลายอุปกรณ์บันทึกข้อมูล เช่น Flash Drive CD/DVD ฮารดิสก์ เทป เป็นต้น ให้ใช้วิธีการทุบ หรือบดให้เสียหาย หรือเผาทำลายด้วยวิธีการทำลายตามมาตรฐานสากลหรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอกนิกส์กำหนด	-	-	ยังไม่เคยเกิดขึ้น
๓.๕.๒ การนำอุปกรณ์บันทึกข้อมูลไปใช้งานใหม่ ให้ฟอร์เมต (Format) อุปกรณ์บันทึกข้อมูลนั้น โดยใช้วิธีการฟอร์เมต (Format) ตามมาตรฐานสากลหรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอกนิกส์กำหนด	✓		
หมวด ๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)			
๑. การเข้าถึงเครือข่ายของผู้ใช้งาน (User)			
๑.๑ การใช้งานระบบเครือข่ายภายนอก (Internet) ให้ดำเนินการ ดังนี้			
๑.๑.๑ กำหนดให้ใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าใช้งาน ระบบเครือข่าย	✓		

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
ภายนอก (Internet)			
๑.๑.๒ ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม ลามกอนาจาร เว็บไซต์ที่มี เนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์ เสื่อมเสีย	✓		
๑.๑.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของกรมสนับสนุนบริการสุขภาพ ผ่านระบบเครือข่าย ภายนอก (Internet) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล	✓		
๑.๑.๔ ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคง ปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเคร่งครัด ได้แก่ ห้ามเปิดเผยข้อมูลของทางราชการโดยไม่ได้รับอนุญาต ห้ามแพร่ภาพหรือข้อมูลใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความ ผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือที่มีลักษณะลามกอนาจาร และ ไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าว ผ่านระบบเครือข่ายภายนอก (Internet) ห้ามเผยแพร่ภาพ ของผู้อื่นที่เกิดจากการสร้างขึ้น ตัดต่อ ต่อเติม หรือดัดแปลงด้วยวิธีการ ทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่จะทำให้ ผู้นั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย	✓		
๑.๑.๕ ห้ามใช้งานระบบเครือข่ายภายนอก (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) สูงที่ ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ ได้แก่ YouTube (ยกเว้นในส่วนที่เกี่ยวกับงานตามภารกิจของหน่วยงาน) หนังออนไลน์ หรือรายการบันเทิงต่างๆ ในเวลาราชการ	✓		
๑.๑.๖ ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่างๆ จากระบบเครือข่าย ภายนอก (Internet) เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบ คอมพิวเตอร์และระบบสารสนเทศ	✓		
๑.๑.๗ หลังจากใช้งานระบบเครือข่ายภายนอก (Internet) แล้วให้ปิดเว็บบราวเซอร์ (Web Browser) เพื่อป้องกันบุคคลอื่นเข้าใช้งาน	✓		

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
๑.๒ การใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ให้ดำเนินการดังนี้			
๑.๒.๑ ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่ แก้ไขเพิ่มเติม โดยเคร่งครัด และห้ามใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ในทางที่ ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศีลธรรม	✓		
๑.๒.๒ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ ด้วยการใช้งาน จดหมายอิเล็กทรอนิกส์ (E - Mail) ที่ส่งโดยโดเมนเนม (Domain Name) ของกรมสนับสนุนบริการสุขภาพ (@hss.mail.go.th	✓		
๑.๒.๓ ต้องตรวจสอบชื่อผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender) ก่อนเปิดจดหมายอิเล็กทรอนิกส์ (E - Mail) เพื่อป้องกันการเปิดไฟล์อันตรายที่อาจมีไวรัสคอมพิวเตอร์ โดยเฉพาะ Executable File ได้แก่ ไฟล์ที่มี นามสกุล .exe, .Com, bat และ inf ที่อาจนำเข้าสู่ระบบเครือข่ายกรมสนับสนุนบริการสุขภาพ	✓		
๑.๒.๔ หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ต้องออกจากระบบ (Log Out) ทันที เพื่อป้องกันบุคคลอื่นเข้าใช้งาน	✓		
๑.๓ การใช้งานเครือข่ายไร้สาย (Wi-Fi) ให้ดำเนินการ ดังนี้			
๑.๓.๑ ผู้ใช้งาน (User) ต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองใน การพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (Wi-Fi)	✓		
๑.๓.๒ ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายไร้สาย (Wi-Fi) ผู้ใช้งาน (User) จะสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะที่ได้รับอนุญาตตามสิทธิ ของเครือข่ายไร้สาย (Wi-Fi) เท่านั้น	✓		
๑.๓.๓ ผู้ใช้งาน (User) ต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็น ทรัพย์สินของ กรมสนับสนุนบริการสุขภาพ ไปใช้งานเครือข่ายไร้สาย (Wi-Fi) ที่ไม่น่าเชื่อถือ	✓		
๑.๓.๔ ผู้ใช้งาน (User) ไม่ควรทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ระหว่างการใช้งาน เครือข่ายไร้สาย (Wi-Fi) เนื่องจากอาจเกิดความไม่ปลอดภัยและอาจขาดการเชื่อมต่อของสัญญาณ	✓		
๑.๓.๕ ห้ามผู้ใช้งาน (User) ติดตั้งและเปิดการทำงานโปรแกรมประเภทดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายของกรมสนับสนุนบริการสุขภาพ และมีความผิดตาม พระราชบัญญัติว่าด้วยการกระทำ	✓		ทำหนังสือถึง IT แล้วได้รับการยกเว้น

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
ผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม			
๑.๔ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้			
๑.๔.๑ การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ (Social Network) ในนามของกรมสนับสนุนบริการ สุขภาพ/กลุ่มตรวจสอบภายใน ผู้รับผิดชอบต้องแสดงตำแหน่ง หน้าที่ สังกัดให้ชัดเจน เพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์ หรือเครื่องหมายแสดงสังกัดได้	✓		
๑.๔.๒ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ควรนำเสนอเกี่ยวกับ ภารกิจงานของ กลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ ได้แก่ วิสัยทัศน์ พันธกิจ ผลการดำเนินงาน และข่าวสาร ที่เป็นประโยชน์ มีความถูกต้อง ใช้ภาษาที่สุภาพ และมีรูปแบบที่น่าสนใจ โดยเนื้อหาต้องผ่านความเห็นชอบจากผู้ที่ได้รับมอบหมายหรือผู้บังคับบัญชาก่อนทุกครั้ง	✓		
๑.๔.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของกลุ่มตรวจสอบภายในและกรมสนับสนุนบริการสุขภาพ ผ่านเครือข่ายสังคม ออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล	✓		
๑.๔.๔ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่างต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบ ด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงในเรื่องที่เกี่ยวข้องต่อไป	✓		
๑.๔.๕ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากกลุ่มตรวจสอบภายใน หรือกรมสนับสนุนบริการสุขภาพ และ ต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว	✓		
๑.๔.๖ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที	✓		
๒.การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) การระบุและยืนยันตัวตนของผู้ใช้งานอยู่ภายนอกองค์กร (User Authentication for External Connections) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองเพื่อตรวจสอบความถูกต้องในการพิสูจน์ ยืนยันตัวตน (Authentication) ก่อนเข้าถึงเครือข่าย ระบบคอมพิวเตอร์ และระบบสารสนเทศ	-	-	ไม่เคยเกิดขึ้น

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
หมวด ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)			
๑. ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	✓		
๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง เพื่อตรวจสอบ ความถูกต้องในการพิสูจน์ ยืนยันตัวตน (Authentication) ก่อนเข้าถึงระบบปฏิบัติการ (Operating System)	✓		
๓. การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) กำหนด ดังนี้			
๓.๑ ผู้ใช้งาน (User) ต้องไม่ดัดแปลงหรือติดตั้งโปรแกรมอรรถประโยชน์ใดๆ บนระบบปฏิบัติการ ทั้งนี้ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์ต่อกลุ่มเทคโนโลยีสารสนเทศ	-	-	ยังไม่เคยเกิดขึ้น
๓.๒ การใช้งานโปรแกรมอรรถประโยชน์อื่นๆ นอกเหนือจากที่ติดตั้งมากับระบบปฏิบัติการ ได้แก่ โปรแกรมประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และ โปรแกรม Formatter กำหนดให้ผู้ดูแลระบบ (Administrator) เท่านั้นที่มีสิทธิใช้งาน	✓		ได้รับการยกเว้นจากกลุ่ม IT
๔. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์และระบบ สารสนเทศ เมื่อเว้นว่างจากการใช้งาน (Session Time Out) เมื่อครบ ๑๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ ได้รับอนุญาต	✓		
หมวด ๖ การจัดทำระบบสำรองของระบบสารสนเท(Disaster Recovery Site)			
๑. งานเทคโนโลยีสารสนเทศต้องจัดทำระบบสารสนเทศและระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน โดยมีขั้นตอน ดังนี้			
๑.๑ ผู้ดูแลระบบ (Administrator) จัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูล และการกู้คืนข้อมูล สารสนเทศ	✓		
๑.๒ ผู้ดูแลระบบ (Administrator) กำหนดรูปแบบการสำรองข้อมูลของระบบการสำรองข้อมูล (Backup System) ดังนี้			
๑.๒.๑ รายชื่อระบบคอมพิวเตอร์และระบบสารสนเทศที่ได้รับการพิจารณาคัดเลือก ดังนี้ (๑) ระบบเว็บไซต์กลุ่มตรวจสอบภายใน	✓		

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
(๒) ระบบงานตรวจสอบภายใน (๓) ระบบการประเมินผลควบคุมภายในสำหรับผู้ตรวจสอบภายใน			
๑.๒.๒ กำหนดรูปแบบการสำรองข้อมูลเฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) หรือ เฉพาะส่วนที่มีการเปลี่ยนแปลง (Differential Backup) ทุกวัน		✓	เนื่องจากข้อมูลไม่ค่อยมีการเปลี่ยนแปลง
๑.๒.๓ กำหนดรูปแบบการสำรองข้อมูลแบบสมบูรณ์ (Full Backup) ทุกเดือน	✓		
๑.๓ ผู้ดูแลระบบ (Administrator) ต้องพิมพ์รายละเอียดไว้บนตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใดที่ใช้สำหรับการสำรองข้อมูล ได้แก่ รูปแบบการสำรองข้อมูลรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล	✓		
๑.๔ ผู้ดูแลระบบ (Administrator) ต้องกำหนดรูปแบบการกู้คืนข้อมูลของระบบการสำรองข้อมูล (Backup System) โดยมีความถี่และรูปแบบ ดังนี้			
๑.๔.๑ การกู้คืนข้อมูลรายเดือนจากตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใดที่ใช้สำหรับการสำรองข้อมูลที่สำรองข้อมูลแบบสมบูรณ์ (Full Backup)	✓		ทำการกู้คืนข้อมูลปีละ ๑ ครั้ง
๒. งานเทคโนโลยีสารสนเทศดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ดังนี้			
๒.๑ กำหนดผู้มีหน้าที่รับผิดชอบระบบสารสนเทศ		✓	
๒.๒ กำหนดผู้มีหน้าที่รับผิดชอบระบบสำรองข้อมูลสารสนเทศ		✓	
๒.๓ กำหนดผู้มีหน้าที่รับผิดชอบการจัดทำแผนดังกล่าว		✓	
๒.๔ กำหนดให้ปรับปรุงแผนดังกล่าวทุก ๑ ปี	✓		พึ่งเริ่มทำแผน
๓. งานเทคโนโลยีสารสนเทศต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ อย่างน้อย ปีละ ๑ ครั้ง ทั้งนี้แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และ แผนการสำรองข้อมูล กลุ่มตรวจสอบภายใน รวมถึงการทดสอบสภาพความพร้อมใช้งานได้นำข้อมูลไปรวมไว้ในแผนบริหารความต่อเนื่องใน	✓		

ข้อปฏิบัติ	ปฏิบัติได้	ปฏิบัติไม่ได้	ปัญหาอุปสรรค
สภาวะวิกฤตด้านสารสนเทศของกลุ่มตรวจสอบภายใน			
หมวดที่ ๗ การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ กำหนดให้ผู้ที่ได้รับมอบหมายปฏิบัติดังนี้			
๑. จัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ อย่างน้อยปีละ ๑ ครั้ง	✓		
๒. จัดให้มีการจัดเรียงลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและนำความเสี่ยงที่อยู่ในระดับสูงถึงระดับสูงมาก มาจัดทำแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ	✓		
๓. นำแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศไปสู่การปฏิบัติ	✓		
๔. ติดตามประเมินผลแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ		✓	ทำเพิ่มเดือนสิงหาคม ๖๔
หมวดที่ ๘ การบริหารจัดการทรัพย์สินสารสนเทศมีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ			
๑.ทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยอย่างน้อยมีรายละเอียดเกี่ยวกับชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบและรายละเอียดเกี่ยวกับคุณลักษณะของทรัพย์สิน เช่น CPU RAM Hard Disk เป็นต้น	✓		
๒.ขึ้นทะเบียนทรัพย์สินที่ได้รับจัดสรรใหม่ทุกครั้ง		✓	**ยังไม่ดำเนินการ
๓.มีการตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง	✓		
๔.หน่วยงานต้องระบุรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์-เครือข่ายและ software	✓		
๕.กำหนดข้อปฏิบัติในการคืนทรัพย์สินภายใน ๗ วัน ตามกำหนดเวลา และกรณีการใช้งานประจำทุกวัน ต้องคืนทรัพย์เมื่อสิ้นสุดการจ้าง/หมดสัญญา/มีการโอน-ย้าย-ลาออกหรือเกษียณอายุ ภายใน ๑ วัน	✓		
๖.มาตรการในการจัดสรรคอมพิวเตอร์และอุปกรณ์ คือ เครื่องคอมพิวเตอร์ ๑ ต่อ บุคลากร ๑ คน ส่วนเครื่องพิมพ์ ๑ ต่อ บุคลากร ๓ คน เครื่องสแกนเนอร์ ๑ ต่อ บุคลากร ๕ คน สำรองไฟ ๑ ต่อ บุคลากร ๑ คน		✓	ยังมีสำรองไฟไม่เพียงพอ